Orthogonal MDS Diffusion Matrices Over Galois Rings

Chik How Tan and Theo Fanuela Prabowo

Temasek Laboratories, National University of Singapore

{*tsltch,tslfp*}*@nus.edu.sg*

December 14, 2017

Overview

Background

Motivation

Background

Motivation

- MDS matrix (Maximum Distance Separable) is commonly used in block cipher algorithm to provide diffusion of bit/byte

Background

Motivation

- MDS matrix (Maximum Distance Separable) is commonly used in block cipher algorithm to provide diffusion of bit/byte
- MDS matrix is also to ensure the minimum differential probability

Background

Motivation

- MDS matrix (Maximum Distance Separable) is commonly used in block cipher algorithm to provide diffusion of bit/byte
- MDS matrix is also to ensure the minimum differential probability
- Currently, all of the MDS matrices used in block cipher are over $\mathbb{F}_{2^k}$ (usually $k = 8$ in AES algorithm)

Background

Motivation

- MDS matrix (Maximum Distance Separable) is commonly used in block cipher algorithm to provide diffusion of bit/byte
- MDS matrix is also to ensure the minimum differential probability
- Currently, all of the MDS matrices used in block cipher are over $\mathbb{F}_{2^k}$ (usually $k = 8$ in AES algorithm)
- For permutation-based structure algorithm (Hash function, Authenticated encryptions, etc), they are big block size, say 512 bits or 1024 bits. Then bigger MDS matrix is required

Background

Motivation

- MDS matrix (Maximum Distance Separable) is commonly used in block cipher algorithm to provide diffusion of bit/byte
- MDS matrix is also to ensure the minimum differential probability
- Currently, all of the MDS matrices used in block cipher are over $\mathbb{F}_{2^k}$ (usually $k = 8$ in AES algorithm)
- For permutation-based structure algorithm (Hash function, Authenticated encryptions, etc), they are big block size, say 512 bits or 1024 bits. Then bigger MDS matrix is required
- All of the constructions of MDS matrix are over finite fields

Background

Motivation

- MDS matrix (Maximum Distance Separable) is commonly used in block cipher algorithm to provide diffusion of bit/byte
- MDS matrix is also to ensure the minimum differential probability
- Currently, all of the MDS matrices used in block cipher are over $\mathbb{F}_{2^k}$ (usually $k = 8$ in AES algorithm)
- For permutation-based structure algorithm (Hash function, Authenticated encryptions, etc), they are big block size, say 512 bits or 1024 bits. Then bigger MDS matrix is required
- All of the constructions of MDS matrix are over finite fields
  - D. Augot et. al. [2014], K. C. Gupta et. al. [2017], Y. Li et. al. [2016], S. M. Sim et. al. [2015], etc

Background

Motivation

- MDS matrix (Maximum Distance Separable) is commonly used in block cipher algorithm to provide diffusion of bit/byte
- MDS matrix is also to ensure the minimum differential probability
- Currently, all of the MDS matrices used in block cipher are over $\mathbb{F}_{2^k}$ (usually $k = 8$ in AES algorithm)
- For permutation-based structure algorithm (Hash function, Authenticated encryptions, etc), they are big block size, say 512 bits or 1024 bits. Then bigger MDS matrix is required
- All of the constructions of MDS matrix are over finite fields
  - D. Augot et. al. [2014], K. C. Gupta et. al. [2017], Y. Li et. al. [2016], S. M. Sim et. al. [2015], etc
- We explore MDS matrix over Galois ring and its constructions

Galois Rings

Galois rings and their properties

- Galois ring: $GR(2^n, k) = \mathbb{Z}_{2^n}[x]/(f(x))$

Galois Rings

Galois rings and their properties

- Galois ring: $GR(2^n, k) = \mathbb{Z}_{2^n}[x]/(f(x))$
- Epimorphism: $\mu : GR(2^n, k) = \mathbb{Z}_{2^n}[x]/(f(x)) \longrightarrow \mathbb{F}_{2^k} = \mathbb{F}_2[x]/(\bar{f}(x))$

$$\mu(\sum_{i=0}^{k-1} a_i \alpha^i) = \sum_{i=0}^{k-1} \bar{a}_i \bar{\alpha}^i, \qquad a_i \in \mathbb{Z}_{2^n}, \;\; \bar{a}_i \in \mathbb{F}_2$$

Galois Rings

Galois rings and their properties

- Galois ring: $GR(2^n, k) = \mathbb{Z}_{2^n}[x]/(f(x))$
- Epimorphism: $\mu : GR(2^n, k) = \mathbb{Z}_{2^n}[x]/(f(x)) \longrightarrow \mathbb{F}_{2^k} = \mathbb{F}_2[x]/(\bar{f}(x))$

$$\mu(\sum_{i=0}^{k-1} a_i \alpha^i) = \sum_{i=0}^{k-1} \bar{a}_i \bar{\alpha}^i, \qquad a_i \in \mathbb{Z}_{2^n}, \;\; \bar{a}_i \in \mathbb{F}_2$$

- Unit element: $\beta \in GR(2^n, k)$ s.t $\exists\, \gamma$ and $\beta\gamma = 1$. Denote $U(GR(2^n, k))$ as all unit elements in $GR(2^n, k)$. $|\,U(GR(2^n, k))\,| = 2^{(n-1)k}(2^k - 1)$

Galois Rings

Galois rings and their properties

- Galois ring: $GR(2^n, k) = \mathbb{Z}_{2^n}[x]/(f(x))$
- Epimorphism: $\mu : GR(2^n, k) = \mathbb{Z}_{2^n}[x]/(f(x)) \longrightarrow \mathbb{F}_{2^k} = \mathbb{F}_2[x]/(\bar{f}(x))$

$$\mu(\sum_{i=0}^{k-1} a_i \alpha^i) = \sum_{i=0}^{k-1} \bar{a}_i \bar{\alpha}^i, \qquad a_i \in \mathbb{Z}_{2^n}, \;\; \bar{a}_i \in \mathbb{F}_2$$

- Unit element: $\beta \in GR(2^n, k)$ s.t $\exists\, \gamma$ and $\beta\gamma = 1$. Denote $U(GR(2^n, k))$ as all unit elements in $GR(2^n, k)$. $|\,U(GR(2^n, k))\,| = 2^{(n-1)k}(2^k - 1)$
- Square element: $\beta \in GR(2^n, k)$ s.t. $\exists\, \gamma$ and $\beta = \gamma^2$. Note: 1 is square and -1 is non-square

Galois Rings

Galois rings and their properties

- Galois ring: $GR(2^n, k) = \mathbb{Z}_{2^n}[x]/(f(x))$
- Epimorphism: $\mu : GR(2^n, k) = \mathbb{Z}_{2^n}[x]/(f(x)) \longrightarrow \mathbb{F}_{2^k} = \mathbb{F}_2[x]/(\bar{f}(x))$

$$\mu(\sum_{i=0}^{k-1} a_i \alpha^i) = \sum_{i=0}^{k-1} \bar{a}_i \bar{\alpha}^i, \qquad a_i \in \mathbb{Z}_{2^n}, \;\; \bar{a}_i \in \mathbb{F}_2$$

- Unit element: $\beta \in GR(2^n, k)$ s.t $\exists\, \gamma$ and $\beta\gamma = 1$. Denote $U(GR(2^n, k))$ as all unit elements in $GR(2^n, k)$. $|\,U(GR(2^n, k))\,| = 2^{(n-1)k}(2^k - 1)$
- Square element: $\beta \in GR(2^n, k)$ s.t. $\exists\, \gamma$ and $\beta = \gamma^2$. Note: 1 is square and -1 is non-square
- The number of square elements in $U(GR(2^n, k))$ is $2^{(n-2)k-1}(2^k - 1)$

Galois Rings

Galois rings and their properties

- Galois ring: $GR(2^n, k) = \mathbb{Z}_{2^n}[x]/(f(x))$
- Epimorphism: $\mu : GR(2^n, k) = \mathbb{Z}_{2^n}[x]/(f(x)) \longrightarrow \mathbb{F}_{2^k} = \mathbb{F}_2[x]/(\bar{f}(x))$

$$\mu(\sum_{i=0}^{k-1} a_i \alpha^i) = \sum_{i=0}^{k-1} \bar{a}_i \bar{\alpha}^i, \qquad a_i \in \mathbb{Z}_{2^n}, \;\; \bar{a}_i \in \mathbb{F}_2$$

- Unit element: $\beta \in GR(2^n, k)$ s.t $\exists\, \gamma$ and $\beta\gamma = 1$. Denote $U(GR(2^n, k))$ as all unit elements in $GR(2^n, k)$. $|\, U(GR(2^n, k))\,| = 2^{(n-1)k}(2^k - 1)$
- Square element: $\beta \in GR(2^n, k)$ s.t. $\exists\, \gamma$ and $\beta = \gamma^2$. Note: 1 is square and -1 is non-square
- The number of square elements in $U(GR(2^n, k))$ is $2^{(n-2)k-1}(2^k - 1)$

Lemma

Let j, l be integers s.t. $0 \leq j < \frac{k}{2}$ and $0 \leq l < 2^{n-2}$. If $2 \mid c_i$, for all $i \neq 2j$, $i \leq k-1$, then $-5^l\alpha^{2j} + \sum_{i \neq 2j,\, i \leq k-1} c_i \alpha^i$ is not a square in $U(GR(2^n, k))$.

Hadamard Matrices

Definition

- A matrix M is Hadamard if $MM^T = cI$, where is a constant.

Hadamard Matrices

Definition

- A matrix M is Hadamard if $MM^T = cI$, where is a constant.
- If $c = 1$, M is called orthogonal.

Hadamard Matrices

Definition

- A matrix M is Hadamard if $MM^T = cI$, where is a constant.
- If $c = 1$, M is called orthogonal.

Pseudo Hadamard Matrices

$$\begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{b} & \mathbf{a} \end{bmatrix}$$

2×2

PHD$(\mathbf{a}, \mathbf{b})$

$$\begin{bmatrix} \mathbf{a} & \mathbf{b} & \mathbf{c} & \mathbf{d} \\ \mathbf{b} & \mathbf{a} & \mathbf{d} & \mathbf{c} \\ \mathbf{c} & \mathbf{d} & \mathbf{a} & \mathbf{b} \\ \mathbf{d} & \mathbf{c} & \mathbf{b} & \mathbf{a} \end{bmatrix}$$

4×4

PHD$(\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d})$

$$\begin{bmatrix} \mathbf{a} & \mathbf{b} & \mathbf{c} & \mathbf{d} & \mathbf{e} & \mathbf{f} & \mathbf{g} & \mathbf{h} \\ \mathbf{b} & \mathbf{a} & \mathbf{d} & \mathbf{c} & \mathbf{f} & \mathbf{e} & \mathbf{h} & \mathbf{g} \\ \mathbf{c} & \mathbf{d} & \mathbf{a} & \mathbf{b} & \mathbf{g} & \mathbf{h} & \mathbf{e} & \mathbf{f} \\ \mathbf{d} & \mathbf{c} & \mathbf{b} & \mathbf{a} & \mathbf{h} & \mathbf{g} & \mathbf{f} & \mathbf{e} \\ \mathbf{e} & \mathbf{f} & \mathbf{g} & \mathbf{h} & \mathbf{a} & \mathbf{b} & \mathbf{c} & \mathbf{d} \\ \mathbf{f} & \mathbf{e} & \mathbf{h} & \mathbf{g} & \mathbf{b} & \mathbf{a} & \mathbf{d} & \mathbf{c} \\ \mathbf{g} & \mathbf{h} & \mathbf{e} & \mathbf{f} & \mathbf{c} & \mathbf{d} & \mathbf{a} & \mathbf{b} \\ \mathbf{h} & \mathbf{g} & \mathbf{f} & \mathbf{e} & \mathbf{d} & \mathbf{c} & \mathbf{b} & \mathbf{a} \end{bmatrix}$$

8×8

PHD$(\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}, \mathbf{f}, \mathbf{g}, \mathbf{h})$

Enabling Hadamard $(1, -1)$-matrices

$$\begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{b} & -\mathbf{a} \end{bmatrix} = \begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{b} & \mathbf{a} \end{bmatrix} \odot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$\mathsf{HD}(\mathbf{a}, \mathbf{b}; S) \quad \mathsf{PHD}(\mathbf{a}, \mathbf{b}) \quad S$$

Enabling Hadamard $(1, -1)$-matrices

$$\begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{b} & -\mathbf{a} \end{bmatrix} = \begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{b} & \mathbf{a} \end{bmatrix} \odot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$\mathsf{HD}(\mathbf{a}, \mathbf{b}; S) \quad \mathsf{PHD}(\mathbf{a}, \mathbf{b}) \quad S$$

Proposition

- There are 8 2×2 enabling Hadamard $(1, -1)$-matrices

Enabling Hadamard $(1, -1)$-matrices

$$\begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{b} & -\mathbf{a} \end{bmatrix} = \begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{b} & \mathbf{a} \end{bmatrix} \odot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$\mathsf{HD}(\mathbf{a}, \mathbf{b}; S) \quad \mathsf{PHD}(\mathbf{a}, \mathbf{b}) \quad S$$

Proposition

- There are 8 2×2 enabling Hadamard $(1, -1)$-matrices
- There are 256 4×4 enabling Hadamard $(1, -1)$-matrices

Enabling Hadamard $(1, -1)$-matrices

$$\begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{b} & -\mathbf{a} \end{bmatrix} = \begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{b} & \mathbf{a} \end{bmatrix} \odot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$\mathsf{HD}(\mathbf{a}, \mathbf{b}; S) \quad \mathsf{PHD}(\mathbf{a}, \mathbf{b}) \quad S$$

Proposition

- There are 8 2×2 enabling Hadamard $(1, -1)$-matrices
- There are 256 4×4 enabling Hadamard $(1, -1)$-matrices
- There are $2^{19} = 524,288$ 8×8 enabling Hadamard $(1, -1)$-matrices

Enabling Hadamard $(1, -1)$-matrices

$$\begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{b} & -\mathbf{a} \end{bmatrix} = \begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{b} & \mathbf{a} \end{bmatrix} \odot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$\mathsf{HD}(\mathbf{a}, \mathbf{b}; S) \quad \mathsf{PHD}(\mathbf{a}, \mathbf{b}) \quad S$$

Proposition

- There are 8 2×2 enabling Hadamard $(1, -1)$-matrices
- There are 256 4×4 enabling Hadamard $(1, -1)$-matrices
- There are $2^{19} = 524,288$ 8×8 enabling Hadamard $(1, -1)$-matrices

Some 4×4 enabling Hadamard $(1, -1)$-matrices

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 1 & 1 & 1 \\ -1 & -1 & -1 & 1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \end{bmatrix}.$$

MDS matrices

Definition

- An $m \times m$ matrix M is MDS if every $r \times r$ submatrix of M is non-singular for all $1 \leq r \leq m$.

MDS matrices

Definition

- An $m \times m$ matrix M is MDS if every $r \times r$ submatrix of M is non-singular for all $1 \leq r \leq m$.

Theorem

An $m \times m$ matrix $M = (a_{ij})$ over $U(GR(2^n, k))$ is MDS if and only if $\bar{M} = (\bar{a}_{ij})$ over $\mathbb{F}_{2^k}$ is MDS, where $\bar{a}_{ij} = \mu(a_{ij})$

MDS matrices

Definition

- An $m \times m$ matrix M is MDS if every $r \times r$ submatrix of M is non-singular for all $1 \leq r \leq m$.

Theorem

An $m \times m$ matrix $M = (a_{ij})$ over $U(GR(2^n, k))$ is MDS if and only if $\bar{M} = (\bar{a}_{ij})$ over $\mathbb{F}_{2^k}$ is MDS, where $\bar{a}_{ij} = \mu(a_{ij})$

Strategy

- Construct $m \times m$ Hadamard MDS matrix $\bar{M} = (\bar{a}_{ij})$ over $\mathbb{F}_{2^k}$

MDS matrices

Definition

- An $m \times m$ matrix M is MDS if every $r \times r$ submatrix of M is non-singular for all $1 \leq r \leq m$.

Theorem

An $m \times m$ matrix $M = (a_{ij})$ over $U(GR(2^n, k))$ is MDS if and only if $\bar{M} = (\bar{a}_{ij})$ over $\mathbb{F}_{2^k}$ is MDS, where $\bar{a}_{ij} = \mu(a_{ij})$

Strategy

- Construct $m \times m$ Hadamard MDS matrix $\bar{M} = (\bar{a}_{ij})$ over $\mathbb{F}_{2^k}$
- Lift $\bar{M}$ to $M = (a_{ij})$ over $U(GR(2^n, k))$ as $\bar{a}_{ij} = \mu(a_{ij})$, where $\sum_{i=1}^{m} a_{1i}^2 = 1$

MDS matrices

Definition

- An $m \times m$ matrix M is MDS if every $r \times r$ submatrix of M is non-singular for all $1 \leq r \leq m$.

Theorem

An $m \times m$ matrix $M = (a_{ij})$ over $U(GR(2^n, k))$ is MDS if and only if $\bar{M} = (\bar{a}_{ij})$ over $\mathbb{F}_{2^k}$ is MDS, where $\bar{a}_{ij} = \mu(a_{ij})$

Strategy

- Construct $m \times m$ Hadamard MDS matrix $\bar{M} = (\bar{a}_{ij})$ over $\mathbb{F}_{2^k}$
- Lift $\bar{M}$ to $M = (a_{ij})$ over $U(GR(2^n, k))$ as $\bar{a}_{ij} = \mu(a_{ij})$, where $\sum_{i=1}^{m} a_{1i}^2 = 1$
- $M \odot S$ is orthogonal MDS matrix over $U(GR(2^n, k))$, where S is enabling Hadamard $(1, -1)$-matrix

2×2 Orthogonal MDS Matrices over $GR(2^n, k)$

Lemma

If $\mathbf{u}, \mathbf{v} \in U(GR(2^n, k))$ *and* $\mathbf{u}^2 + \mathbf{v}^2 \in U(GR(2^n, k))$, *then* $\mathbf{u}^2 + \mathbf{v}^2$ *is not a square in* $U(GR(2^n, k))$.

2×2 Orthogonal MDS Matrices over $GR(2^n, k)$

Lemma

If $\mathbf{u}, \mathbf{v} \in U(GR(2^n, k))$ *and* $\mathbf{u}^2 + \mathbf{v}^2 \in U(GR(2^n, k))$, *then* $\mathbf{u}^2 + \mathbf{v}^2$ *is not a square in* $U(GR(2^n, k))$.

Corollary

There is no 2×2 *orthogonal MDS matrix over* $U(GR(2^n, k))$.

2×2 Orthogonal MDS Matrices over $GR(2^n, k)$

Lemma

If $\mathbf{u}, \mathbf{v} \in U(GR(2^n, k))$ *and* $\mathbf{u}^2 + \mathbf{v}^2 \in U(GR(2^n, k))$, *then* $\mathbf{u}^2 + \mathbf{v}^2$ *is not a square in* $U(GR(2^n, k))$.

Corollary

There is no 2×2 *orthogonal MDS matrix over* $U(GR(2^n, k))$.

Proof.

Let M be 2×2 an orthogonal MDS matrix over $U(GR(2^n, k))$, say $M = \begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{bmatrix}$. Then, we must have $\mathbf{a}^2 + \mathbf{b}^2 = 1$ and $\mathbf{c}^2 + \mathbf{d}^2 = 1$. By previous Lemma, $\mathbf{u}^2 + \mathbf{v}^2$ is a non-square. Therefore, there is no 2×2 orthogonal MDS matrix over $U(GR(2^n, k))$. □

4×4 Orthogonal MDS Matrices over $GR(2^n, k)$

Proposition

For $2 \mid k$, $\omega \in \mathbb{F}_{2^k}$, s.t. $\omega^3 = 1$ and $z \in \mathbb{F}_{2^k} \setminus \{1, \omega, \omega^2\}$, then $\mathsf{HD}(1, z, z\omega, z\omega^2; \mathbb{I})$ is an orthogonal MDS matrices over $\mathbb{F}_{2^k}$

4×4 Orthogonal MDS Matrices over $GR(2^n, k)$

Proposition

For $2 \mid k$, $\omega \in \mathbb{F}_{2^k}$, s.t. $\omega^3 = 1$ and $z \in \mathbb{F}_{2^k} \setminus \{1, \omega, \omega^2\}$, then $\mathrm{HD}(1, z, z\omega, z\omega^2; \mathbb{I})$ is an orthogonal MDS matrices over $\mathbb{F}_{2^k}$

Theorem

Let $\mathbf{c}, \mathbf{d}, \mathbf{z} \in U(GR(2^n, k))$ *s.t.* $\mu(\mathbf{c}) = \omega$, $\mu(\mathbf{d}) = \omega^2$ *and* $\mu(\mathbf{z}) \in \mathbb{F}_{2^k} \setminus \{1, \omega, \omega^2\}$. *If* $1 + \mathbf{c}^2 + \mathbf{d}^2 = 0$, *then* $\mathrm{HD}(1, \mathbf{z}, \mathbf{zc}, \mathbf{zd}; S)$ *is an orthogonal MDS matrix over* $U(GR(2^n, k))$, *where* S *is an enabling Hadamard* $(1, -1)$*-matrix if one of the following holds:*

1. $k = 4$, $f(x) = x^4 + x + 1$, $\mathbf{c} = \alpha^2 + \alpha$, $\mathbf{d} = \alpha^2 - \alpha - 1$,
2. $k = 6$, $f(x) = x^6 + x^5 + 1$, $\mathbf{c} = \alpha^5 + \alpha^4 + \alpha^3 + 1$, $\mathbf{d} = \alpha^5 + \alpha^4 - \alpha^3$,
3. $k = 8$, $f(x) = x^8 + x^7 + x^2 + x + 1$, $\mathbf{c} = \alpha^7 - \alpha^5 - \alpha^3 + \alpha$, $\mathbf{d} = \alpha^7 - \alpha^5 + \alpha^3 + \alpha + 1$,
4. $k = 10$, $f(x) = x^{10} + x^5 + x^2 + x + 1$, $\mathbf{c} = \alpha^5 - \alpha$, $\mathbf{d} = \alpha^5 + \alpha + 1$.

4×4 Orthogonal MDS Matrices over $GR(2^n, k)$

Proposition

For $4 \,|\, k$, $\beta \in \mathbb{F}_{2^4} \subset \mathbb{F}_{2^k}$, s.t. $\sum_{i=0}^{3} \beta^{2^i} = 1$, then HD$(\beta, \beta^2, \beta^4, \beta^8; \mathbb{I})$ is an orthogonal MDS matrices over $\mathbb{F}_{2^k}$

4×4 Orthogonal MDS Matrices over $GR(2^n, k)$

Proposition

For $4 \mid k$, $\beta \in \mathbb{F}_{2^4} \subset \mathbb{F}_{2^k}$, s.t. $\sum_{i=0}^{3} \beta^{2^i} = 1$, then HD$(\beta, \beta^2, \beta^4, \beta^8; \mathbb{I})$ is an orthogonal MDS matrices over $\mathbb{F}_{2^k}$

Theorem

Let $\mathbf{z}_i \in U(GR(2^n, k))$ s.t $\mu(\mathbf{z}_i) = \beta^{2^i}$ and $\mathbf{z}_1^2 + \mathbf{z}_2^2 + \mathbf{z}_3^2 + \mathbf{z}_4^2 = 1$. If one of the following holds, then $\mathrm{HD}(\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3, \mathbf{z}_4, S)$ *is orthogonal MDS over $U(GR(2^n, k))$.*

1. $k = 4$, $f(x) = x^4 + x + 1$, $\mathbf{z}_0 = \alpha^3 + \alpha + 1$, $\mathbf{z}_1 = \alpha^3 - 1$, $\mathbf{z}_2 = \alpha^3 + \alpha^2 + 1$, $\mathbf{z}_3 = \alpha^3 - \alpha^2 - \alpha$,
2. $k = 8$, $f(x) = x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$,
   $\mathbf{z}_0 = \alpha^7 - \alpha^6 - \alpha^5 - \alpha^4 - \alpha^3 - \alpha$, $\mathbf{z}_1 = \alpha^7 + \alpha^6 - \alpha^3 + \alpha + 1$,
   $\mathbf{z}_2 = \alpha^6 - \alpha^5 - \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$, $\mathbf{z}_3 = \alpha^6 - \alpha^3 + \alpha^2 + \alpha + 1$,
3. $k = 16$, $f(x) = x^{16} + x^{15} + x^{10} + x^9 + x^4 + x^3 + 1$,
   $\mathbf{z}_0 = \alpha^{15} + \alpha^{14} + \alpha^{13} - \alpha^9 + \alpha^8 - \alpha^6 + \alpha^4 + \alpha^2 + 1$,
   $\mathbf{z}_1 = \alpha^{14} + \alpha^{13} + \alpha^{12} + \alpha^{10} + \alpha^9 + \alpha^5 - \alpha^2 + \alpha + 1$,
   $\mathbf{z}_2 = \alpha^{14} - \alpha^{11} + \alpha^8 + \alpha^7 + \alpha^4 + \alpha^2 - 1$,
   $\mathbf{z}_3 = \alpha^{15} + \alpha^{14} - \alpha^{12} - \alpha^{11} + \alpha^{10} + \alpha^7 + \alpha^6 - \alpha^5 + \alpha^2 + \alpha$.

Conclusion

Conclusion

- We discussed some basic properties of Galois ring

Conclusion

Conclusion

- We discussed some basic properties of Galois ring
- We constructed all 4×4 and 8×8 enabling Hadamard $(1, -1)$-matrices

Conclusion

Conclusion

- We discussed some basic properties of Galois ring
- We constructed all 4×4 and 8×8 enabling Hadamard $(1, -1)$-matrices
- We showed that matrix over $\mathbb{F}_{2^k}$ is MDS iff an extended matrix over $U(GR(2^n, k))$ is MDS

Conclusion

Conclusion

- We discussed some basic properties of Galois ring
- We constructed all 4×4 and 8×8 enabling Hadamard $(1, -1)$-matrices
- We showed that matrix over $\mathbb{F}_{2^k}$ is MDS iff an extended matrix over $U(GR(2^n, k))$ is MDS
- We proved that there is no 2×2 orthogonal MDS matrix over $GR(2^n, k))$

Conclusion

Conclusion

- We discussed some basic properties of Galois ring
- We constructed all 4×4 and 8×8 enabling Hadamard $(1, -1)$-matrices
- We showed that matrix over $\mathbb{F}_{2^k}$ is MDS iff an extended matrix over $U(GR(2^n, k))$ is MDS
- We proved that there is no 2×2 orthogonal MDS matrix over $GR(2^n, k))$
- constructed 4×4 orthogonal MDS matrices over $U(GR(2^n, k))$

Conclusion

Conclusion

- We discussed some basic properties of Galois ring
- We constructed all 4×4 and 8×8 enabling Hadamard $(1, -1)$-matrices
- We showed that matrix over $\mathbb{F}_{2^k}$ is MDS iff an extended matrix over $U(GR(2^n, k))$ is MDS
- We proved that there is no 2×2 orthogonal MDS matrix over $GR(2^n, k))$
- constructed 4×4 orthogonal MDS matrices over $U(GR(2^n, k))$
- For future work, we will
  - construct more 4×4 and 8×8 orthogonal MDS matrices over $U(GR(2^n, k))$

Conclusion

Conclusion

- We discussed some basic properties of Galois ring
- We constructed all 4×4 and 8×8 enabling Hadamard $(1, -1)$-matrices
- We showed that matrix over $\mathbb{F}_{2^k}$ is MDS iff an extended matrix over $U(GR(2^n, k))$ is MDS
- We proved that there is no 2×2 orthogonal MDS matrix over $GR(2^n, k))$
- constructed 4×4 orthogonal MDS matrices over $U(GR(2^n, k))$
- For future work, we will
  - construct more 4×4 and 8×8 orthogonal MDS matrices over $U(GR(2^n, k))$
  - apply these orthogonal MDS matrices in block cipher algorithm and analyse its security

Thank you