ESTABLISHING CONDITIONS FOR DIFFUSION MATRICES

NGUYEN DINH THUC
Faculty of Information Technology
University of Science, Ho Chi Minh City, Viet Nam
{ndthuc@fit.hcmuns.edu.vn}

NGUYEN THANH BINH
Faculty of Mathematics and Computer Science
University of Science, Ho Chi Minh City, Viet Nam
{ntbinh@math.hcmuns.edu.vn}

Various cryptosystems have used nonsingular matrices for their key rounds. The security and/or speed of such as cryptosystems depend on the diffusion degree of the matrices. In this work, we consider the diffusion formulary of Daemen and Ridijnen and establish conditions for the diffusion matrix. Based on these conditions, we propose an algorithm to generate a diffusion matrix that has degree of diffusion greater than 2.

1. Introduction

In this part, we re-present the formulary which has been presented in [1] and give some notions which will be used in this paper.

Given M is an n×n nonsingular matrix in the field Z_p and a column vector:

$$X = \begin{bmatrix} x_1 \\ x_2 \\ \\ x_n \end{bmatrix}$$

We define:

- $wt(X) = card\{x_i \neq 0, i = 1...n\}$.
- $dwt(X) = card\{x_i = 0, i = 1...n\}$.

We have, $dwt(X) + wt(X) = n.$

Diffusion degree of matrix M is defined by:

$$d(M) = \min_{\vec{X} \neq 0}\{wt(X_{n\times1}) + wt(M_{n\times n}.X_{n\times1})\}$$

Matrix M is called nontrivial diffusion matrix if its diffusion degree $d(M) > 2$; otherwise, M is trivial diffusion matrix.

Various cryptosystems, e.g. Hill/matrix-cipher [2,3], DES [4], AES [5],…, use nonsingular matrices as a main component in their encryption/decryption process. The security of cryptosystems which use the diffusion matrices in their key rounds requires the diffusion degrees of these matrices are greatest as possible. In this paper, we establish conditions for the existence of nontrivial diffusion matrices and propose a generic method to generate these nontrivial diffusion matrices.

2. Conditions for diffusion matrix

Proposition 1. $2 \le d(M) \le n+1$, where M is an n×n nonsingular matrix.

Proof. Since M is nonsingular, the equation

$$M_{n\times n}.X_{n\times1} = 0_{n\times1} \leftrightarrow X_{n\times1} = 0_{n\times1}$$

It implies that $wt(M.X) \ge 1, \forall X \neq \vec{0}$.

Hence, $wt(X_{n\times1}) + wt(M_{n\times n}.X_{n\times1}) \ge 1+1 = 2, \forall X \neq \vec{0}$.

Besides, $wt(M.X) \le n$.

Let X_0 such that $wt(X_0) = 1$. We have:

$d(M) \le wt(X_0) + wt(M.X_0) \le 1+n$.

Then, $2 \le d(M) \le n+1$.

□

Theory 1.

Suppose that $rank(M) = r$. The generic solution of the following equation

$$M_{n\times n}.X_{n\times1} = 0$$

has the form:

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix} = x_{f_1}.h_1 + x_{f_2}.h_2 + \dots + x_{f_{n-r}}.h_{n-r}$$

where $x_{f_1}, x_{f_2}, \dots, x_{f_{n-r}}$ are the free variables and where $h_1, h_2, \dots, h_{n-r}$ are $n \times 1-$columns that represent particular solutions of the system. As the free variables x_{f_i} range over all possible values, the general solution generates possible solutions.

Proof. It is easy to prove by Gauss-Jordan method, and the definition of the rank of a matrix.

□

Proposition 2.

$$\min_{X \neq 0} \left\{ wt\left(X_{n\times1}\right) \middle| M_{n\times n}.X_{n\times1} = 0 \right\} \leq rank(M) + 1.$$

Proof.

According to theory 1, the generic solution of the equation:

$$M_{n\times n}.X_{n\times1} = 0 \ (*)$$

has the form:

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix} = x_{f_1}.h_1 + x_{f_2}.h_2 + \dots + x_{f_{n-r}}.h_{n-r}$$

We consider two cases:

- _rank (M)= n:_ it is trivial to imply the goal.
- _rank (M)= r < n:_

So let $x_{f_2} = x_{f_3} = \dots = x_{f_{n-r}} = 0, x_{f_1} = 1$, we have a solution X_0 of (*).

Then, $wt(X_0) \leq n - (n - r - 1) = r + 1$.

□

We note the following properties of matrix M:

- $T(k)$: $\forall\ 1 \leq k_1 < k$, all square sub-matrices, generated by k_1 columns and k_1 rows in M, are invertible.
- $G(k)$: $\forall\ 1 \leq k_1 < k,\ \exists\ j, k_1 \leq j \leq n + 1 - k + k_1$, all $j \times j$ sub-matrices, generated by j columns and j rows in M, are invertible.
- $H(k)$: $\forall\ 1 \leq k_1 < k,\ \exists\ j, k_1 \leq j \leq n + 1 - k + k_1$, all $j \times j$ sub-matrices, generated by j columns and j rows in M, satisfy this inequality: $rank(A_{j\times j}) \geq k_1$.
- $L(k)$: $\forall\ 1 \leq k_1 < k,\ \exists\ j, k_1 \leq j \leq n + 1 - k + k_1$, all $j \times j$ sub-matrices, generated by j columns and j rows in M, satisfy this inequality: $rank(A_{j\times j}) \geq k_1 + j - n - 1$.

Proposition 3. Suppose that M is an $n \times n$ matrix in the field Z_p, $2 \leq k \leq n+1$. Then, if M has the property $G(k)$, $d(M) \geq k$.

Proof.

Suppose that M has the property $G(k)$.

Let $1 \leq k_1 < k$ and X is a vector satisfying that $wt(X) = k_1$.

We will prove: $wt(M.X) \geq k - k_1$.

Otherwise, we suppose that: $wt(M.X) \leq k - k_1 - 1$.

Then, $dwt\left(M.X\right) \geq n + 1 - k + k_1$.

Since M has the property $G(k)$, $\exists\ j_0, k_1 \leq j_0 \leq n + 1 - k + k_1$, all $j_0 \times j_0$ sub-matrices, generated by j_0 columns and j_0 rows in M, are invertible.

So: $dwt\left(M.X\right) \geq n + 1 - k + k_1 \geq j_0$.

It means that there exist the rows $d_1 < d_2 < \dots < d_{j_0}$ so that:

$$\begin{pmatrix} row\ d_1 \\ row\ d_2 \\ \dots \\ row\ d_{j_0} \end{pmatrix}_{j_0\times n} .X_{n\times1} = \begin{pmatrix} row\ d_1 \\ row\ d_2 \\ \dots \\ row\ d_{j_0} \end{pmatrix}_{j_0\times n} . \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \dots \\ 0 \end{pmatrix}_{j_0\times1}$$

Since $wt(X) = k_1$, it exists $c_1 < c_2 < \dots < c_{k_1}$ so that $x_i \neq 0 \leftrightarrow i \in \left\{c_1, \dots, c_{k_1}\right\}$. (*)

We choose: $c_{k_1+1}, \dots, c_{j_0} \in \{1, .., n\} / \{c_1, \dots, c_{k_1}\}$.

Suppose that $A_{j_0\times j_0}$, generated by the rows $d_1, \dots, d_{j_0}$ and the columns $c_1, \dots, c_{j_0}$.

We also imply that:

$$A_{j_0\times j_0}.\begin{pmatrix} x_{c_1} \\ x_{c_2} \\ \dots \\ x_{c_{j0}} \end{pmatrix}_{j_0\times 1} = \begin{pmatrix} 0 \\ 0 \\ \dots \\ 0 \end{pmatrix}_{j_0\times 1}$$

Since M has the property $G(k)$, $A_{j_0\times j_0}$ is an invertible matrix.
So, we have:

$$\begin{pmatrix} x_{c_1} \\ x_{c_2} \\ \dots \\ x_{c_{j0}} \end{pmatrix}_{j_0\times 1} = \begin{pmatrix} 0 \\ 0 \\ \dots \\ 0 \end{pmatrix}_{j_0\times 1}$$

It completely contradicts to (*).
Thus, $wt(M.X) \geq k - k_1$.

It implies that: $wt\left(X_{n\times 1}\right) + wt\left(M_{n\times n}.X_{n\times 1}\right) \geq k$, all X.

We have: $d(M) \geq k$.

□

Proposition 4. Suppose that M is an $n\times n$ matrix in the field Z_p, $2 \leq k \leq n+1$. If M has the property $T(k)$, $d(M) \geq k$.

Proof. It is derived from proposition 3.

□

Proposition 5. Suppose that M is an $n\times n$ matrix in the field Z_p, $2 \leq k \leq n+1$. If $d(M) \geq k$, then M has the property $H(k)$.

Proof.
Suppose M is a matrix satisfying: $d(M) \geq k$.
We need to prove: M has the property $H(k)$.
On the contrary, M does not satisfy $H(k)$.
So, it implies that $\exists\ 1 \leq k_1 < k$, $\forall\ j, k_1 \leq j \leq n+1-k+k_1$, there is a $j\times j$ sub-matrix, generated by j columns and j rows in M, satisfying : $rank(A_{j\times j}) \leq k_1 - 1$.

Since $rank(A_{j\times j}) \leq k_1 - 1 < j$, $A_{j\times j}$ is singular.

According to theory 1, the equation:

$$A_{j\times j}.X_{j\times 1} = 0_{j\times 1}$$

has the nontrivial solution $X_0 = \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_j \end{pmatrix}$ satisfying that :

$$1 \leq wt\left(X_0\right) \leq rank(A_{j\times j}) + 1$$

Suppose that $A_{j\times j}$, generated by the rows $d_1, ..., d_j$ and the columns $c_1, ..., c_j$.

Choosing $Y = \begin{pmatrix} y_1 \\ y_2 \\ \dots \\ y_n \end{pmatrix}$ so that $y_{c_i} = x_i, \forall i \in \{1,..,j\}$, and $y_i = 0, \forall i \in \{1,...,n\} / \{c_1,...,c_j\}$.

Then, $dwt(M_{n\times n}.Y_{n\times 1}) \geq j$ and $wt(Y_{n\times 1}) = wt(X_{j\times 1})$

We have: $wt(M_{n\times n}.Y_{n\times 1}) \leq n - j$.

Thus,

$wt\left(Y_{n\times 1}\right) + wt\left(M_{n\times n}.Y_{n\times 1}\right) \leq wt(X_{j\times 1}) + n - j$

$\leq rank(A_{j\times j}) + 1 + n - j$

, all j, $k_1 \leq j \leq n+1-k+k_1$.

We imply that:

$d(M) \leq rank(A_{j\times j}) + 1 + n - j, \forall\ j, k_1 \leq j \leq n+1-k+k_1$.

By choosing $j = n+1-k+k_1$, we have:

$d(M) \leq rank(A_{j\times j}) + 1 + n - (n+1-k+k_1)$

$\leq rank(A_{j\times j}) + k - k_1$.

Since $rank(A_{j\times j}) \leq k_1 - 1$, we result that:

$d(M) \leq (k_1 - 1) + k - k_1 = k - 1$.

It is contradict to our supposition, $d(M) \geq k$.

So, we have our goal.

□

Proposition 6. Suppose that M is an $n\times n$ matrix in the field Z_p, $2 \leq k \leq n+1$. If $d(M) \geq k$, then M has the property $L(k)$.

Proof.

Suppose M is a matrix so that $d(M) \geq k$.

We have to prove M has the property $L(k)$.

In fact, suppose that M does not satisfy $L(k)$.

So, it implies that:

$\exists\ 1 \leq k_1 < k,\ \forall\ j, k_1 \leq j \leq n+1-k+k_1$, there is a $j \times j$ sub-matrix, generated by j columns and j rows in M, satisfying: $rank(A_{j\times j}) \leq k_1 + j - n - 2$.

Since $rank(A_{j\times j}) \leq k_1 + j - n - 2 < j$, $A_{j\times j}$ is singular.

According to theory 1, the equation:

$$A_{j\times j}.X_{j\times 1} = 0_{j\times 1}$$

has the nontrivial solution $X_0 = \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_j \end{pmatrix}$ satisfying that:

$$1 \leq wt\left(X_0\right) \leq rank(A_{j\times j}) + 1$$

Suppose that $A_{j\times j}$ is generated by the rows $d_1, \dots, d_j$ and the columns $c_1, \dots, c_j$.

Choosing $Y = \begin{pmatrix} y_1 \\ y_2 \\ \dots \\ y_n \end{pmatrix}$ so that $y_{c_i} = x_i, \forall i \in \{1, \dots, j\}$, and $y_i = 0, \forall i \in \{1,..,n\} / \{c_1, \dots, c_j\}$.

Then, $dwt(M_{n\times n}.Y_{n\times 1}) \geq j$ and $wt(Y_{n\times 1}) = wt(X_{j\times 1})$.

We have: $wt(M_{n\times n}.Y_{n\times 1}) \leq n - j$.

Thus,

$$wt\left(Y_{n\times 1}\right) + wt\left(M_{n\times n}.Y_{n\times 1}\right) \leq wt(X_{j\times 1}) + n - j$$

$$\leq rank(A_{j\times j}) + 1 + n - j$$

all j , $k_1 \leq j \leq n+1-k+k_1$.

We imply that:

$$d(M) \leq rank(A_{j\times j}) + 1 + n - j, \forall\ j, k_1 \leq j \leq n+1-k+k_1 .$$

Since $rank(A_{j\times j}) \leq k_1 + j - n - 2$, we result that:

$$d(M) \leq (k_1 + j - n - 2) + 1 + n - j = k - 1.$$

It is contradict to our supposition, $d(M) \geq k$.

So, we have our goal.

□

Proposition 7. Suppose that M is an $n \times n$ matrix in the field Z_p , $2 \leq k \leq n+1$. Then $d(M) = n+1 \leftrightarrow$ all square sub-matrices, generated by the rows and the columns of M, are invertible.

Proof.

$(\leftarrow)$ Suppose that all square sub-matrices, generated by the rows and the columns of M, are invertible. (*)

Since the largest order of a square sub-matrix of M is n, (*) is equivalent that M has the property $T(n+1)$.

According to proposition 4, we imply that $d(M) \geq n+1$.

Since M is invertible, according to proposition 1, we imply that $d(M) \leq n+1$.

Thus, $d(M) = n+1$.

$(\rightarrow)$ Suppose that $d(M) = n+1$.

It also means that $d(M) \geq n+1$.

According to proposition 5, we have:

$\forall\ 1 \leq k_1 < n+1,\ \exists\ j, k_1 \leq j \leq n+1-(n+1)+k_1 = k_1$, all $j \times j$ sub-matrices, generated by j columns and j rows in M, satisfy this inequality: $rank(A_{j\times j}) \geq k_1$.

It also means that $\forall\ 1 \leq k_1 \leq n,$, all $k_1 \times k_1$ sub-matrices, generated by k_1 columns and k_1 rows in M, satisfying this inequality: $rank(A_{k_1\times k_1}) \geq k_1$, or $rank(A_{k_1\times k_1}) = k_1$.

Thus, all square sub-matrices, generated by the rows and the columns of M, are invertible.

□

3. Generating a nontrivial diffusion matrix

In this section, we will present a generic method that helps us to generate a nontrivial diffusion matrix M. Our method is based all previous conditions in section 2 and the LU factorization [6]. It is easy to prove the following theorem:

Theory 2.

(i) A lower-triangle matrix $L_{n\times n} = (l_{ij})_{n\times n}$ is nonsingular if $\prod_{i=1}^{n} l_{ii} \neq 0$.

(ii) An upper-triangle matrix $U_{n\times n} = (u_{ij})_{n\times n}$ is nonsingular if $\prod_{i=1}^{n} u_{ii} \neq 0$.

(iii) If L and U are nonsingular matrices then A = LU is also nonsingular.

(iv) If A is nonsingular and P is a permutation matrix then PA is also nonsingular.

□

We can use the properties of a lower-triangle matrix L and an upper-triangle matrix U to generate a nontrivial diffusion M, it means $d(M) > 2$.

Let:

$$L = \begin{pmatrix} l_{11} & 0 & \dots & 0 \\ l_{21} & l_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ l_{n1} & l_{n2} & \dots & l_{nn} \end{pmatrix}, U = \begin{pmatrix} u_{11} & u_{12} & \dots & u_{1n} \\ 0 & u_{22} & \dots & u_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & u_{nn} \end{pmatrix}$$

are nonsingular matrices. We have $\prod_{i=1}^{n} l_{ii} \neq 0, \prod_{j=1}^{n} u_{jj} \neq 0$.

We have the following proposition:

Proposition 8.

If both L and U satisfy that:

- $l_{21} = 0; l_{31} + \dots + l_{n1} \neq 0; u_{1j} \neq 0, \forall j \in \{1,..,n\}$.
- $u_{2j} \neq 0; l_{ii}, u_{jj} \neq 0, \forall i, j \in \{1,...,n\}$.

and $M = L.U$, then $d(M) > 2$.

Proof.

We will prove that $d(M) > 2$.

In fact, let X be a $n \times 1$ matrix $X \neq 0_{n\times 1}$.

We consider two following cases:

<u>Case 1:</u> $wt(X) \geq 2$:

Since L, U are nonsingular, M is also nonsingular. Thus, the equation $M.X = 0$ has an only solution X= 0.

It results that: $wt(X) + wt(M.X) \geq 2+1 = 3$, $\forall X \neq 0$.

So, if $wt(X) \geq 2$, $wt(X) + wt(M.X) > 2$.

<u>Case 2:</u> $wt(X) = 1$:

Let $X = \begin{bmatrix} x_1 \\ x_2 \\ \\ x_n \end{bmatrix}$.

Suppose that: $x_i = a \neq 0, x_j = 0, j \neq i \in \{1,..,n\}$.

Then, the product of U and X is **a** times of the i^th column of U.

It means that:

$$U.X = a.\begin{pmatrix} u_{1i} \\ u_{2i} \\ \dots \\ u_{ii} \\ 0 \\ \dots \\ 0 \end{pmatrix}.$$

So:

$$L.(U.X) = a.L.\begin{pmatrix} u_{i1} \\ u_{i2} \\ \dots \\ u_{ii} \\ 0 \\ \dots \\ 0 \end{pmatrix}.$$

$$\rightarrow L.(U.X) = a.\left[u_{1i}.\begin{pmatrix} l_{11} \\ l_{21} \\ \dots \\ l_{i1} \\ \dots \\ \dots \\ l_{n1} \end{pmatrix} + u_{2i}.\begin{pmatrix} 0 \\ l_{22} \\ \dots \\ l_{i2} \\ \dots \\ \dots \\ l_{n2} \end{pmatrix} + \dots + u_{ii}\begin{pmatrix} 0 \\ 0 \\ \dots \\ l_{ii} \\ l_{(i+1)i} \\ \dots \\ l_{ni} \end{pmatrix} \right].$$

$$\rightarrow L.(U.X) = \begin{pmatrix} a.u_{1i}.l_{11} \\ a.\left(u_{1i}.l_{21} + u_{2i}.l_{22}\right) \\ \ldots \\ \ldots \\ \ldots \\ \ldots \\ a.\sum_{j=1}^{i} u_{ji}.l_{nj} \end{pmatrix}.$$

We will consider further two sub-cases:

- $\underline{i = 1}$:

We have: $L.(U.X) = a.u_{11}\begin{bmatrix} l_{11} \\ l_{21} \\ \ldots \\ l_{n1} \end{bmatrix}$.

Since $l_{21} = 0; l_{31} + \ldots + l_{n1} \neq 0; l_{11} \neq 0$, then $wt\left(L.\left(U.X\right)\right) \geq 2$.

So: $wt(X) + wt(M.X) \geq 1 + 2 = 3$.

- $\underline{i \geq 2}$:

We have: $L.(U.X) = \begin{bmatrix} a.u_{1i}.l_{11} \\ a.\left(u_{1i}.l_{21} + u_{2i}.l_{22}\right) \\ \ldots \\ a.\sum_{j=1}^{i} u_{ji}.l_{nj} \end{bmatrix}$.

Since, $l_{21} = 0; u_{1j} \neq 0; u_{2j} \neq 0; l_{ii}, u_{jj} \neq 0, \forall i, j \in \{1, \ldots, n\}$, it results that:

$$L.(U.X) = \begin{bmatrix} a.u_{1i}.l_{11} \\ a.u_{2i}.l_{22} \\ \ldots \\ a.\sum_{j=1}^{i} u_{ji}.l_{nj} \end{bmatrix}$$

and $a.u_{1i}.l_{11}, a.u_{2i}.l_{22} \neq 0$.

So: $wt(X) + wt(M.X) \geq 1 + 2 = 3$.

Thus, $wt(X) + wt(M.X) \geq 3, \forall\ X \neq \vec{0}$.

We result that: $d(M) > 2$.

□

According to the proposition 8, we have the generic method to generate the nontrivial diffusion matrix M as the following:

Input: a lower-triangle matrix L and an upper-triangle matrix U so that:

$$L = \begin{pmatrix} l_{11} & 0 & \ldots & 0 \\ l_{21} & l_{22} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ l_{n1} & l_{n2} & \ldots & l_{nn} \end{pmatrix}, U = \begin{pmatrix} u_{11} & u_{12} & \ldots & u_{1n} \\ 0 & u_{22} & \ldots & u_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & u_{nn} \end{pmatrix}$$

+ $l_{21} = 0; l_{31} + \ldots + l_{n1} \neq 0; u_{1j} \neq 0, \forall j \in \{1, .., n\}$.

+ $u_{2j} \neq 0; l_{ii}, u_{jj} \neq 0, \forall i, j \in \{1, \ldots, n\}$.

Output: $M = L.U$.

4. Conclusion

We succeed in generating a diffusion matrix satisfying the order of diffusion is greater than 2, and analyzing some conditions of a diffusion matrix. It is helpful to improve the quality of the linear cryptosystem.

References

1. J. Daemen, V. Rijmen, ”The wide trial design strategy”, Advances in Cryptology – Eurocrypt 2002.
2. Murray Eisenberg, “Hill cipher: A Linear Algebra Project with Mathematica”, University of Massachusetts, 1999.
3. Sharokh Saeedna, “How to make the Hill cipher secure”, Cryptologia, 24(4), pp 353-360, Oct 2000.
4. Scott Sutherland, “An introduction of cryptography”, MSTP MATH Workshop, 2005.
5. J. Daemen, V. Rijmen, “The design of Rijndael: AES – the advanced encryption standard”, Springer-Verlag, ISBN 3-540-42580-2, 2002.
6. Carl D. Meyer, “Matrix analysis and applied linear algebra”, SIAM, Philadelphia, 2000.