Direct construction of quasi-involutory recursive-like MDS matrices from 2-cyclic codes

Cauchois Victor [1] Loidreau Pierre [1] Merkiche Nabil [23]

[1]DGA-MI / IRMAR

[2]DGA-IP

[3]Sorbonnes Université, UPMC, LIP6

FSE 2017 March 6, 2017

Motivations

Definition

MDS matrices are matrices such that any minor is non singular.

- MDS matrices are widely used in Blockciphers and Hash functions.
- Lightweight designs $\Rightarrow$ circulant or recursive matrices.
- Involutory matrices $\Rightarrow$ Both encryption and decryption with the same structure.
- No circulant involutory MDS matrix [GR14].

Agenda

- Recursive involutory MDS matrix ?
- We propose a new direct construction of MDS matrices that are recursive-like and quasi-involutory.
- Implementations and results

Plan

1. Involutory recursive MDS matrices
2. Quasi-involutory recursive-like MDS matrices
3. Implementations

Recursive matrices

From $g(X) = X^m + \sum_{i=0}^{m-1} g_i X^i \in \mathbb{F}_{2^n}[X]$, we build the matrix :

$$C_g = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & 1 \\ g_0 & g_1 & \dots & g_{m-2} & g_{m-1} \end{pmatrix}$$

Definition

M is a recursive matrix $\Leftrightarrow \exists\ g \in \mathbb{F}_{2^n}[X]$ monic of degree m such that

$$M = C_g^m$$

Companion matrices

$$C_g = \begin{pmatrix} X & \mod & g(X) \\ X^2 & \mod & g(X) \\ & \vdots & \\ X^m & \mod & g(X) \end{pmatrix}$$

Successive powers of companion matrices have a similar description :

$$C_g^i = \begin{pmatrix} X^i & \mod & g(X) \\ X^{i+1} & \mod & g(X) \\ & \vdots & \\ X^{i+m-1} & \mod & g(X) \end{pmatrix}, \forall i \in \mathbb{N}$$

Redundancy matrices of cyclic codes

Let $\mathcal{C}$ be a $[2m, m]_{2^n}$ cyclic code. It has a circulant generator matrix :

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_m & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_m & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & g_0 & g_1 & \dots & g_m \end{pmatrix}$$

Assume $g_m = 1$, this code has a systematic generator matrix shaped as :

$$\tilde{G} = \begin{pmatrix} X^m & \mod & g(X) & 1 & 0 & \dots & 0 \\ X^{m+1} & \mod & g(X) & 0 & 1 & \ddots & 0 \\ & \vdots & & \vdots & \ddots & \ddots & \vdots \\ X^{2m-1} & \mod & g(X) & 0 & \dots & 0 & 1 \end{pmatrix}$$

Involutory recursive MDS matrices ?

- A recursive matrix C_g^m is an involutory matrix if

$$C_g^{2m} = I_m$$

- Construct MDS cyclic codes $\Rightarrow$ BCH codes.

- No element of even order in $\mathbb{F}_{2^n}$ $\Rightarrow$ No BCH code yielding involutory recursive MDS matrix.

Plan

1. Involutory recursive MDS matrices
2. Quasi-involutory recursive-like MDS matrices
3. Implementations

Skewing polynomial rings

Let $\theta : x \mapsto x^{[1]}$ the squaring in $\mathbb{F}_{2^{2m}}$.

Definition

The ring of 2-polynomials, $\mathbb{F}_{2^{2m}}[X, \theta]$, is defined as the set $\{\sum_i a_i X^i,\ a_i \in \mathbb{F}_{2^{2m}}\}$ together with :

- *Addition* : usual polynomial addition.
- *Multiplication*: $X * a = \theta(a) * X = a^{[1]} * X$.

Skewing powers of companion matrices

Let $g\langle X\rangle = X^m + \sum_{i=0}^{m-1} g_i X^i \in \mathbb{F}_{2^{2m}}[X,\theta]$.

Theorem

$$C_g^{[i-1]} C_g^{[i-2]} \dots C_g^{[1]} C_g = \begin{pmatrix} X^i & \bmod_* & g\langle X\rangle \\ X^{i+1} & \bmod_* & g\langle X\rangle \\ & \vdots & \\ X^{i+m-1} & \bmod_* & g\langle X\rangle \end{pmatrix}$$

Definition

M is a recursive-like matrix $\Leftrightarrow \exists\ g \in \mathbb{F}_{2^{2m}}[X,\theta]$ monic of degree m such that

$$M = C_g^{[m-1]} C_g^{[m-2]} \dots C_g^{[1]} C_g$$

Redundancy matrices of 2-cyclic codes

Let $\mathcal{C}$ be a $[2m, m]_{2^{2m}}$ 2-cyclic code. It has a circulant generator matrix :

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_m & 0 & \dots & 0 \\ 0 & g_0^{[1]} & g_1^{[1]} & \dots & g_m^{[1]} & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & g_0^{[m-1]} & g_1^{[m-1]} & \dots & g_m^{[m-1]} \end{pmatrix}$$

Assume $g_m = 1$, this code has a systematic generator matrix shaped as :

$$\tilde{G} = \begin{pmatrix} X^m & \bmod_* & g\langle X\rangle & 1 & 0 & \dots & 0 \\ X^{m+1} & \bmod_* & g\langle X\rangle & 0 & 1 & \ddots & 0 \\ & \vdots & & \vdots & \ddots & \ddots & \vdots \\ X^{2m-1} & \bmod_* & g\langle X\rangle & 0 & \dots & 0 & 1 \end{pmatrix}$$

Quasi-involutory Recursive-like MDS matrices

A recursive-like matrix is a quasi-involutory matrix if

$$C_g^{[2m-1]}C_g^{[2m-2]}\dots C_g^{[1]}C_g = I_m$$

$$\left(C_g^{[m-1]}C_g^{[m-2]}\dots C_g^{[1]}C_g\right)^{[m]}(C_g^{[m-1]}C_g^{[m-2]}\dots C_g^{[1]}C_g) = I_m$$

g yields a quasi-involutory recursive-like matrix if

$$X^{2m} - 1 \bmod {}_*g\langle X\rangle = 0$$

There exist $[2m, m]_{2^{2m}}$ 2-cyclic MDS matrix whose a redundancy matrix of a systematic generator matrix is quasi-involutory.

2-cyclic Gabidulin codes

Let λ be a normal element in $\mathbb{F}_{2^{2m}}$. The following matrix is the parity-check matrix of a Maximum Rank Distance (thus MDS) 2-cyclic code, $\mathcal{C}$:

$$H_\lambda = \begin{pmatrix} \lambda^{[0]} & \lambda^{[1]} & \dots & \lambda^{[2m-1]} \\ \lambda^{[1]} & \lambda^{[2]} & \dots & \lambda^{[0]} \\ \vdots & \ddots & \ddots & \vdots \\ \lambda^{[m-1]} & \lambda^{[m]} & \dots & \lambda^{[m-2]} \end{pmatrix}$$

All roots of g unique monic polynomial generating $\mathcal{C}$ are roots of $X^{2m} - 1 \Rightarrow X^{2m} - 1 \bmod {}_* g\langle X \rangle = 0$.

Thus g yields a quasi-involutory recursive-like matrix.

Direct Construction

1. Choose a normal element $\lambda \in \mathbb{F}_{2^{2m}}$.
2. Define

$$H_{\lambda,1} = \begin{pmatrix} \lambda^{[0]} & \dots & \lambda^{[m-1]} \\ \vdots & \ddots & \vdots \\ \lambda^{[m-1]} & \dots & \lambda^{[2m-2]} \end{pmatrix} \text{ and } H_{\lambda,2} = \begin{pmatrix} \lambda^{[m]} & \dots & \lambda^{[2m-1]} \\ \vdots & \ddots & \vdots \\ \lambda^{[2m-1]} & \dots & \lambda^{[m-2]} \end{pmatrix}$$

3. Compute $H_\lambda = (H_{\lambda,1} \mid H_{\lambda,2})$
4. Compute $M = H_{\lambda,2} H_{\lambda,1}^{-1}$. The inverse matrix is $N = M^{[m]}$.
5. Compute C_g from the first line of M.

M is then a quasi-involutory recursive-like MDS matrix, recursively generated by C_g.

An example with small parameters $m = 4$

Let β be a a root of the irreducible polynomial $x^8 + x^4 + x^3 + x^2 + 1$ (`0x11c`). β is a generator of the multiplication group of $\mathbb{F}_{2^8}$.

- We chose to consider the normal element $\lambda = \beta^{21}$.
- We compute $H_{\beta^{21}}$:

$$\begin{pmatrix} \beta^{21} & \beta^{42} & \beta^{84} & \beta^{168} & \beta^{81} & \beta^{162} & \beta^{69} & \beta^{138} \\ \beta^{42} & \beta^{84} & \beta^{168} & \beta^{81} & \beta^{162} & \beta^{69} & \beta^{138} & \beta^{21} \\ \beta^{84} & \beta^{168} & \beta^{81} & \beta^{162} & \beta^{69} & \beta^{138} & \beta^{21} & \beta^{42} \\ \beta^{168} & \beta^{81} & \beta^{162} & \beta^{69} & \beta^{138} & \beta^{21} & \beta^{42} & \beta^{84} \end{pmatrix}$$

- Hence the MDS matrix M is written :

$$M = \begin{pmatrix} \beta^{199} & \beta^{96} & \beta^{52} & \beta^{123} \\ \beta^{190} & \beta^{218} & \beta^{231} & \beta^{125} \\ \beta^{194} & \beta^{227} & \beta^{224} & \beta^{66} \\ \beta^{76} & \beta^{54} & \beta^{217} & \beta^{28} \end{pmatrix}$$

An example with small parameters $m = 4$

- Its inverse matrix is $N = M^{[4]}$ and is written :

$$N = \begin{pmatrix} \beta^{124} & \beta^{6} & \beta^{67} & \beta^{183} \\ \beta^{235} & \beta^{173} & \beta^{126} & \beta^{215} \\ \beta^{44} & \beta^{62} & \beta^{14} & \beta^{36} \\ \beta^{196} & \beta^{99} & \beta^{157} & \beta^{193} \end{pmatrix}$$

- The companion matrix which recursively generates M is associated with $g\langle X\rangle = \beta^{199} + \beta^{96}X + \beta^{52}X^2 + \beta^{123}X^3 + X^4$ and is written :

$$C_g = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \beta^{199} & \beta^{96} & \beta^{52} & \beta^{123} \end{pmatrix}$$

Plan

1. Involutory recursive MDS matrices
2. Quasi-involutory recursive-like MDS matrices
3. Implementations

Normal Basis and Squaring

Let α be a normal element in $\mathbb{F}_{2^{2m}}$. $\mathcal{B} = \{\alpha, \alpha^{[1]}, ..., \alpha^{[2m-1]}\}$ is a basis of $\mathbb{F}_{2^{2m}}$ as $\mathbb{F}_2$-space.

In such a basis, squaring consists in a cycling shift of the components of the vector representation :

$$X = \sum_{i=0}^{1m-1} x_i \alpha^{[i]} \Longrightarrow X^{[1]} = \sum_{i=0}^{2m-1} x_i \alpha^{[i+1]}$$

Thus, it admits an efficient hardware implementation : fixed bits permutation.

Implementing recursive-like matrices

Implementing matrix-vector product with a recursive-like matrix is quite similar as classical case. The following algorithm computes it :

Algorithm 1 Matrix vector product

Require: $\mathbf{x} \in \mathbb{F}_{2^{2m}}^{m}$ an input vector and C_g

Ensure: $\mathbf{y} = M\mathbf{x}$, with $M = C_g^{[m-1]} C_g^{[m-2]} \ldots C_g^{[1]} C_g$

1: $\mathbf{y} \leftarrow \mathbf{x}^{[1]}$ ▷ Initialization

2: **for** $i = 0$ to $m - 1$ **do**

3: $\quad \mathbf{y} \leftarrow C_g \mathbf{y}^{[-1]}$ ▷ Matrix-vector product with companion matrix

4: **end for**

5: $\mathbf{y} \leftarrow \mathbf{y}^{[m-1]}$ ▷ Final step

6: **return** $\mathbf{y}$

And the inverse ?

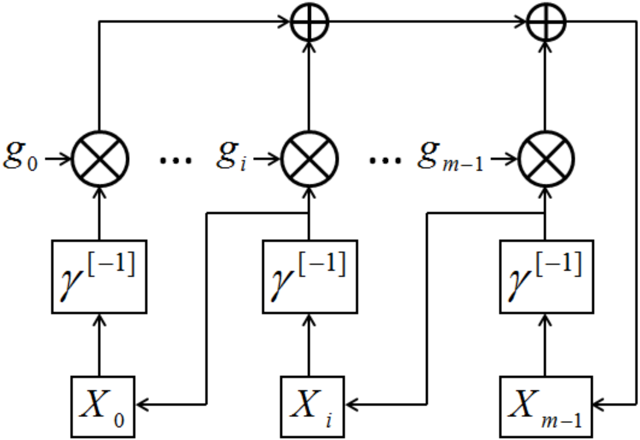
Algorithm 2 Matrix-vector product for the inverse matrix

Require: $\mathbf{x} \in \mathbb{F}_{2^{2m}}^m$ an input vector and C_g

Ensure: $\mathbf{y} = M^{-1}\mathbf{x}$, with $M = C_g^{[m-1]} C_g^{[m-2]} \dots C_g^{[1]} C_g$

1: $\mathbf{y} \leftarrow \mathbf{x}^{[-m+1]}$ ▷ Initialization
2: **for** $i = 0$ to $m - 1$ **do**
3: $\quad \mathbf{y} \leftarrow C_g \mathbf{y}^{[-1]}$ ▷ Matrix-vector product with companion matrix
4: **end for**
5: $\mathbf{y} \leftarrow \mathbf{y}^{[-1]}$ ▷ Final step
6: **return** $\mathbf{y}$

Skewed-LFSR



Exhaustive search of MDS matrices

matrix type	Matrix Size	Ground Field	XOR Count	Reference
Circulant	3×3	$\mathbb{F}_{2^4}$	$1 + 2 \times 4$	[LS16]
Skewed Recursive	3×3	$\mathbb{F}_{2^4}$	$3 + 2 \times 4$	this work
Circulant	4×4	$GL(4, \mathbb{F}_2)$	$3 + 3 \times 4$	[LW16]
Circulant	4×4	$\mathbb{F}_{2^4}$	$3 + 3 \times 4$	[LW16]
Skewed Recursive	4×4	$\mathbb{F}_{2^4}$	$6 + 3 \times 4$	this work
Circulant	6×6	$\mathbb{F}_{2^4}$	$12 + 5 \times 4$	[LS16]

Table: Best known MDS matrices with $\mathbb{F}_{2^4}$ elements

Exhaustive search of Involutory MDS matrices

matrix type	Matrix Size	Ground Field	XOR Count	Reference
Circulant	3×3	$\mathbb{F}_{2^4}$	$12 + 2 \times 4$	[LS16]
Skewed Recursive	3×3	$\mathbb{F}_{2^4}$	$12 + 2 \times 4$	this work
Circulant	4×4	$GL(4, \mathbb{F}_2)$	$5 + 3 \times 4$	[LW16]
Skewed Recursive	4×4	$\mathbb{F}_{2^4}$	$13 + 3 \times 4$	this work
Skewed Recursive	6×6	$\mathbb{F}_{2^4}$	$17 + 5 \times 4$	this work

Table: Best known Involutory MDS matrices with $\mathbb{F}_{2^4}$ elements

Conclusion

- An algebraic framework to understand recursive and recursive-like matrices.
- A new direct construction of MDS matrices with interesting implementation properties.
- A new promising architecture : the SLFSR.