Symmetric Circulant Matrices
and Publickey Cryptography

A. V. Ramakrishna
Department of Mathematics, R.V.R and J.C College of Engineering
Chowdavaram, Guntur-522019, Andhra Pradesh, India
amathi7@gmail.com

T. V. N. Prasanna
Department of Mathematics, NRI Institute of Technology, Visadala
Guntur-522009, Andhra Pradesh, India
tvnp11@gmail.com

Abstract. An important aspect of cryptography with matrices is that given
$N \times N$ matrix $P$ over a field $F$ find a class of matrices $G$ over $F$ such that the
associated doubly circulant matrix $G_c$ is singular in order that the equation
$AGB = P$ in circulant matrices $A, B$ has infinitely many solutions. The aim
of this note is to present such a class of matrices $G$. We also present a direct
method of finding the inverse of a symmetric circulant matrix of order $n$,
$(a \ b\ b \ldots\ b)$ where $a + (n - 1)b \neq 0$.

Keywords: Symmetric circulant matrix, Doubly circulant matrix, Trap-
door function

1. INTRODUCTION

Cryptography enables us to store sensitive information or transmit it across
insecure networks, like the Internet, so that it cannot be read by anyone else
except the intended recipient. Cryptography is the science of using mathe-
matics to encrypt and decrypt messages. In cryptographic terminology, the
original, undisguised message is called plain text or cleartext. Encoding the
contents of the message in such a way that it hides its contents from outsiders is called encryption. The encrypted message is called ciphertext. The process of retrieving the plaintext from the ciphertext is called decryption.

The Principal Goal of (Public Key) Cryptography is to allow two parties to safely exchange confidential information, even if they have communicate only via a channel that is being monitored by an adversary.

Mukhesh Kumar Singh[1] gave an algorithm for public key cryptography using simple multiplication of matrices over a given commutative ring and transformed to the cryptography problem to the matrix equation $AGB = P$ in circulant matrices $A, B$ has infinitely many solutions found and obtained a condition for existence of the solution in terms of $G$ namely that the determinant of the doubly circulant coefficient matrix $G$ is zero. We present a large class of $G$ for which $|G_e|$ is zero.

**Definition 1.1.** An $N \times N$ matrix whose rows are composed of cyclically shifted versions of a length -N list $L$ is called Circulant Matrix.

For example the $3 \times 3$ circulant matrix on the list $L = (a, b, c)$ is

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

The eigen values of the circulant matrix $(a_1, a_2, a_3 ... a_n)$ of order $n$ are given by

$$
\sum_{j=0}^{n-1} a_j \omega^{jk} \text{ for } k = 0, 1, 2, ... n - 1
$$

2. Symmetric Circulant Matrices

**Definition 2.1.** A circulant matrix $A = (a_1, a_2, a_3 ... a_n)$ of order $n$ is symmetric if

(i) $a_{\frac{n}{2}+j} = a_{\frac{n}{2}-(j-2)}$, $2 \leq j \leq \frac{n}{2}$, when $n$ is even

(ii) $a_{\frac{n}{2}+(j+\frac{1}{2})} = a_{\frac{n}{2}+(\frac{3-2j}{2})}$, $1 \leq j \leq \frac{n-1}{2}$, when $n$ is odd.

In particular a circulant matrix $A = (a, b, b ... b)$ of order $n$ is symmetric when $n$ is even (or) odd.

**Theorem 2.2.** For two distinct elements $a, b$ in a field $F$ with $a + (n-1)b \neq 0$ the inverse of symmetric circulant matrix $A = (a, b, b ... b)$ of order $n$ is $A^{-1} = (c, d, d ... d)$ where $c = \frac{a+(n-2)b}{(a-b)(a+(n-1)b)}$ and $d = \frac{-b}{(a-b)(a+(n-1)b)}$.

**Proof.** Using Gauss-Jordan reduction method by writing $A$ and the unit matrix $I$ side by side
Symmetric circulant matrices and publickey cryptography

\[ [A : I] = \begin{bmatrix}
  a & b & b & \ldots & b & : 1 \\
  b & a & b & \ldots & b & : 0 \\
  b & b & a & \ldots & b & : 0 \\
  \vdots & \vdots & \vdots & \ddots & \vdots & : \vdots \\
  b & b & b & \ldots & a & : 0
\end{bmatrix} \]

Operating \( R_1 + R_2 + R_3 + \ldots + R_n \) on \([A : I]\), we get

\[ [A : I] \sim \begin{bmatrix}
  a + (n - 1)b & a + (n - 1)b & a + (n - 1)b & \ldots & a + (n - 1)b & : 1 \\
  b & a & b & \ldots & b & : 0 \\
  b & b & a & \ldots & b & : 0 \\
  \vdots & \vdots & \vdots & \ddots & \vdots & : \vdots \\
  b & b & b & \ldots & a & : 0
\end{bmatrix} \]

Operating \( \frac{R_1}{a + (n-1)b}, R_3 - R_2, R_4 - R_2, \ldots, R_n - R_2 \) successively we get

\[ [A : I] \sim \begin{bmatrix}
  1 & 1 & 1 & \ldots & 1 & : \frac{1}{a + (n-1)b} \\
  b & a & b & \ldots & b & : 0 \\
  0 & b - a & a - b & \ldots & 0 & : 0 \\
  \vdots & \vdots & \vdots & \ddots & \vdots & : \vdots \\
  0 & b - a & 0 & \ldots & a - b & : 0
\end{bmatrix} \]

Continuing this way with a sequence of row operations, we finally get

\[ [A : I] \sim \begin{bmatrix}
  1 & 0 & 0 & \ldots & 0 & : \frac{a + (n-2)b}{(a-b)(a+(n-1)b)} \\
  0 & 1 & 0 & \ldots & 0 & : \frac{-b}{(a-b)(a+(n-1)b)} \\
  0 & 0 & 1 & \ldots & 0 & : \frac{-(a-b)(a+(n-1)b)}{(a-b)(a+(n-1)b)} \\
  \vdots & \vdots & \vdots & \ddots & \vdots & : \vdots \\
  0 & 0 & 0 & \ldots & 1 & : \frac{-b}{(a-b)(a+(n-1)b)}
\end{bmatrix} \]

Therefore \( A^{-1} = \left( \begin{array}{cccc}
  \frac{a + (n-2)b}{(a-b)(a+(n-1)b)} & -b & -b & \ldots & -b \\
  -b & \frac{-b}{(a-b)(a+(n-1)b)} & \frac{-b}{(a-b)(a+(n-1)b)} & \ldots & \frac{-b}{(a-b)(a+(n-1)b)} \\
  \frac{-b}{(a-b)(a+(n-1)b)} & \frac{-b}{(a-b)(a+(n-1)b)} & \frac{-(a-b)(a+(n-1)b)}{(a-b)(a+(n-1)b)} & \ldots & \frac{-b}{(a-b)(a+(n-1)b)} \\
  \end{array} \right) \)

Remark 2.3. The matrix in the above theorem is singular if \( a + (n - 1)b = 0 \).

Remark 2.4. The eigen values of \( A \) in the above theorem are given by \( a + (n - 1)b \) and \( (a - b) \) repeated \( (n - 1) \) times.

3. Symmetric Circulant Matrices in publickey cryptography

**Doubly Circulant Coefficient Matrix:**

The coefficient matrix corresponding to a matrix \( G \) denoted by \( G_c \) is a doubly circulant matrix formed as follows.

Let \([R_1, \ldots, R_n]^t\) be a \( n \times n \) matrix \( G \), \( R_i \) representing the \( i^{th} \) row and \( M_{R_i} \) be the \( n \times n \) circulant matrix obtained by cyclically shifting \( R_i \). Then the doubly circulant matrix \((M_{R_1} \ M_{R_2} \ M_{R_3} \ldots \ M_{R_n})\) is called the coefficient matrix of \( G \).
For example if $G = \begin{bmatrix} a & b \\ b & b \end{bmatrix}$

Then $G_c = (M_{R_1} \ M_{R_2} \ M_{R_3}) = \begin{bmatrix} a & b & b & b & b \\ b & a & b & b & b \\ b & b & a & b & b \\ b & b & b & a & b \\ b & b & b & b & a \end{bmatrix}$

**Trapdoor function:**

If we take two random circulant matrices $A$ of dimension $N \times N$ and $B$ of dimension $M \times M$ and calculate $P = AGB$ where $G$ is an $N \times M$ base matrix, then it is difficult to get $A$ and $B$ from $P$ and $G$ over a chosen ring. Where $F(A, B) = AGB$ serves as a Trapdoor function. In publickey cryptography with matrices in the trapdoor function $P = AGB$, if $G$ is chosen such that doubly circulant matrix $|G_c| = 0$, then it is difficult to find the circulant matrices $A$ and $B$.

For that if we chose our $G$ such that the doubly circulant matrix $G_c$ as symmetric circulant matrix as $(a \ b \ b \ b \ \ldots) \ b$ where $a + (n - 1)b = 0$ then $|G_c| = 0$.

$A = \begin{bmatrix} a_1 & a_2 \\ a_2 & a_1 \end{bmatrix}$, $B = \begin{bmatrix} b_1 & b_2 \\ b_2 & b_1 \end{bmatrix}$, $G = \begin{bmatrix} g_1 & g_2 \\ g_2 & g_2 \end{bmatrix}$

Now $P = AGB$

\[
\begin{bmatrix} p_1 & p_2 \\ p_3 & p_4 \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \\ a_2 & a_1 \end{bmatrix} \begin{bmatrix} g_1 & g_2 \\ g_2 & g_2 \end{bmatrix} \begin{bmatrix} b_1 & b_2 \\ b_2 & b_1 \end{bmatrix}
\]

\[
= \begin{bmatrix} a_1 & a_2 \\ a_2 & a_1 \end{bmatrix} \begin{bmatrix} g_1b_1 + g_2b_2 & g_1b_2 + g_2b_1 \\ g_2b_1 + g_2b_2 & g_2b_2 + g_2b_1 \end{bmatrix}
\]

\[
= \begin{bmatrix} a_1g_1b_1 + a_1g_2b_2 + a_2g_1b_1 + a_2g_2b_2 & a_1g_1b_2 + a_1g_2b_1 + a_2g_2b_2 + a_2g_1b_1 \\ a_2g_1b_1 + a_2g_2b_2 + a_2g_1b_1 + a_2g_2b_2 & a_2g_1b_2 + a_2g_2b_1 + a_2g_2b_2 + a_2g_2b_1 \end{bmatrix}
\]

Writing $x_1 = a_1b_1, x_2 = a_1b_2, x_3 = a_2b_1, x_4 = a_2b_2$ above becomes

\[
\begin{bmatrix} p_1 & p_2 \\ p_3 & p_4 \end{bmatrix} = \begin{bmatrix} g_1x_1 + g_2x_2 + g_2x_3 + g_2x_4 & g_2x_1 + g_1x_2 + g_2x_3 + g_2x_4 \\ g_2x_1 + g_2x_2 + g_1x_3 + g_2x_4 & g_2x_1 + g_2x_2 + g_2x_3 + g_1x_4 \end{bmatrix}
\]

It follows that

$g_1x_1 + g_2x_2 + g_2x_3 + g_2x_4 = p_1$

$g_2x_1 + g_1x_2 + g_2x_3 + g_2x_4 = p_2$

$g_2x_1 + g_2x_2 + g_1x_3 + g_2x_4 = p_3$

$g_2x_1 + g_2x_2 + g_2x_3 + g_1x_4 = p_4$

The above system has an infinite number of solutions for $x_1, x_2, x_3, x_4$ as the determinant of the coefficient matrix is zero. Therefore it is difficult to find the matrices $A$ and $B$ in the trapdoor function.

This method can be extended for any $n$ as follows:
If $g \neq 0$ write $g_1 = g$ and $g_2 = \frac{g}{n^2 - 1}$ for $n > 1$ and $n \times n$ matrix $G = (g_1 \ g_2 \ ... \ g_2)$
Clearly $|G_c| = 0$ where $G_c$ is the coefficient matrix of the system $AXB = P$
so that it has infinitely many solutions $A$ and $B$.

Acknowledgement

The authors are thankful to Prof.I.Ramabhadra Sarma for his valuable comments and suggestions.

References

[1] Mukhesh Kumar Singh Public key Cryptography with Matrices, Proceedings of the
2004 IEEE Workshop on Information Assurance, United states Military Academy,West
Point, NY 10-11 June.
[2] Robert M.Gray Toplitz and Circulant Matrices : A review, Information Systems Lab-
oratory, Department of Electrical Engineering, Stanford University.

Received: April, 2013