IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2018, No. 1, pp. 180–200. DOI:10.13154/tosc.v2018.i1.180-200

On Efficient Constructions of Lightweight MDS Matrices

Lijing Zhou, Licheng Wang* and Yiru Sun

State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications, Beijing, China
wanglc2012@126.com,379739494@qq.com,410654266@qq.com

Abstract. The paper investigates the maximum distance separable (MDS) matrix over the matrix polynomial residue ring. Firstly, by analyzing the minimal polynomials of binary matrices with 1 XOR count and element-matrices with few XOR counts, we present an efficient method for constructing MDS matrices with as few XOR counts as possible. Comparing with previous constructions, our corresponding constructions only cost 1 minute 27 seconds to 7 minutes, while previous constructions cost 3 days to 4 weeks. Secondly, we discuss the existence of several types of involutory MDS matrices and propose an efficient necessary-and-sufficient condition for identifying a Hadamard matrix being involutory. According to the condition, each involutory Hadamard matrix over a polynomial residue ring can be accurately and efficiently searched. Furthermore, we devise an efficient algorithm for constructing involutory Hadamard MDS matrices with as few XOR counts as possible. We obtain many new involutory Hadamard MDS matrices with much fewer XOR counts than optimal results reported before.

Keywords: MDS matrix · XOR count · matrix polynomial residue ring · involutory matrix

1 Introduction

In a block cipher, the linear diffusion layer is a significant component required for the security of the cipher. The diffusion power of a matrix is usually measured by the branch number. A linear layer with a larger branch number is considered more effectively resilient to differential and linear cryptanalysis. The maximum possible branch number of an $n \times n$ matrix is $n + 1$. Matrices reaching the limitation are called as the maximum distance separable (MDS) matrices, and they are broadly used in many cryptosystems like PHOTON [15], SQUARE [13], LED [16] and AES [14]. Recently, improving the implementation has becoming a hot topic in cryptography. Some lightweight block ciphers [16, 8, 9, 30] and lightweight hash functions [15, 4, 6] are proposed to reduce the implementation cost. While, in the lightweight cryptosystems, the linear diffusion layer influences the performance of cryptosystems largely. Therefore, it is imperative to design lightweight MDS matrices for lightweight cryptography.

Recursive construction[15] is an important method to construct lightweight MDS matrices. Specifically, the main idea is that selecting a matrix A that is sparse and compact in implementation, and then calculate A^k to get an MDS matrix. This method was successfully used for the constructions of hash function PHOTON [15], block cipher LED [16] and authenticated encryption scheme PRIMATEs [1]. Further investigation of

*Corresponding author

Received: 2017-09-01, Revised: 2017-11-23, Accepted: 2018-01-23, Published: 2018-03-01

underlying this method can be found in [2, 3, 7, 26, 29]. However, the ciphers which adopt these matrices are not suited for round-based or low-latency implementations.

To reduce search space, Hadamard matrix, Circulant matrix and Special Optimal matrix [22, 25, 11, 19] are usually used as templates for constructing MDS matrices. In [19], Junod et al. proved that there are at most $3(n-1)$ identity elements in an $n \times n$ MDS matrix and an MDS matrix which has exactly $3(n-1)$ identity elements is called an *Optimal matrix*. Since the elements of these templates are repeated, hence their search space can be reduced obviously. Additionally, Liu et al. [21] and Sim et al. [25] adopted the equivalence classes regarding MDS matrices for the further reduction of the search space.

The XOR count proposed by Khoo et al. in CHES2014 [20] is an important metric for measuring the cost of implementation of a diffusion matrix. Specifically, Khoo et al. [20] used the XOR count to measure the number of XORs required to compute the multiplication of a fixed element. Additionally, they showed that there are MDS matrices with higher Hamming weight than the AES diffusion matrix, but fewer XORs. After that, many works [23, 11, 25, 21, 22, 27, 28, 31] measured the lightweight of MDS matrices with XOR counts.

1.1 Related Works

1.1.1 Matrix Polynomial

Recently, many papers constructed lightweight MDS matrices with entries being matrix polynomials generated by a fixed binary matrix. However, to the best of our knowledge, their entries are chosen from a matrix representation of $GF(2^m)$, where $GF(2^m)$ denotes the finite field $\mathbb{F}_{2^8}$. For instance, $f(x) \in \mathbb{F}_2[x]$ and $f(x)$ is an irreducible polynomial of degree m. If T is a binary matrix satisfying $f(T) = 0$, then $\mathbb{F}_2[T] \cong \mathbb{F}_2[x]/(f(x)) \cong GF(2^m)$. Therefore, $\mathbb{F}_2[T]$ is a matrix representation of the finite field $GF(2^m)$ and any element of $\mathbb{F}_2[T]$ can be represented as a matrix polynomial like $t_{m-1}T^{m-1} + t_{m-2}T^{m-2} + ... + t_0 I$, where $t_i = 1$ or 0 $(i = 0, 1, ..., m-1)$.

At FSE 2015, Sim et al. [25] constructed lightweight non-involutory or involutory $n \times n$ (n=4, 8, 16 or 32) MDS matrices over $GF(2^m)$ (m=4 or 8) such as Hadamard matrix, Hadamard-Chauchy matrix, Subfield-Hadamard matrix and Compact Chauchy matrix. At CRYPTO 2016, Beierle et al. [11] took the advantage of the multiplication of special element to devise lightweight Circulant MDS matrices over $GF(2^m)$. Nakahara et al. [24] and Gupta et al. [12] investigated lightweight Circulant MDS matrices and proved that Circulant involutory MDS matrices do not exist over $GF(2^m)$. At IACR Transactions on Symmetric Cryptology 2016, Sarkar et al. [27] showed that Toeplitz matrix cannot be both involutory and MDS and investigated the lower bounds of XOR counts of 4×4 MDS matrices over $GF(2^4)$ and $GF(2^8)$. At S&P 2017, Sarkar et al. [28] further presented characterizations of Toeplitz matrices in light of MDS property and improved the lower bounds of XOR counts of 8×8 MDS matrices by obtaining Toeplitz MDS matrices with lower XOR counts over $GF(2^4)$ and $GF(2^8)$.

1.1.2 $GL(m, \mathbb{F}_2)$

Recently, many new MDS matrices with few XORs were researched over $GL(m, \mathbb{F}_2)$, where $GL(m, \mathbb{F}_2)$ denotes the set of all $m \times m$ non-singular matrices with entries in $\mathbb{F}_2$. At FSE 2016, Li et al. [22] constructed many new 4×4 MDS matrices over $GL(m, \mathbb{F}_2)$ and successfully presented involutory Circulant MDS matrices over $GL(m, \mathbb{F}_2)$ though it has been proved that the involutory Circulant MDS matrix does not exist over the finite field. Specifically, they constructed Circulant matrices, involutory Circulant matrices, Hadamard matrices and involutory Hadamard matrices over $GL(4, \mathbb{F}_2)$ and $GL(8, \mathbb{F}_2)$. Moreover, Bai

et al. [23] constructed 4×4 MDS matrices over $GL(4, \mathbb{F}_2)$ with 10 XORs by utilizing some special matrix structures, where non-identity entries are repeated or achieved by other non-identity entries. At S&P 2017, Zhang et al. [31] constructed the lightest 4×4 Circulant MDS matrices over $GL(4, \mathbb{F}_2)$ with 12 XORs by investigating the characteristics of permutation group.

A fact must be pointed that the optimal results can be definitely constructed over $GL(m, \mathbb{F}_2)$. However, when m is greater than or equal to 8 and non-identity entries of MDS matrices are not repeated, the search space is extremely large. Therefore, the construction of lightweight MDS matrices cannot be completed in an acceptable time.

1.1.3 Motivations

To achieve MDS matrices with the least XOR counts, the matrix representation of $GF(2^m)$ and $GL(m, \mathbb{F}_2)$ face some limitations as follows:

- For the matrix representation of $GF(2^m)$, the search space is too small to find MDS matrices with the least XOR counts when m is greater than or equal to 8. For instance, when constructing 4×4 circulant MDS matrices $Circ(I, I, A, B)$ over $GF(2^8)$, the search space is about 6.553×10^4. Moreover, when $m = 8$, there is no matrix with 1 XOR in the matrix representation of $GF(2^8)$.

- For $GL(m, \mathbb{F}_2)$, the search space is too large to complete the constructions of MDS matrices in an acceptable time when m is greater than or equal to 8. For instance, when constructing 4×4 circulant MDS matrices $Circ(I, I, A, B)$ over $GL(8, \mathbb{F}_2)$, the search space is about 1.099×10^{12}.

- While, for matrix polynomial residue rings, the search space is suited. For instance, when constructing 4×4 circulant MDS matrices $Circ(I, I, A, B)$ over the matrix polynomial residue rings generated by 8×8 binary non-singular matrices with 1 XOR, the search space is about 4.516×10^6. Additionally, in the search space, there are lots of entries with 1 XOR.

In this paper, we find a trade-off between search space and XOR counts. Specifically, MDS matrices with as few XORs as possible are efficiently constructed over the matrix polynomial residue ring.

1.2 Contributions

In this paper, we focus on constructing MDS matrices with as few XOR counts as possible. The platform for running algorithms is specified as follows: Intel i5-5300 CPU with 2.30GHz, 4GB memory, Windows 10 OS. Moreover, the programming language is the C language. We investigate the feasibilities of building MDS matrices over the matrix polynomial residue ring. Our contributions are summarized as follows:

- We analyze the distribution of the minimal polynomials of $m \times m (m = 4 \text{ or } 8)$ non-singular binary matrices with 1 XOR as well as the distribution of elements with few XORs in $m \times m$ matrix polynomial residue rings. By using such distributions, we can significantly optimize the search space of constructions.

- To construct MDS matrices with as few XORs as possible, an efficient algorithm is presented. Results are summarized as follows:

  (1) In case of entries being 4×4 binary matrices, 288 MDS matrices of order 4 with 10 XORs are built within 2 minutes.

  (2) In case of entries being 8×8 binary matrices, 40320 MDS matrices of order 4 with 10 XORs are built within 2 minutes.

(3) In case of entries being 16×16 binary matrices, an MDS matrix of order 4 with 10 XORs is constructed within 1 minute.

- We extend some results about the involutory MDS matrix as follows:

  (1) We propose three theorems regarding the existences of involutory MDS matrices.

  (2) We propose an efficient necessary-and-sufficient condition for identifying a Hadamard matrix being involutory. By incorporating the proposed condition, another efficient algorithm for constructing involutory Hadamard MDS matrices with few XORs is proposed. Comparing with 1 day consumed by [22] to construct 80640 involutory Hadamard matrices with 40 XORs, the presented algorithm only costs about 1 minute to construct 80640 involutory Hadamard matrices with 20 XORs.

- We analyze the search space of our constructions comparing with constructions over $GL(m, \mathbb{F}_2)$.

Roadmap. In Sec.1, necessary preliminaries are presented. Sec.2 proposes five kinds of structure-matrix and then investigates the distribution of the minimal polynomial and distribution of elements with fewer XORs on matrix polynomial residue rings. Sec.3 presents the design of an algorithm for constructing lightweight non-involutory MDS matrices and analyzes the search space. Sec.4 discusses the involutory MDS matrix and constructs involutory Hadamard MDS matrices. Finally, a short conclusion is given in Sect. 5.

2 Preliminaries

In this section, we present some basic definitions and theorems.

2.1 MDS Matrices

Let R be a ring with identity, m be a positive integer and $x \in R^m$. The *Hammnig weight* of x is defined as the number of nonzero entries of x and is expressed by $\omega(x)$. Let M be an $n \times n$ matrix over R. The *branch number* of M is the minimum number of nonzero components in the input vector v and output vector $u = Mv$ as we search for all nonzero $v \in R^n$, i.e. the branch number of M is $B_M = \min_{v \neq 0}\{\omega(v) + \omega(Mv)\}$, and $B_M \leq n + 1$. A *maximum distance separable* (MDS) $n \times n$ matrix has the maximum branch number n+1. $GL(m, \mathbb{F}_2)$ denotes the set of all non-singular $m \times m$ binary matrices.

A linear diffusion layer is a linear map and can be represented by a matrix as follows:

$$L = \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ L_{2,1} & L_{2,2} & \cdots & L_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ L_{n,1} & L_{n,2} & \cdots & L_{n,n} \end{pmatrix},$$

where $L_{i,j}$ $(1 \leq i, j \leq n)$ is an $m \times m$ binary matrix. In the present paper, the whole matrix like above L is called the *structure-matrix* and the entry like above $L_{i,j}$ is called the *element-matrix*. $M(n, m)$ denotes all $n \times n$ matrices over $GL(m, \mathbb{F}_2)$. We investigate MDS matrices from $M(n, m)$ where n=4 and m=4, 8 or 16. For $X = (x_1, x_2, ..., x_n)^T \in (\mathbb{F}_2^m)^n$,

$$L(X) = \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ L_{2,1} & L_{2,2} & \cdots & L_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ L_{n,1} & L_{n,2} & \cdots & L_{n,n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{n} L_{1,i}(x_i) \\ \sum_{i=1}^{n} L_{2,i}(x_i) \\ \vdots \\ \sum_{i=1}^{n} L_{n,i}(x_i) \end{pmatrix},$$

where $L_{i,j}(x_k) = L_{i,j} \cdot x_k$, for $1 \leq i, j \leq n, 1 \leq k \leq n$.

Theorem 1. *[22] Let L be a matrix, then L is MDS if and only if all square sub-matrices of L are of full rank.*

2.2 XOR Count

Let $a, b \in \mathbb{F}_2$. $a+b$ is called a bit XOR operation. Let $A \in GL(m, \mathbb{F}_2)$, $x = (x_1, x_2, ..., x_m)^T \in \mathbb{F}_2^m$. $\#A$ is called the XOR count[20] of A that denotes the number of XOR operations required to evaluate Ax directly. Let $\omega(A)$ be the number of 1's in A, then $\#A = \omega(A) - m$. For $L \in M(n, m)$, $\#(L)$ denotes *the sum of XOR counts* of L and $\#(L) = \sum_{i,j=1}^{n} \#(L_{ij})$. For instance, let $x = (a, b, c, d)^T \in \mathbb{F}_2^4$, and the XOR counts of the following matrix is 4.

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

$$Ax = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} d \\ c+d \\ b+c+d \\ a+c \end{pmatrix}.$$

For $A \in GL(m, \mathbb{F}_2)$, a simplified representation of A is given by extracting the non-zero positions in each row of A. For example, [3,2,4,[1,3]] is the representation of the following matrix.

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

2.3 Matrix Polynomial Residue Ring

$(f(x))$ denotes the *ideal* generated by the polynomial $f(x)$. Let T be an $n \times n$ binary matrix, and $f(x)$ be the minimal polynomial of T. The degree of $f(x)$ be k, $k \leq n$. Therefore, $\mathbb{F}_2[T] \cong \mathbb{F}_2[x]/(f(x))$ since T satisfies $f(T) = 0$, where $\mathbb{F}_2[T]$ denotes the matrix polynomial residue ring generated by T. Therefore, the matrix computations in $\mathbb{F}_2[T]$ are equivalent to polynomial computations in $\mathbb{F}_2[x]/(f(x))$.

For instance, let $B, C \in \mathbb{F}_2[T]$,

$$\begin{aligned} B &= b_{k-1}T^{k-1} + \cdots + b_1 T + b_0 I, \\ C &= c_{k-1}T^{k-1} + \cdots + c_1 T + c_0 I, \\ b(x) &= b_{k-1}x^{k-1} + \cdots + b_1 x + b_0, \\ c(x) &= c_{k-1}x^{k-1} + \cdots + c_1 x + c_0. \end{aligned}$$

Then, $B + C = b(x) + c(x)|_{x=T}$, $BC = b(x)c(x)|_{x=T}$.

3 Structure-matrices and element-matrices

The underlying section firstly introduces five kinds of structure-matrix that are suitable to construct MDS matrices with the least sum of XOR counts. Secondly, we discuss how to choose element-matrices by analyzing the distribution of the minimal polynomials of $m \times m$ ($m = 4$ or 8) non-singular binary matrices with 1 XOR and the distribution of element-matrices with few XORs in $m \times m$ matrix polynomial residue rings.

3.1 Five Kinds of Structure-matrix

Let $L_1, L_2 \in M(n,m)$. If L_1 can be transformed to L_2 by exchanging rows or columns, then we define that L_1 is equivalent to L_2 since L_1 has the same sum of XOR counts as L_2. If a matrix has more identity binary matrices being entries, then the matrix may has less sum of XOR counts since an identity binary matrix has 0 XOR count. Additionally, in an MDS matrix, any 2×2 sub-matrix could not be $\begin{pmatrix} I & I \\ I & I \end{pmatrix}$, otherwise the matrix is not MDS.

In our algorithms, we only use five kinds of structure-matrix as follows:

$$S_1 = \begin{pmatrix} & I & I & I \\ I & I & & \\ I & & I & \\ I & & & I \end{pmatrix}, S_2 = \begin{pmatrix} & I & I & I \\ I & I & & \\ I & & I & \\ & & & I \end{pmatrix}, S_3 = \begin{pmatrix} & I & I & I \\ I & I & & \\ I & & I & \\ & & I & \end{pmatrix},$$

$$S_4 = \begin{pmatrix} & I & I & I \\ I & I & & \\ I & & I & \\ I & & & \end{pmatrix}, S_5 = \begin{pmatrix} I & I & & \\ & I & I & \\ & & I & I \\ I & & & I \end{pmatrix},$$

where I is the identity binary matrix and the remaining entries can be any other non-singular binary matrices.

According to [19], there exist at most $3(n-1)$ identity matrices being entries in an $n \times n$ MDS matrix. The type of matrix is called the *Optimal matrix* and it is the same as the aforementioned structure-matrix S_1. For example, the following matrix is an Optimal matrix.

$$\begin{pmatrix} A_{1,1} & I & I & \cdots & I \\ I & I & A_{2,3} & \cdots & A_{2,n} \\ I & A_{3,2} & I & \cdots & A_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ I & A_{n,2} & A_{n,3} & \cdots & I \end{pmatrix}$$

In previous papers, *Circulant matrix, Hadamard matrix and Optimal matrix* are usually used to construct lightweight MDS matrices. Such matrices are presented as follows:

$$Circ(I,I,A,B) = \begin{pmatrix} I & I & A & B \\ B & I & I & A \\ A & B & I & I \\ I & A & B & I \end{pmatrix}, Had(I,A,B,C) = \begin{pmatrix} I & A & B & C \\ A & I & C & B \\ B & C & I & A \\ C & B & A & I \end{pmatrix},$$

$$Special\ Optimal\ Matrix = \begin{pmatrix} A & I & I & I \\ I & I & A & B \\ I & B & I & A \\ I & A & B & I \end{pmatrix}.$$

It may be noted that the $Circ(I,I,A,B)$ and the *Special Optimal Matrix* are special cases of S_5 and S_1, respectively.

3.2 Element-matrices

In the present paper, element-matrices (entries) of MDS matrices are chosen from matrix polynomial residue rings. The underlying subsection introduces how we choose generator matrices of matrix polynomial residue rings. Furthermore, we analyze elements with few XORs of matrix polynomial residue rings.

3.2.1 Generator Matrix of Matrix Polynomial Residue Ring

Let T be a non-singular $m \times m$ binary matrix with 1 XOR. $f(x)$ is the minimal polynomial of T. Then, $\mathbb{F}_2[T]$ is a matrix polynomial residue ring generated by T and $\mathbb{F}_2[T]$ is isomorphic to $\mathbb{F}_2[x]/(f(x))$. Let S' be one of five structure-matrices mentioned at Sec.2.1. When we want to construct MDS matrices with as few XORs as possible by utilizing S' over $\mathbb{F}_2[T]$, there may be as many T as possible to be non-identify element-matrices. In the structure-matrix S', if S' has at least 2 Ts, then there must exist a sub-matrix like $\begin{pmatrix} I & I \\ I & T \end{pmatrix}$. According to the requirement of MDS, the sub-matrix should be of full rank. The full rank denotes that the sub-matrix's rank is $2m$. Therefore, $I + T$ should be non-singular. Consequently, T should satisfy: (i) $\#(T) = 1$; (ii) T and $I + T$ are non-singular. The detail of searching for all T will be described in *Algorithm* 1.

3.2.2 Analyzing Matrix Polynomial Residue Ring

First, we analyze minimal polynomials of 4×4 non-singular binary matrices with 1 XOR and element-matrices with few XORs in 4×4 matrix polynomial residue rings. Specifically, we search for every T satisfying $T \in GL(4, \mathbb{F}_2)$, $\#T$=1 and $I + T$ is non-singular. The number of T is 72. Let $f(x)$ be the minimal polynomial of T, $b(x) \in \mathbb{F}_2[x]/(f(x))$. We search for all $b(x)$ satisfying $1 \leq \#b(T) \leq 3$. Results are presented as follows:

1. Search results of $f(x)$: $x^4 + x + 1,\ x^4 + x^2 + 1,\ x^4 + x^3 + 1$.
2. Search results of $b(x)$ satisfying $\#b(T)$=1: $x,\ x^3 + 1,\ x^3 + x,\ x^3 + x^2$.
3. Search results of $b(x)$ satisfying $\#b(T)$=2: $x^2,\ x^2 + 1,\ x^2 + x,\ x^3$.
4. Search results of $b(x)$ satisfying $\#b(T)$=3: $x + 1,\ x^2,\ x^3,\ x^3 + x^2 + 1$.

Let $g(x)$ be one of $x^4 + x + 1,\ x^4 + x^2 + 1$ and $x^4 + x^3 + 1$. We discover that there are exactly 24 non-singular 4×4 binary matrices with 1 XOR count whose minimal polynomial is $g(x)$. The distributions of matrix polynomials with 1,2 or 3 XOR counts are described in Table 1. Table 1 is a statistical result by searching all elements on $GL(4, \mathbb{F}_2)$.

Table 1: Matrix polynomials on the 4×4 binary matrix polynomial residue rings

Condition	$f(x)$	Number of T	$f(x)$	Number of T
$\#f(T)$=1	x	72	$x^3 + 1$	24
	$x^3 + x$	24	$x^3 + x^2$	24
$\#f(T)$=2	x^2	48	$x^2 + 1$	24
	$x^2 + x$	24	x^3	24
$\#f(T)$=3	$x + 1$	24	x^2	24
	x^3	24	$x^3 + x^2 + 1$	24

T is the 4×4 binary matrix. T and $I + T$ are non-singular and $\#(T) = 1$.

Second, we analyze minimal polynomials of 8×8 non-singular binary matrices with 1 XOR and element-matrices with few XORs in 8×8 matrix polynomial residue rings. Specifically, we search for all matrix T satisfying $T \in GL(8, \mathbb{F}_2)$, $\#T$=1 and $I + T$ is non-singular. The number of T is 282240. Let $f(x)$ be the minimal polynomial of T, $b(x) \in \mathbb{F}_2[x]/(f(x))$. We search for every T to find every $f(x)$ and all $b(x)$ satisfying $1 \leq \#b(T) \leq 3$. Search results are as follows:

1. Search results of $f(x)$ satisfying $f(T) = 0$:

$$x^8 + x + 1, x^8 + x^2 + 1, x^8 + x^3 + 1, x^8 + x^4 + 1, x^8 + x^5 + 1, x^8 + x^6 + 1, x^8 + x^7 + 1.$$

2. Search results of $b(x)$ satisfying $\#b(T)$=1:

$$x, x^7+1, x^7+x, x^7+x^2, x^7+x^3, x^7+x^4, x^7+x^5.$$

3. Search results of $b(x)$ satisfying $\#b(T)$=2:

$$x^2, x^6+1, x^6+x, x^6+x^2, x^6+x^3, x^6+x^4, x^6+x^5.$$

4. Search results of $b(x)$ satisfying $\#b(T)$=3:

$$x^2, x^3, x^5+1, x^5+x, x^5+x^2, x^5+x^3, x^5+x^4, x^7+x^6+1.$$

Let $g(x)$ be one of x^8+x+1, x^8+x^2+1, x^8+x^3+1, x^8+x^4+1, x^8+x^5+1, x^8+x^6+1 and x^8+x^7+1. We discover that there are exactly 40320 non-singular 8×8 binary matrices with 1 XOR count whose minimal polynomial is $g(x)$. The distributions of matrix polynomials with 1,2 or 3 XOR counts are described in Table 2. Table 2 is a statistical result by searching all elements on $GL(8,\mathbb{F}_2)$.

Table 2: Matrix polynomials on the 8×8 binary matrix polynomial residue rings

Condition	$f(x)$	Number of T	$f(x)$	Number of T
$\#f(T)$=1	x	282240	x^7+1	40320
	x^7+x	40320	x^7+x^2	40320
	x^7+x^3	40320	x^7+x^4	40320
	x^7+x^5	40320	x^7+x^6	40320
$\#f(T)$=2	x^2	241920	x^6+1	40320
	x^6+x	40320	x^6+x^2	40320
	x^6+x^3	40320	x^6+x^4	40320
	x^6+x^5	40320		
$\#f(T)$=3	x^2	40320	x^3	201600
	x^5+1	40320	x^5+x	40320
	x^5+x^2	40320	x^5+x^3	40320
	x^5+x^4	40320	x^7+x^6+1	40320

T is the 8×8 binary matrix. T and $I+T$ are non-singular and $\#(T)=1$.

4 Lightweight MDS Matrices

In this section, we present an efficient algorithm for constructing lightweight MDS matrices.

4.1 Entries Expression

Entries of MDS matrices are chosen from the $m\times m$ matrix polynomial residue ring, m=4, 8 or 16. For instance, the Special Optimal matrix

$$Special\ Optimal\ Matrix = \begin{pmatrix} A & I & I & I \\ I & I & A & B \\ I & B & I & A \\ I & A & B & I \end{pmatrix}.$$

Let T be a non-singular binary matrix with 1 XOR. $f(x)$ is the minimal polynomial of T. $A, B \in \mathbb{F}_2[T]$, $a(T)=A$, $b(T)=B$, where $a(x), b(x) \in \mathbb{F}_2[x]/(f(x))$. Therefore, in our

construction, the Special Optimal matrix can be replaced as the following matrix:

$$\begin{pmatrix} a(x) & 1 & 1 & 1 \\ 1 & 1 & a(x) & b(x) \\ 1 & b(x) & 1 & a(x) \\ 1 & a(x) & b(x) & 1 \end{pmatrix}.$$

4.2 Identifying MDS matrices

In this subsection, we investigate the method for identifying an MDS matrix from our construction algorithms.

4.2.1 Necessary and sufficient condition of MDS

According to Theorem 1, $L \in M(n, m)$, L is MDS if and only if all square sub-matrices of L are full rank. That a sub-matrix is full rank is equivalent to that the corresponding sub-determinant is non-singular since entries of the sub-matrix are $m \times m$ binary matrices. Therefore, a necessary-and-sufficient condition for a matrix being MDS can be described as follows:

Theorem 2. *[22] Let $L=(L_{i,j})$, $1 \leq i, j \leq n$, and the entries of L are $m \times m$ matrices over $\mathbb{F}_2$. Then L is an MDS matrix if and only if all square sub-matrices of L of order t are of full rank for $1 \leq t \leq n$.*

4.2.2 Identifying MDS matrices

According to Theorem 2, identifying MDS matrices needs to calculate all sub-determinants of the candidate matrix. On the one hand, determinants can be calculated efficiently over the polynomial residue ring. On the other hand, matrix polynomial residue ring is isomorphic to polynomial residue ring. Therefore, identifying MDS matrices over matrix polynomial residue ring is efficient. For instance, because entries are expressed as polynomials in the presented algorithms, so a candidate matrix can be expressed as follows:

$$\begin{pmatrix} x & 1 & 1 & 1 \\ 1 & 1 & x & x^2+1 \\ 1 & x^2+1 & 1 & x \\ 1 & x & x^2+1 & 1 \end{pmatrix}.$$

Sub-determinants are calculated with *the complete expansion of determinant*. Therefore, a sub-determinant of order 3 can be calculated as follows:

$$\begin{vmatrix} x & 1 & 1 \\ 1 & 1 & x \\ 1 & x^2+1 & 1 \end{vmatrix} = x + x + (x^2+1) + 1 + (x^4+x^2) + 1 = x^4 + 1.$$

Then, let T be substituted into $x^4 + 1$ to get $T^4 + I$.

Finally, this sub-matrix is full rank if and only if $T^4 + I$ is non-singular. $T^4 + I$ is non-singular if and only if $x^4 + 1$ is relatively prime to $f(x)$, where $f(x)$ is the minimal polynomial of T. Therefore, identifying MDS matrices over matrix polynomial residue ring is more efficient than identifying over $GL(m, \mathbb{F}_2)$.

4.3 Algorithm for Constructing Lightweight MDS matrices

To construct lightweight 4×4 MDS matrices over the $m \times m (m = 4, 8 \text{ or } 16)$ matrix polynomial residue ring, Algorithm 1 is presented below. S_i is the structure-matrix of MDS

Algorithm 1 Construction of lightweight MDS matrices

for Search for every permutation $\{a_1, a_2, ..., a_m\}$ of $\{1, 2, ..., m\}$. **do**
  for i from 1 to m **do**
    for j from 1 to m and $j \neq a_i$ **do**
      Construct the binary matrix T=$[a_1, \ldots, [a_i, j], \ldots, a_m]$. Therefore, T is a non-singular binary matrix with 1 XOR.
      Find the minimal polynomial of T.
      Find polynomials $b_1(x), \cdots, b_k(x)$ satisfying $\#b(T) \leq 3$.
      for t from 1 to 5 **do**
        for In S_t, each entry, which is not 1, comes from $\{b_1(x), \cdots, b_k(x)\}$ **do**
          if This matrix is MDS **then**
            Record the MDS matrix and its sum of XORs.
          end if
        end for
      end for
    end for
  end for
end for

matrices discussed in Sec.3.1. In each following experiments, we construct corresponding results by exhaustive search on corresponding matrix polynomial residue rings.

The platform for running Algorithm 1 is specified as follows: Intel i5-5300 CPU with 2.30GHz, 4GB memory, Windows 10 OS. The programming language is the C language. By running Algorithm 1, we get the following results:

1. Over 4×4 matrix polynomial residue ring, it takes less than 2 minutes to identify 288 MDS matrices within the form of S_1 which have only 10 XORs. Moreover, it takes about 13 minutes to verify that there does not exist MDS matrices with 10 XORs in S_2, S_3, S_4 or S_5. An example is presented as follows: Among all the matrices with the form S_2, S_3, S_4 and S_5, it takes about 13 minutes to verify that there does not exist an MDS matrix which has only 10 XORs.

   Example 1. Let $T = [[1, 2], 3, 4, 1]$ be a 4×4 binary matrix. The following matrix is an MDS matrix with 10 XORs.

$$\begin{pmatrix} T^2+T & I & I & I \\ I & I & T & T^2+T \\ I & T^2+T & I & T^3+T^2 \\ I & T & T^3+T^2 & I \end{pmatrix}$$

2. Over 8×8 matrix polynomial residue ring, it costs only 1 minute 16 seconds to construct 40320 MDS matrices with 10 XORs. An example is presented as follows:

   Example 2. Let $T = [[2, 4], 3, 4, 5, 6, 7, 8, 1]$ be a 8×8 binary matrix. The following matrix is an MDS matrix with 10 XORs.

$$\begin{pmatrix} T^2 & I & I & I \\ I & I & T & T^2 \\ I & T & I & T^7+T \\ I & T^7+T & T^2 & I \end{pmatrix}$$

3. Over 16×16 matrix polynomial residue ring, it costs about 1 minute to construct Circulant MDS matrix with 12 XORs and Optimal MDS matrix with 10 XORs. Let $T \in GL(16, \mathbb{F}_2)$ and $T = [[1, 2], 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 1]$. The minimal polynomial of T is $x^{16} + x^{15} + 1$. Two examples are presented below:

Example 3. Let L_1 be a Circulant MDS matrix with 12 XORs.

$$L_1 = \begin{pmatrix} I & I & T & T^{14}+T^{13} \\ T^{14}+T^{13} & I & I & T \\ T & T^{14}+T^{13} & I & I \\ I & T & T^{14}+T^{13} & I \end{pmatrix}$$

Example 4. Let L_2 be an Optimal MDS matrix with 10 XORs.

$$L_2 = \begin{pmatrix} T & I & I & I \\ I & I & T & T^{14}+T^{13} \\ I & T^{14}+T^{13} & I & T \\ I & T & T^{14}+T^{13} & I \end{pmatrix}$$

Details of constructions of Algorithm 1 are shown in Table 3. Moreover, comparisons with major previous constructions of lightweight MDS matrices are described in Table 4.

Table 3: Number of lightweight MDS matrices and running time

Matrix type	Element	Sum of XORs	Number	Running time
$Circ(I, I, A, B)$	$\mathbb{F}_2[T_{4\times4}]$	12	96	00:00:01
$Had(I, A, B, C)$	$\mathbb{F}_2[T_{4\times4}]$	20	288	00:00:04
Special Optimal	$\mathbb{F}_2[T_{4\times4}]$	13	48	00:00:01
S_1	$\mathbb{F}_2[T_{4\times4}]$	10	288	00:01:42
S_3	$\mathbb{F}_2[T_{4\times4}]$	10	48	00:05:05
$Circ(I, I, A, B)$	$\mathbb{F}_2[T_{8\times8}]$	12	96	00:01:27
$Had(I, A, B, C)$	$\mathbb{F}_2[T_{8\times8}]$	20	241920	00:07:00
Special Optimal	$\mathbb{F}_2[T_{8\times8}]$	10	40320	00:01:16
S_1	$\mathbb{F}_2[T_{8\times8}]$	10	1128960	14:00:00
$Circ(I, I, A, B)$	$\mathbb{F}_2[T_{16\times16}]$	12	1	00:00:30
Special Optimal	$\mathbb{F}_2[T_{16\times16}]$	10	1	00:00:30

In previous constructions, lightweight MDS matrices are usually constructed with structure-matrices such as Circulant matrix, Hadamard matrix, Special Optimal matrix etc. [11, 23, 21, 22]. In these structure-matrices, non-identity entries are repeated like the following structure-matrix:

$$Cir(I, I, A, B) = \begin{pmatrix} I & I & A & B \\ B & I & I & A \\ A & B & I & I \\ I & A & B & I \end{pmatrix}.$$

By exhaustive search on $GL(8, \mathbb{F}_2)$, we discover that there are 1048320 matrices with no more than 3 XORs. Therefore, if A, $B \in GL(8, \mathbb{F}_2)$, $1 \leq \#A \leq 3$ and $1 \leq \#B \leq 3$, then the search space of $Cir(I, I, A, B)$ is $1048320 \times 1048320 \approx 1.099 \times 10^{12}$. However, by searching on $GL(8, \mathbb{F}_2)$, we discover that if $\#T = 1$ and $T + I$ is non-singular, then the number of T is 282240. Moreover, there are at most 4 elements with 1 or 2 XORs in each $\mathbb{F}_2[T]$. Consequently, the search space of $Cir(I, I, A, B)$ is only $282240 \times 4 \times 4 \approx 4.516 \times 10^6$.

If non-identity entries are chosen from $GL(8, \mathbb{F}_2)$ and are not repeated, then the search space of construction is too large that the construction cannot be completed in an acceptable time. For instance, the following matrix is the structure-matrix S_5.

$$S_5 = \begin{pmatrix} I & I & A_1 & A_2 \\ A_3 & I & I & A_4 \\ A_5 & A_6 & I & I \\ I & A_7 & A_8 & I \end{pmatrix}.$$

- Over $GL(8, \mathbb{F}_2)$, the search space of S_5 is $1048320^8 \approx 1.458 \times 10^{48}$.
- Over 8×8 binary matrix polynomial residue rings, the search space of S_5 is $282240 \times 4^8 \approx 1.849 \times 10^{10}$.

Table 4: Comparisons with previous constructions of MDS matrices

Matrix type	Elements	Sum of XORs	Ref.
$Had(I, A, B, C)$	$GL(4, \mathbb{F}_2)$	16	[22]
$Special\ Optimal$	$GL(4, \mathbb{F}_2)$	13	[22]
$Circ(I, I, A, B)$	$GL(4, \mathbb{F}_2)$	12	[22]
$Had(\texttt{0x1}, \texttt{0x2}, \texttt{0x8}, \texttt{0x9})$	$\mathbb{F}_{2^4}/\texttt{0x13}$	20	[25]
$Circ(\texttt{0x1}, \texttt{0x1}, \texttt{0x9}, \texttt{0x4})$	$\mathbb{F}_{2^4}/\texttt{0x13}$	12	[21]
$Circulant$	$\mathbb{F}_{2^4}$	12	[11]
$Special\ Structure - matrix$	$GL(4, \mathbb{F}_2)$	10	[23]
$Toeplizt$	$\mathbb{F}_{2^4}/\texttt{0x19}$	10	[27]
$Had(I, A, B, C)$	$\mathbb{F}_2[T_{4\times4}]$	20	Ours
$Special\ Optimal$	$\mathbb{F}_2[T_{4\times4}]$	13	Ours
$Circ(I, I, A, B)$	$\mathbb{F}_2[T_{4\times4}]$	12	Ours
S_1	$\mathbb{F}_2[T_{4\times4}]$	10	Ours
$Circ(I, I, A, B)$	$GL(8, \mathbb{F}_2)$	12	[22]
$Had(I, A, A^T, B)$	$GL(8, \mathbb{F}_2)$	20	[22]
$Special\ Optimal$	$GL(8, \mathbb{F}_2)$	10	[22]
$Had(\texttt{0x01}, \texttt{0x02}, \texttt{0x04}, \texttt{0x91})$	$\mathbb{F}_{2^8}/\texttt{0x1c3}$	52	[25]
$Subfield - Had(\texttt{0x1}, \texttt{0x2}, \texttt{0x8}, \texttt{0x9})$	$\mathbb{F}_{2^4}/\texttt{0x13}$	40	[25]
$Circ(\texttt{0x02}, \texttt{0x03}, \texttt{0x01}, \texttt{0x01})$	$\mathbb{F}_{2^8}/\texttt{0x11b}$	56	[14]
$Circ(\texttt{0x1}, \texttt{0x1}, \texttt{0x2}, \texttt{0x91})$	$\mathbb{F}_{2^8}/\texttt{0x1c3}$	24	[21]
$Circulant$	$\mathbb{F}_{2^8}$	24	[11]
$Toeplizt$	$\mathbb{F}_{2^8}/\texttt{0x1c3}$	27	[27]
$Circ(I, I, A, B)$	$\mathbb{F}_2[T_{8\times8}]$	12	Ours
$Had(I, A, B, C)$	$\mathbb{F}_2[T_{8\times8}]$	20	Ours
$Special\ Optimal$	$\mathbb{F}_2[T_{8\times8}]$	10	Ours
S_1	$F_2[T_{8\times8}]$	10	Ours
$Circ(I, I, A, B)$	$\mathbb{F}_2[T_{16\times16}]$	12	Ours
$Special\ Optimal$	$\mathbb{F}_2[T_{16\times16}]$	10	Ours

5 Lightweight Involutory MDS Matrices

If a matrix A is ivolutory, then it means that $A^2 = I$. In other word, the inverse of A is A itself. The involutory matrix is suited to be used in design of symmetric cryptography. The underlying section first investigates the existence of some types of involutory MDS matrix. Then, we present an efficient necessary-and-sufficient condition for identifying an involutory Hadamard matrix. Finally, with this condition, we propose an extremely efficient algorithm for constructing lightweight involutory Hadamard MDS matrices.

5.1 Existence of Involutory MDS Matrices

Theorem 3. *Let L be an $n \times n (n \geq 2)$ MDS matrix over $GL(m, \mathbb{F}_2)$ as the following matrix where entries of i-th row and entries of i-th column are identity matrices except $A_{i,i}$. If L is involutory, then the number of identity matrices of L is less than $2n - 1$.*

$$L = \begin{pmatrix} A_{1,1} & \cdots & A_{1,i-1} & I & A_{1,i+1} & \cdots & A_{1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_{i-1,1} & \cdots & A_{i-1,i-1} & I & A_{i-1,i+1} & \cdots & A_{i-1,n} \\ I & \cdots & I & A_{i,i} & I & \cdots & I \\ A_{i+1,1} & \cdots & A_{i+1,i-1} & I & A_{i+1,i+1} & \cdots & A_{i+1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_{n,1} & \cdots & A_{n,i-1} & I & A_{n,i+1} & \cdots & A_{n,n} \end{pmatrix}. \quad (1)$$

Proof. In this proof, we use the proof by contradiction and assume that L has greater than or equal to $2n-1$ identity matrices.

When $n = 2k$, k=1,2,3$\cdots$. As L is involutory and it is the form of Eq.1, therefore,

$$L^2 = \begin{pmatrix} * & \cdots & * & \cdots & * \\ \vdots & & \vdots & & \vdots \\ * & \cdots & A_{i,i}^2 + I & \cdots & * \\ \vdots & & \vdots & & \vdots \\ * & \cdots & * & \cdots & * \end{pmatrix} = \begin{pmatrix} I & 0 & \cdots & 0 \\ 0 & I & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & I \end{pmatrix}$$

$$\Rightarrow A_{i,i}^2 = 0 \Rightarrow A_{i,i} \textit{ is singular.}$$

Because L is MDS, thus $A_{i,i}$ is non-singular. This is a contradiction. Therefore, the assumption is wrong. Consequently, in this case, the number of identity matrices is less than $2n-1$.

When $n = 2k+1$, k=1,2,3$\cdots$. As L is ivolutory, therefore,

$$L^2 = \begin{pmatrix} * & \cdots & * & \cdots & * \\ \vdots & & \vdots & & \vdots \\ * & \cdots & A_{i,i}^2 & \cdots & * \\ \vdots & & \vdots & & \vdots \\ * & \cdots & * & \cdots & * \end{pmatrix} = \begin{pmatrix} I & 0 & \cdots & 0 \\ 0 & I & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & I \end{pmatrix} \Rightarrow A_{i,i}^2 = I$$

$$\Rightarrow A_{i,i}^2 + I = 0 \Rightarrow (A_{i,i} + I)^2 = 0 \Rightarrow A_{i,i} + I \textit{ is singular.}$$

As L is assumed to have greater than or equal to $2n-1$ identity matrices, therefore, there must exist a sub-matrix such as $\begin{pmatrix} I & I \\ I & A_{i,i} \end{pmatrix}$ in L, and it is easy to know that the sub-matrix is of full rank if and only if $A_{i,i} + I$ is non-singular. Because L is MDS, so the sub-matrix is of full rank. Therefore, $A_{i,i} + I$ is non-singular. This is a contradiction. Thus, in this case, L could not have greater than or equal to $2n-1$ identity matrces.

Consequently, the assumption is wrong. Therefore, if L is involutory, then L has less than $2n-1$ identity matrices. Moreover, the theorem is equal to prove that if L is involutory, then any $A_{p,q}$ $(1 \le p, q \le n, p \ne i, q \ne i)$ or $A_{i,i}$ is an identity matrix. □

Theorem 4. *Let L be an $n \times n$ $(n \ge 2)$ MDS matrix over $GL(m, \mathbb{F}_2)$ as the following matrix where entries of i-th row and entries of j-th column are identity matrices except $A_{i,j}$, $i \ne j$. If L is involutory, then the order of L is an even number.*

$$L = \begin{pmatrix} A_{1,1} & \cdots & A_{1,j-1} & I & A_{1,j+1} & \cdots & A_{1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_{i-1,1} & \cdots & A_{i-1,j-1} & I & A_{i-1,j+1} & \cdots & A_{i-1,n} \\ I & \cdots & I & A_{i,j} & I & \cdots & I \\ A_{i+1,1} & \cdots & A_{i+1,j-1} & I & A_{i+1,j+1} & \cdots & A_{i+1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_{n,1} & \cdots & A_{n,j-1} & I & A_{n,j+1} & \cdots & A_{n,n} \end{pmatrix}, \tag{2}$$

Proof. In this proof, we use the proof by contradiction and assume that the order of L is an odd number. That is, $n = 2k+1$, $k \ge 1$.

According to Eq. 2, $i \neq j$ and that L is involutory, we have

$$L^2 = \begin{pmatrix} * & * & * & * & * \\ * & \ddots & * & * & * \\ * & * & \ddots & * & * \\ * & I & * & \ddots & * \\ * & * & * & * & * \end{pmatrix}, \tag{3}$$

where I is at the ith row and the jth column.

Due to that L is involutory, therefore,

$$L^2 = \begin{pmatrix} I & 0 & \cdots & 0 \\ 0 & I & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & I \end{pmatrix} \tag{4}$$

According to Eq. 3, at ith row and jth column, the element is I. However, according to Eq. 4, at ith row and jth column, the element is 0. It is a contradiction. Consequently, the assumption is wrong. Therefore, the order of L is an even number. □

Theorem 5. *Let $T \in GL(m, \mathbb{F}_2)$, A_1, A_2, $\cdots$, $A_n \in \mathbb{F}_2[T]$. If $Circ(A_1, A_2, ..., A_n)$ is MDS, then $Circ(A_1, A_2, ..., A_n)$ is not involutory, where $n \geq 3$.*

Proof. $L = Circ(A_1, A_2, ..., A_n)$ is an MDS matrix as the following matrix, where A_1, A_2, $\cdots$, $A_n \in \mathbb{F}_2[T]$.

$$Circ(A_1, A_2, ..., A_n) = \begin{pmatrix} A_1 & A_2 & \cdots & A_n \\ A_n & A_1 & \cdots & A_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ A_2 & A_3 & \cdots & A_1 \end{pmatrix}$$

We use the proof by contradiction and assume that $Circ(A_1, A_2, ..., A_n)$ is involutory. According to such theorem and the assumption, when $n = 2k + 1$, $k = 1, 2, 3 \cdots$, then

$$L^2 = \begin{pmatrix} A_1 & \cdots & A_{k+1} & \cdots & A_{2k+1} \\ \vdots & & \vdots & & \vdots \\ * & \cdots & * & \cdots & A_{k+1} \\ \vdots & & \vdots & & \vdots \\ * & \cdots & * & \cdots & A_1 \end{pmatrix} \begin{pmatrix} A_1 & \cdots & A_{k+1} & \cdots & A_{2k+1} \\ \vdots & & \vdots & & \vdots \\ * & \cdots & * & \cdots & A_{k+1} \\ \vdots & & \vdots & & \vdots \\ * & \cdots & * & \cdots & A_1 \end{pmatrix}$$

$$= \begin{pmatrix} * & * & \cdots & A_{k+1}^2 \\ * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * \end{pmatrix} = \begin{pmatrix} I & 0 & \cdots & 0 \\ 0 & I & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & I \end{pmatrix} \Rightarrow A_{k+1}^2 = 0 \Rightarrow A_{k+1} \textit{ is singular.}$$

Because L is MDS, so A_{k+1} is non-singular. This is a contradiction. Therefore, in this case, L can not be involutory.

When $n = 2k$, $k = 2, 3, 4 \cdots$, then

$$L^2 = \begin{pmatrix} A_1 & \cdots & A_k & \cdots & A_{2k-1} & A_{2k} \\ \vdots & & \vdots & & \vdots & \vdots \\ * & \cdots & * & \cdots & A_k & A_{k+1} \\ \vdots & & \vdots & & \vdots & \vdots \\ * & \cdots & * & \cdots & A_1 & A_2 \\ * & \cdots & * & \cdots & A_{2k} & A_1 \end{pmatrix} \begin{pmatrix} A_1 & \cdots & A_k & \cdots & A_{2k-1} & A_{2k} \\ \vdots & & \vdots & & \vdots & \vdots \\ * & \cdots & * & \cdots & A_k & A_{k+1} \\ \vdots & & \vdots & & \vdots & \vdots \\ * & \cdots & * & \cdots & A_1 & A_2 \\ * & \cdots & * & \cdots & A_{2k} & A_1 \end{pmatrix}$$

$$= \begin{pmatrix} * & \cdots & A_k^2 + A_{2k}^2 & 0 \\ * & \cdots & * & * \\ \vdots & \cdots & \vdots & \vdots \\ * & \cdots & * & * \end{pmatrix} = \begin{pmatrix} I & 0 & \cdots & 0 \\ 0 & I & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & I \end{pmatrix} \Rightarrow A_k^2 + A_{2k}^2 = 0.$$

There is a 2×2 sub-matrix $\begin{pmatrix} A_k & A_{2k} \\ A_{2k} & A_k \end{pmatrix}$ in L.

$$L = \begin{pmatrix} A_1 & \cdots & A_k & \cdots & A_{2k} \\ \vdots & & \vdots & & \vdots \\ A_{k+1} & \cdots & A_{2k} & \cdots & A_k \\ \vdots & & \vdots & & \vdots \\ * & \cdots & * & \cdots & * \end{pmatrix}$$

According above discussions, $A_k^2 + A_{2k}^2 = 0$. Because L is MDS, so $\begin{vmatrix} A_k & A_{2k} \\ A_{2k} & A_k \end{vmatrix} = A_k^2 + A_{2k}^2$ is non-singular. This is a contradiction. Therefore, in this case, L can not be involutory. □

5.2 Involutory Hadamard Matrices

In this subsection, we investigate the involutory Hadamard matrix.

Theorem 6. *Let $T \in GL(m, \mathbb{F}_2)$, $f(x)$ is the minimal polynomial of T and $a_1(x)$, $a_2(x)$, $\cdots$, $a_{2^k}(x) \in \mathbb{F}_2[x]/(f(x))$. Then, $L = Had(a_1(T), a_1(T), \cdots, a_{2^k}(T))$ is involutory if and only if*

$$\sum_{i=1}^{2^k} a_i(x)^2 \equiv 1 \pmod{f(x)}$$

Proof. Because $T \in GL(m, \mathbb{F}_2)$ and $L = Had(a_1(T), a_2(T), \cdots, a_{2^k}(T))$ is involutory, so

$$L^2 = \begin{pmatrix} \sum_{i=1}^{2^k}(a_i(T))^2 & & & \\ & \sum_{i=1}^{2^k}(a_i(T))^2 & & \\ & & \ddots & \\ & & & \sum_{i=1}^{2^k}(a_i(T))^2 \end{pmatrix} = \begin{pmatrix} I & & & \\ & I & & \\ & & \ddots & \\ & & & I \end{pmatrix}$$

$$\Leftrightarrow \sum_{i=1}^{2^k}(a_i(x))^2 \equiv (\sum_{i=1}^{2^k} a_i(x))^2 \equiv 1 \pmod{f(x)}$$

□

Corollary 1. *Let $T \in GL(m, \mathbb{F}_2)$, $f(x)$ is the minimal polynomial of T and $a(x)$, $b(x)$ and $c(x) \in \mathbb{F}_2[x]/(f(x))$. $L = Had(I, a(T), b(T), c(T))$ is involutory if and only if*

$$(a(x) + b(x) + c(x))^2 \equiv 0 \pmod{f(x)}$$

Proof. According to Theorem 6, $Had(I, a(T), b(T), c(T))$ is involutory if and only if

$$(1 + a(x) + b(x) + c(x))^2 \equiv 1 \pmod{f(x)}.$$

$$(1 + a(x) + b(x) + c(x))^2 \equiv 1 \pmod{f(x)} \Leftrightarrow (a(x) + b(x) + c(x))^2 \equiv 0 \pmod{f(x)}.$$

□

We construct lightweight involutory Hadamard MDS matrices as $Had(I, A, B, C)$. In our experiments, $A \in GL(8, \mathbb{F}_2)$, $\#A$=1, $A + I$ is non-singular. $f(x)$ is the minimal polynomial of A. $b(x)$, $c(x) \in \mathbb{F}_2[x]/(f(x))$ and $B = b(A)$, $C = c(A)$. According to Corollary 1, $Had(I, A, B, C)$ is involutory if and only if $(x + b(x) + c(x))^2 \equiv 0 \pmod{f(x)}$. So, $x^2 \equiv (b(x) + c(x))^2 \pmod{f(x)}$. As mentioned in Sec.3.2.3, the minimal polynomial of A must be one of the following polynomials:

$$x^8 + x + 1, x^8 + x^2 + 1, x^8 + x^3 + 1, x^8 + x^4 + 1, x^8 + x^5 + 1, x^8 + x^6 + 1, x^8 + x^7 + 1.$$

We find all $g(x)$ satisfying $g^2(x) \equiv x^2 \pmod{f(x)}$, where $f(x)$ is one of above minimal polynomials. For $x^8 + x + 1$, $x^8 + x^3 + 1$, $x^8 + x^5 + 1$, $x^8 + x^7 + 1$, there is only one solution x. For $x^8 + x^2 + 1$, $x^8 + x^4 + 1$, $x^8 + x^6 + 1$, there are 16 solutions.

Specifically, solutions of $g(x)$ satisfying $g^2(x) \equiv x^2 \pmod{x^8 + x^2 + 1}$ are as follows:

x	$x^4 + 1$	$x^5 + x^2$	$x^5 + x^4 + x^2 + x + 1$
$x^6 + x^3 + x^2 + x$	$x^6 + x^4 + x^3 + x^2 + 1$	$x^6 + x^5 + x^3$	$x^6 + x^5 + x^4 + x^3 + x + 1$
$x^7 + x^3 + 1$	$x^7 + x^4 + x^3 + x$	$x^7 + x^5 + x^3 + x^2 + x + 1$	$x^7 + x^5 + x^4 + x^3 + x^2$
$x^7 + x^6 + x^2 + 1$	$x^7 + x^6 + x^4 + x^2 + x$	$x^7 + x^6 + x^5 + x + 1$	$x^7 + x^6 + x^5 + x^4$

Solutions of $g(x)$ satisfying $g^2(x) \equiv x^2 \pmod{x^8 + x^4 + 1}$ are as follows:

x	$x^4 + x^2 + x + 1$	$x^5 + x^3$	$x^5 + x^4 + x^3 + x^2 + 1$
$x^6 + x + 1$	$x^6 + x^4 + x^2 + x$	$x^6 + x^5 + x^3 + 1$	$x^6 + x^5 + x^4 + x^3 + x^2$
x^7	$x^7 + x^4 + x^2 + 1$	$x^7 + x^5 + x^3 + x$	$x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$
$x^7 + x^6 + 1$	$x^7 + x^6 + x^4 + x^2$	$x^7 + x^6 + x^5 + x^3 + x + 1$	$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x$

Solutions of $g(x)$ satisfying $g^2(x) \equiv x^2 \pmod{x^8 + x^6 + 1}$ are as follows:

x	$x^4 + x^3 + x + 1$	$x^5 + x^3 + 1$	$x^5 + x^4$
$x^6 + x^3 + x^2 + 1$	$x^6 + x^4 + x^2$	$x^6 + x^5 + x^2 + x$	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$x^7 + x^2 + 1$	$x^7 + x^4 + x^3 + x^2$	$x^7 + x^5 + x^3 + x^2 + x$	$x^7 + x^5 + x^4 + x^2 + x + 1$
$x^7 + x^6 + x^3 + x$	$x^7 + x^6 + x^4 + x + 1$	$x^7 + x^6 + x^5 + 1$	$x^7 + x^6 + x^5 + x^4 + x^3$

Interestingly, by doing experiments, we discover that the involutory Hadamard MDS matrix cannot be constructed via x^8+x+1, x^8+x^3+1, x^8+x^5+1, x^8+x^7+1. However, the involutory Hadamard MDS matrix can be constructed via x^8+x^2+1, x^8+x^4+1 x^8+x^6+1. Therefore, we say that $x^8 + x^2 + 1$, $x^8 + x^4 + 1$, $x^8 + x^6 + 1$ are adaptive.

Algorithm 2 is specially designed to construct lightweight 4×4 involutory Hadamard MDS matrices over the matrix polynomial residue ring. The platform of Algorithm 2 is the same as Algorithm 1. In the following experiments, we construct corresponding results by exhaustive search on corresponding matrix polynomial residue rings. By running the Algorithm 2, we get the following results:

1. Over 4×4 matrix polynomial residue rings, construction of 288 involutory Hadamard MDS matrices with 24 XORs only takes about 2 seconds.

Algorithm 2 Construction of lightweight involutory Hadamard MDS matrices

for Search for every permutation $\{a_1, a_2, ..., a_8\}$ of $\{1, 2, ..., 8\}$. **do**
  for i from 1 to 8 **do**
    for j from 1 to 8 and $j \neq a_i$ **do**
      Construct the binary matrix T=$[a_1, ... , [a_i, j] ..., a_8]$. Therefore, T is a non-singular binary matrix with 1 XOR.
      Find the minimal polynomial $f(x)$ of T.
      Find polynomials $b_1(x), \cdots, b_k(x)$ satisfying $\#b(T) \leq 3$.
      Find all $q(x)$ satisfying $q(x)^2 \equiv x^2 \pmod{f(x)}$. Let the results be $q_1(x), ..., q_d(x)$
      for t from 1 to k **do**
        Let $b(x) = b_t(x)$
        for h from 1 to d **do**
          Let $c(x) = b_t(x) + q_h(x)$.
          if $Had(1, x, b(x), c(x))$ is MDS **then**
            Record this involutory Hadamard MDS matrix and its sum of XORs.
          end if
        end for
      end for
    end for
  end for
end for

2. Over 8×8 matrix polynomial residue rings, construction of 80640 involutory Hadamard MDS matrices with 20 XORs only takes about 1 minutes and 4 seconds.

Two examples are presented as follows:

Example 5. $T = [[1, 2], 3, 4, 1]$ is a 4×4 binary matrix. The following matrix is an involutory Hadamard MDS matrix with 24 XORs.

$$\begin{pmatrix} I & T & T^2 & T^2+T \\ T & I & T^2+T & T^2 \\ T^2 & T^2+T & I & T \\ T^2+T & T^2 & T & I \end{pmatrix}$$

Example 6. $T = [4, 1, 2, 8, 6, 3, [5, 8], 7]$ is a 8×8 binary matrix. The following matrix is an involutory Hadamard MDS matrix with 20 XORs.

$$\begin{pmatrix} I & T & T^6+T^4 & T^2 \\ T & I & T^2 & T^6+T^4 \\ T^6+T^4 & T^2 & I & T \\ T^2 & T^6+T^4 & T & I \end{pmatrix}$$

Comparisons with previous constructions of lightweight involutory Hadamard MDS matrices are depicted in Table 5. Comparisons with [22] are depicted in Table 6. In Table 5 and Table 6, the *sum of XORs* denotes the sum of XOR counts of the entirety-matrix.

Next, we analyze search spaces of our constructions and constructions over $GL(8, \mathbb{F}_2)$.

- Over $GL(8, \mathbb{F}_2)$, there are 1048320 matrices with 1, 2 or 3 XORs. Therefore, to construct involutory Hadamard MDS matrices $Had(I, A, B, C)$ over $GL(8, \mathbb{F}_2)$, the search space of $Had(I, A, B, C)$ is $1048320^3 \approx 1.152 \times 10^{18}$.

- Over the 8×8 matrix polynomial residue ring, we discover that if A and $A + I$ are non-singular, $\#A = 1$ and the minimal polynomial of A is adaptive to construct involutory Hadamard MDS matrices, then the number of A is 120960. According to Corollary 1, $Had(1, x, b(x), c(x))$ is involutory if and only if $(b(x) + c(x))^2 = x^2$. For the minimal polynomial $f(x)$ of each A, there are only 16 kinds of $g(x)$ satisfying

Table 5: Comparisons with previous constructions of lightweight involutory Hadamard MDS matrices

Matrix type	Element	Sum of XORs	Ref.
$Had(I, A, A^{-1}, A + A^{-1})$	$GL(4, \mathbb{F}_2)$	24	[22]
$Had(\texttt{0x1}, \texttt{0x4}, \texttt{0x9}, \texttt{0xd})$	$\mathbb{F}_{2^4}/\texttt{0x13}$	24	[18][25]
$Had(\texttt{0x1}, \texttt{0x2}, \texttt{0x6}, \texttt{0x4})$	$\mathbb{F}_{2^4}/\texttt{0x19}$	24	[1]
$Had(I, A, B, C)$	$\mathbb{F}_2[T_{4\times4}]$	24	Ours
$Hadamard - Cauchy(\texttt{0x01}, \texttt{0x02}, \texttt{0xfc}, \texttt{0xfe})$	$\mathbb{F}_{2^8}/\texttt{0x11b}$	296	[12]
$Had(\texttt{0x01}, \texttt{0x02}, \texttt{0x04}, \texttt{0x06})$	$\mathbb{F}_{2^8}/\texttt{0x11d}$	88	[5]
$Had(\texttt{0x01}, \texttt{0x02}, \texttt{0xb0}, \texttt{0xb2})$	$\mathbb{F}_{2^8}/\texttt{0x165}$	64	[25]
$Subfield - Had(\texttt{0x1}, \texttt{0x4}, \texttt{0x9}, \texttt{0xd})$	$\mathbb{F}_{2^4}/\texttt{0x13}$	48	[25]
$Had(I, A, A^{-1}, A + A^{-1})$	$GL(8, \mathbb{F}_2)$	40	[22]
$Had(I, A, B, C)$	$\mathbb{F}_2[T_{8\times8}]$	20	Ours

Table 6: Comparisons of construction efficiency with [22]

Matrix type	Element	Sum of XORs	Number	Running time	Ref.
$Optimal(sepcial)$	$GL(8, \mathbb{F}_2)$	10	40320	no mentioned	[22]
$Optimal(special)$	$\mathbb{F}_2[T_{8\times8}]$	10	40320	1min 16sec	Ours
$Circ(I, I, A, B)$	$GL(8, \mathbb{F}_2)$	12	80640	3days	[22]
$Circ(I, I, A, B)$	$\mathbb{F}_2[T_{8\times8}]$	12	80640	1min 27sec	Ours
$Had(I, A, A^T, B)$	$GL(8, \mathbb{F}_2)$	20	622	4weeks	[22]
$Had(I, A, B, C)$	$\mathbb{F}_2[T_{8\times8}]$	20	241920	7min	Ours
$InvolutoryHad(I, A, A^{-1}, A + A^{-1})$	$GL(8, \mathbb{F}_2)$	40	80640	1day	[22]
$InvolutoryHad(I, A, B, C)$	$\mathbb{F}_2[T_{8\times8}]$	20	80640	1min 04sec	Ours

$g(x)^2 = x^2$. Therefore, $b(x) = c(x) + g(x)$. Consequently, the search space of $Had(1, A, B, C)$, in our construction, is $120960\times2^8\times16 \approx 4.954\times10^8$, which is much fewer than 1.152×10^{18}.

Table 7: Comparisons of search space of constructing lightweight MDS matrices

Matrix type	Element	Search space
$Circ(I, I, A, B)$	$GL(8, \mathbb{F}_2)$	1.099×10^{12}
$Circ(I, I, A, B)$	$\mathbb{F}_2[T_{8\times8}]$	4.516×10^6
S_5	$GL(8, \mathbb{F}_2)$	1.458×10^{48}
S_5	$\mathbb{F}_2[T_{8\times8}]$	1.849×10^{10}
$Involutory\ Had(I, A, B, C)$	$GL(8, \mathbb{F}_2)$	1.152×10^{18}
$Involutory\ Had(I, A, B, C)$	$\mathbb{F}_2[T_{8\times8}]$	4.954×10^8

6 Conclusions

This paper investigates the construction of 4×4 lightweight MDS matrices over the $m \times m$ matrix polynomial residue ring, where m=4, 8 or 16. With the high efficiency of identifying MDS matrices, the distribution of minimal polynomials of non-singular binary matrices and the distribution of elements with few XORs, we propose an efficient algorithm to construct lightweight MDS matrices. Besides, we propose three theorems about the existence of involutory MDS matrices over $GL(m, \mathbb{F}_2)$ and over the matrix polynomial residue ring. Moreover, we propose an efficient necessary and sufficient condition for identifying an involutory Hadamard matrix. By incorporating this condition, we propose

another efficient algorithm to construct lightweight involutory Hadamard MDS matrices and we get optimized results as compared to previous works.

Acknowledgments

We want to give our thanks to the anonymous reviews of FSE 2018 and to Dr. Bing Sun for his effort to improving the quality of our manuscript. This work is supported by the National Key Research and Development Program (No. 2016YFB0800602) and the National Natural Science Foundation of China (NSFC) (No. 61502048).

References

[1] Andreeva, E., Bilgin, B., Bogdanov, A., Luykx, A., Mendel, F., Mennink, B., Mouha, N., Wang, Q., Yasuda, K.: PRIMATEs v1. Submission to the CAESAR Competition. http://competitions.cr.yp.to/round1/primatesv1.pdf (2014)

[2] Augot, D., Finiasz, M.: Direct construction of recursive MDS diffusion layers using shortened BCH codes. In: International Conference on Fast Software Encryption, pp. 3-17. Springer, Heidelberg (2014)

[3] Augot, D., Finiasz, M.: Exhaustive search for small dimension recursive MDS diffusion layers for block ciphers and hash functions. In: Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on, pp. 1551-1555. IEEE. (2013)

[4] Aumasson, J. P., Henzen, L., Meier, W., Naya-Plasencia, M.: Quark: A lightweight hash. In: International Workshop on Cryptographic Hardware and Embedded Systems. pp. 1-15. Springer, Heidelberg (2010)

[5] Barreto, P., Rijimen, V.: The anubis block cipher. Submission to the NESSIE Project (2000)

[6] Bogdanov, A., Knežević, M., Leander, G., Toz, D., Varıcı, K., Verbauwhede, I.: SPONGENT: A lightweight hash function. In: International Workshop on Cryptographic Hardware and Embedded Systems. pp. 312-325. Springer, Heidelberg (2011)

[7] Berger, T.P.: Construction of recursive MDS diffusion layers from Gabidulin codes. In: International Conference on Cryptology in India. INDOCRYPT 2013. LNCS, vol. 8250, pp. 274–285. Springer, Cham (2013)

[8] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404 (2013)

[9] Bogdanov, A.A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007)

[10] Berger, T. P., El Amrani, N.: Codes over $L(GF(2)^m, GF(2)^m)$, MDS Diffusion Matrices and Cryptographic Applications. In: International Conference on Codes, Cryptology, and Information Security. pp. 197-214. Springer International Publishing (2015)

[11] Beierle, C., Kranz, T., Leander, G.: Lightweight Multiplication in $GF(2^n)$ with Applications to MDS Matrices. In: Annual Cryptology Conference. pp. 625-653. Springer Berlin Heidelberg (2016)

[12] Chand Gupta, K., Ghosh Ray, I.: On constructions of circulant MDS matrices for lightweight cryptography. In: Huang, X., Zhou, J. (eds.) ISPEC 2014. LNCS, vol. 8434, pp. 564–576. Springer, Heidelberg (2014)

[13] Daemen, J., Knudsen, L., Rijmen, V.: The block cipher Square. In: International Workshop on Fast Software Encryption, pp. 149-165. Springer, Heidelberg (1997)

[14] Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Springer, Heidelberg (2002)

[15] Guo, J., Peyrin, T., Poschmann, A.: The PHOTON family of lightweight hash functions. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 222–239. Springer, Heidelberg (2011)

[16] Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED block cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer, Heidelberg (2011)

[17] Gupta, K. C., Ray, I. G.: On constructions of MDS matrices from companion matrices for lightweight cryptography. In: International Conference on Availability, Reliability, and Security, pp. 29-43. Springer, Heidelberg(2013)

[18] Jean, J., Nikolic, I., Peyrin, T.:Joltik v1.1. Submission to the CAESAR competition(2014) http://www1.spms.ntu.edu.sg/ syllab/Joltik

[19] Junod, P., Vaudenay, S.: Perfect diffusion primitives for block ciphers. In: International Workshop on Selected Areas in Cryptography. pp. 84-99. Springer, Heidelberg (2004)

[20] Khoo K, Peyrin T, Poschmann A Y, et al. FOAM: searching for hardware-optimal SPN structures and components with a fair comparison. In: International Workshop on Cryptographic Hardware and Embedded Systems. pp. 433-450. Springer, Heidelberg (2014).

[21] Liu, M., Sim, S. M.: Lightweight MDS generalized circulant matrices. In: International Conference on Fast Software Encryption. pp. 101-120. Springer, Heidelberg (2016)

[22] Li, Y., Wang, M.: On the construction of lightweight circulant involutory MDS matrices. In: International Conference on Fast Software Encryption. pp. 121-139. Springer, Berlin, Heidelberg (2016)

[23] Li T., Bai J., Sun Y., Wang D., Lin D.: The Lightest 4x4 MDS Matrices over GL (4, F2) http://eprint.iacr.org/2016/686.pdf (2016)

[24] Nakahara Jr., J., Abraho, I.: A new involutory mds matrix for the aes. I. J Netw. Secur. 9(2), pp. 109–116 (2009)

[25] Sim, S. M., Khoo, K., Oggier, F., Peyrin, T.: Lightweight MDS involution matrices. In: International Workshop on Fast Software Encryption, pp. 471-493. Springer Berlin Heidelberg(2015)

[26] Sajadieh, M., Dakhilalian, M., Mala, H., Sepehrdad, P.: Recursive diffusion layers for block ciphers and hash functions. In: International Conference on Fast Software Encryption. LNCS, vol. 7549, pp. 385–401. Springer, Heidelberg (2012)

[27] Sarkar S. and Syed H.: Lightweight diffusion layer: Importance of Toeplitz matrices. In: IACR Transactions on Symmetric Cryptology, vol. 2016(1), pp. 95-113, (2016)

[28] Sarkar S. and Syed H.: Analysis of Toeplitz MDS Matrices. In: Australasian Conference on Information Security and Privacy. pp. 3-18, Springer, Cham (2017)

[29] Wu, S.,Wang,M.,Wu,W.: Recursive diffusion layers for (lightweight) block ciphers and hash functions. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 355–371. Springer, Heidelberg (2013)

[30] Yang, G., Zhu, B., Suder, V., Aagaard, M.D., Gong, G.: The Simeck family of lightweight block ciphers. In: Guneysu, T., Handschuh, H. (eds.) CHES 2015. LNCS, vol. 9293, pp. 307–329. Springer, Heidelberg (2015)

[31] Zhang S., Wang Y., Gao Y., and Wang T.: On the Construction of the 4 x 4 Lightest Circulant MDS Matrices. In: Proceedings of the 2017 International Conference on Cryptography. Security and Privacy, pp. 1-6. ACM (2017)