DIGITAL SIGNATURE SCHEME USING GOLDEN MATRICES BASED ON MATRIX EXTENSION OF RSA CRYPTOSYSTEM

P. SUNDARAYYA¹, M.G. VARA PRASAD*² AND P. VENKATA RAMANA³

¹Department of Engineering Mathematics, GITAM Deemed to be University, Visakhapatnam, India.
²Department of Mathematics. NSRIT, Visakhapatnam, India.
³Research Scholar, Department of Engineering Mathematics, GITAM Deemed to be University, Visakhapatnam, India.

(Received On: 19-04-19; Revised & Accepted On: 12-06-19)

ABSTRACT

A.P. Stakhov in [6] proposed the concepts golden matrices and new kind of cryptography. In this paper, we propose a digital signature scheme using Golden matrices based on Matrix extension of RSA Cryptosystem. This proposed work is very rapid fast and simple for technical recognition and can be used for signature protection of digital signals like telecommunication and measurement system.

Keywords: signature scheme, golden matrices, factoring Matrix extension of RSA problem, golden digital signature.

2010 Mathematics Subject Classification: 11T71, 14G50. 68P25.

1. INTRODUCTION

In the last decades the theory of Fibonacci numbers was complemented by the theory of the so-called Fibonacci Q-matrix [1].

This $2 \times 2$ square matrix is defined as

\[ Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \]  \hspace{1cm} (1)

The $k$th power of the Q-matrix can be defined as

\[ Q^k = \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix} \]  \hspace{1cm} (2)

\[ \text{Det}(Q^k) = F_{k+1}F_{k-1} - F_k^2 = (-1)^k \quad \text{where} \quad k = 0, \pm 1, \pm 2, \cdots \]  \hspace{1cm} (3)

$F_k$ is $k$th Fibonacci number and recurrence relation

\[ F_{k+1} = F_k + F_{k-1} \]  \hspace{1cm} (4)

Identity (4) is called “Cassini formula” with terms the initial $F_1 = F_2 = 1$.

Identity (4) generates the Fibonacci numbers 1, 1, 2, 3, 5, 8, 13….and it can be used to

\[ F_{-k} = (-1)^{k+1}F_k \]

2. SOME PROPERTIES OF THE Q-MATRIX

\[ Q^k = \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix} = \begin{pmatrix} F_k + F_{k-1} & F_{k-1} + F_{k-2} \\ F_{k-1} + F_{k-2} & F_{k-2} + F_{k-3} \end{pmatrix} = \begin{pmatrix} F_k & F_{k-1} \\ F_{k-1} & F_{k-2} \end{pmatrix} + \begin{pmatrix} F_{k-1} & F_{k-2} \\ F_{k-2} & F_{k-3} \end{pmatrix} \]  \hspace{1cm} (5)

\[ Q^kQ^l = Q^{k+l} \]  \hspace{1cm} (6)

In [11], introduced and proved symmetrical hyperbolic Fibonacci functions

\[ F_k = \begin{cases} \alpha F_x(k), & \text{if } k = 2x \\ \gamma F_x(k), & \text{if } k = 2x + 1 \end{cases} \]  \hspace{1cm} (7)
Symmetrical hyperbolic Fibonacci sine: \( s_F(k) = \frac{\tau^k - \tau^{-k}}{\sqrt{5}} \) (8)

Symmetrical hyperbolic Fibonacci cosine: \( c_F(k) = \frac{\tau^k + \tau^{-k}}{\sqrt{5}} \) (9)

Where the Golden Proportion \( \tau = \frac{1 + \sqrt{5}}{2} \)

By using (3) generalization of the Cassini formula

\[
[s_F(k)]^2 - c_F(k+1)c_F(k-1) = -1
\]

\[
[c_F(k)]^2 - s_F(k+1)s_F(k-1) = 1
\]

3. THE “GOLDEN” MATRICES

A.P.Stakhov [6] developed a theory of the golden matrices that are a generalization of the matrix (2) for continuous domain. He defined the golden matrices in the terms of the symmetrical hyperbolic Fibonacci function (7) and (8). The golden matrices that are the functions of the continuous variable \( x \) are the following form.

\[
Q_{2x} = \begin{pmatrix}
  c_F(2x+1) & s_F(2x) \\
  s_F(2x) & c_F(2x)
\end{pmatrix}
\]

(12)

\[
Q_{2x+1} = \begin{pmatrix}
  s_F(2x+2) & c_F(2x+1) \\
  c_F(2x+1) & s_F(2x)
\end{pmatrix}
\]

(13)

A.P.Stakhov [6] obtained inverse matrices of (11) and (12). The inverse golden matrices that are the functions of the continuous variable \( x \) are the following form.

\[
Q_{-2x} = \begin{pmatrix}
  s_F(2x-1) & -c_F(2x) \\
  -s_F(2x) & c_F(2x)
\end{pmatrix}
\]

(14)

\[
Q_{-(2x+1)} = \begin{pmatrix}
  -s_F(2x) & c_F(2x+1) \\
  c_F(2x+1) & -s_F(2x+2)
\end{pmatrix}
\]

(15)

Table: Represents the “direct matrices \( Q^k \)” and their “inverse matrices \( Q^{-k} \)”

<table>
<thead>
<tr>
<th>( k )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>( Q_1^k )</td>
<td>1 0</td>
<td>1 0</td>
<td>2 1</td>
<td>3 2</td>
<td>5 3</td>
</tr>
<tr>
<td>( Q_1^{-k} )</td>
<td>1 0</td>
<td>0 1</td>
<td>1 1</td>
<td>2 1</td>
<td>3 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continue this process \( k = 5, 6, 7,.... \)

In [6] the golden matrices were used for creation of a new kind of cryptography called the golden cryptography. In this paper, we propose a digital signature based on Matrix extension of RSA Cryptosystem and golden matrices.

4. PROPOSED TECHNIQUE

In [6] the golden matrices were used for creation of a kind of cryptography is called the golden cryptography. In this paper, we propose a digital signature based on Matrix extension of RSA Cryptosystem and golden matrices.

4.1 Digital signature based on Matrix extension of RSA Cryptosystem

It was proved in [10] that following theorem

Let \( n = p q \) where \( p \) and \( q \) are distinct prime numbers, let \( M \in GL_2(\mathbb{Z}_n) \) be a matrix made up of nonnegative integers less than \( n \).

Let \( g_p = |GL_2(\mathbb{Z}_n)| = (p^2 - 1)(p^2 - p) \), \( g_q = |GL_2(\mathbb{Z}_n)| = (q^2 - 1)(q^2 - q) \) and define \( g = g_p g_q \). Further let \( e, d \in \mathbb{Z}^+ \) such that \( ed = 1 \) (mod \( g \)). Thus the public key and secret keys are “e” and “d” respectively.

We have introduced the “golden” direct and inverse matrices and allow us to develop the following application to digital signature.

Let the initial message \( M \) be a digital signal which are having readings as follows.

\[
m_1 m_2 m_3 m_4 m_5 m_6 m_7 m_8 m_9 \ldots \ldots \in \mathbb{Z}_n^*
\]

(16)

There are many examples of the “digital signals” (16): digital telephony, digital TV, measurement systems and so on.
The problem of protecting the “digital signal” (16) from the hackers is solved usually with application of digital signature methods. Consider a new signature method based on the “golden” matrices.

Let \( M = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} \) \quad (17)

Let \( M \) be an initial matrix can be considered as message matrix, \( m_1, m_2, m_3, m_4 \) readings are less than \( n \)

4.2 Algorithm for signing message:
Note that there are 24 variants (permutations) to form the matrix (17) from the four readings. Let us designate the \( i^{th} \) permutation by \((i = 1, 2, ..., 24)\). The first step of signature protection of the four readings \( m_1, m_2, m_3, m_4 \) is a choice of the permutation \( p_i \).

Let us consider now the following signing algorithms based on matrix multiplication. Here is the message (17) that is formed according to the permutation \( p_i \).

\[
\text{Signing: } S_i(x) = M^d Q^{2x} \pmod{n} \quad (18)
S_2(x) = M^d Q^{2x+1} \pmod{n} \quad (19)
\]

where \( Q^{2x} \) \((12)\) and \( Q^{2x+1} \) \((13)\) are signature matrices.

We can use the variable \( x \) as a signature key or private key. This means that in dependence on the value of the key \( x \) there is an infinite number of transformation of the message \( M \) into signature.

4.3 Algorithm for verification message:

\[
[S_i(x)Q^{-2x}]^e \equiv M \pmod{n} \quad (20)
[S_2(x)Q^{-(2x+1)}]^e \equiv M \pmod{n} \quad (21)
\]

Where \( Q^{-2x} \) \((14)\) and \( Q^{-(2x+1)} \) \((14)\) are verification matrices.

Let us consider the transformation for the above case when we choose the “golden” matrix \((12)\) as the digital matrix.

For the given value of the digital signature key \( x = \alpha \) the “golden” digital can be represented as follows:

**Signing:**

Suppose that \( M^d = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}^d \equiv \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \pmod{n} \)

Now \( M^d Q^{2x} = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \begin{pmatrix} F_2(2a+1) & sF_3(2a) \\ F_3(2a) & cF_3(2a-1) \end{pmatrix} \)
\[
= \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix} \pmod{n} = S_1(a) \quad (22)
\]

where
\[
s_{11} = c_1 F_2(2a+1) + c_2 sF_3(2a) \quad (23)
\]
\[
s_{12} = c_1 sF_3(2a) + c_2 F_3(2a-1) \quad (24)
\]
\[
s_{21} = c_3 F_2(2a+1) + c_4 sF_3(2a) \quad (25)
\]
\[
s_{22} = c_3 sF_3(2a) + c_4 F_3(2a-1) \quad (26)
\]

**Verification:**

\[
[S_1(a)Q^{-2a}]^e \equiv \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix} \begin{pmatrix} F_3(2a-1) & -sF_3(2a) \\ -sF_3(2a) & cF_3(2a+1) \end{pmatrix}^e \equiv \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix} \pmod{n} \quad (27)
\]

where
\[
v_{11} = s_{11} F_3(2a-1) - s_{12} sF_3(2a) \quad (28)
\]
\[
v_{12} = -s_{11} sF_3(2a) + s_{12} F_3(2a+1) \quad (29)
\]
\[
v_{21} = s_{21} F_3(2a-1) - s_{22} sF_3(2a) \quad (30)
\]
\[
v_{22} = -s_{21} sF_3(2a) + s_{22} F_3(2a+1) \quad (31)
\]

For calculation of the matrix element given by \((28)\) we can use the \((23)\) and \((24)\). Then we get
\[
v_{11} = [c_1 F_3(2a+1) + c_2 sF_3(2a)] cF_3(2a+1) - [c_1 sF_3(2a) + c_2 F_3(2a-1)] sF_3(2a) \]
\[
= c_1 [cF_3(2a+1) F_3(2a-1) - sF_3(2a)]^2 + c_2 [sF_3(2a) cF_3(2a-1) - F_3(2a-1) sF_3(2a)] \quad (32)
\]

Using the identity \((8)\) we can write the expression \((32)\) as follows:
\[
v_{11} = c_1 x + c_2 x = c_1 \]

© 2019, IJMA. All Rights Reserved 65
In this way using the identity (8) and (9) we can calculate remaining matrix elements (29) - (31)

\[ v_{12} = c_2, \ v_{21} = c_3, \ v_{22} = c_4 \]

Then

\[
\begin{bmatrix}
S_1(a)Q^{-2a} \end{bmatrix}^e = \begin{bmatrix}
v_{11} & v_{12} \\
v_{21} & v_{22} \\
\end{bmatrix}^e (mod \ n) \\
\begin{bmatrix}
c_1 & c_2 \\
c_3 & c_4 \\
\end{bmatrix}^e (mod \ n) \\
= \begin{bmatrix}
m_1 & m_2 \\
m_3 & m_4 \\
\end{bmatrix}^d (mod \ n) \\
= M^d (mod \ n) \\
= M (mod \ n) \\
\end{bmatrix}
\]

\[ [S_1(a)Q^{-2a}]^e = M (mod \ n) \] (33)

5. EXAMPLE

Let \( p = 5, q = 7, n = 35, g_p = (p^2 - 1)(p^2 - p) = 480, g_q = (q^2 - 1)(q^2 - q) = 2016 \) and \( g = g_pg_q = 967680, e = 199 \) such that \( g.c.d (199, 967680) = 1 \) and \( 199 \times d = 1 (mod \ 967680) \) then \( d = 34039 \), choose \( x = 10 \)

\[ Q^{2x} = Q^{20} = \begin{bmatrix} 10946 & 6765 \\ 6765 & 4181 \end{bmatrix} \] and \( Q^{-2x} = Q^{-20} = \begin{bmatrix} 4181 & -6765 \\ -6765 & 10946 \end{bmatrix} \)

Let \( m_1 = 2, m_2 = 5, m_3 = 1, m_4 = 3, \) clearly \( m_1, m_2, m_3, m_4 < 35 \)

\[ : M = \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix} \]

Compute \( M^d = \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix}^{34039} (mod \ 35) = \begin{bmatrix} 8 & 15 \\ 24 & 32 \end{bmatrix} (mod \ 35) \)

Signature:

\[ M^dQ^{2x} = M^{34039}Q^{20} = \begin{bmatrix} 8 & 15 \\ 24 & 32 \end{bmatrix} \begin{bmatrix} 10946 & 6765 \\ 6765 & 4181 \end{bmatrix} (mod \ 35) = \begin{bmatrix} 8 & 15 \\ 24 & 32 \end{bmatrix} (mod \ 35) \]

Verifications:

\[ [S_1(a)Q^{-2a}]^e = [S_1(10)Q^{-20}]^{199} = \begin{bmatrix} 10946 & 6765 \\ 6765 & 4181 \end{bmatrix}^{199} (mod \ 35) = \begin{bmatrix} 8 & 15 \\ 24 & 32 \end{bmatrix} (mod \ 35) = M \]

6 PERFORMANCE EVALUATION

We use the following notation to analyze the performance of the proposed technique:

\( T_{sign} \) is the full signature time, \( T_{ver} \) is full verification time, \( T_{exp} \) is the time for a modular exponentiation, \( T_{add} \) is the time of modular addition, \( T_{mul} \) is the time modular multiplication.

If we consider expressions (22) to (26), we can write the expressions for a full signature time

\[ T_{sign} = 4T_{add} + 8T_{mul} + T_{exp} \] (34)

If we consider expressions (27) to (31), we can write the expressions for a full verification time

\[ T_{ver} = 4T_{add} + 8T_{mul} + T_{exp} \] (35)

Analysis of the expressions (34) and (35) show that the golden signature is fast signature. This means that the golden signature can be used for signature protection of digital in scale of time.

CONCLUSION

In this paper, we presented a signature scheme based on Matrix extension of RSA Cryptosystem and golden matrices, the main result of the present article is a develop of one more application of the golden proportion, that is, a creation of one of the kind of digital signature called as the golden digital signature. The proposed technique is the fast signature and secure. This means that the golden signature can be used for signature protection of digital on a scale of time.
REFERENCES

9. Chih-Chwen ChuangJames George Dunham, Matrix Extensions of the RSA Algorithm CRYPTO1990: Advances in Cryptology-CRYPTO’ 90, 140-155
10. Andrew Pangia, A Matrix Extension of the RSA Cryptosystem,2014

Source of support: Nil, Conflict of interest: None Declared.
[Copy right © 2019. This is an Open Access article distributed under the terms of the International Journal of Mathematical Archive (IJMA), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.]