International Journal of Mathematical Archive-10(6), 2019, 63-67
Available online through www.ijma.info ISSN 2229 – 5046

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

P. SUNDARAYYA[1], M.G. VARA PRASAD*[2] AND P. VENKATA RAMANA[3]

[1]Department of Engineering Mathematics,
GITAM Deemed to be University, Visakhapatnam, India.

[2]Department of Mathematics. NSRIT, Visakhapatnam, India.

[3]Research 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 proposed 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 2×2 square matrix is defined as $Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ (1)

The k^{th} power of the Q-matrix can be defined as $Q^k = \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix}$ (2)

Det(Q^k) = $F_{k+1}F_{k-1} - F_k{}^2 = (-1)^k$ where $k = 0, \pm1, \pm2, \cdot \cdot$ (3)

F_k is k^{th} Fibonacci number and recurrence relation

$$F_{k+1} = F_k + F_{k-1} \tag{4}$$

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

Identity (4) generates the Fibonacci numbers1, 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

$$Q^k = \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix} = \begin{pmatrix} F_k + F_{k-1} & F_{k-1} + F_{k-2} \\ F_{k-1} + F_{k-2} & F_{k-2} + F_{k-3} \end{pmatrix} = \begin{pmatrix} F_k & F_{k-1} \\ F_{k-1} & F_{k-2} \end{pmatrix} + \begin{pmatrix} F_{k-1} & F_{k-2} \\ F_{k-2} & F_{k-3} \end{pmatrix}$$

$$Q^k = Q^{k-1} + Q^{k-2} \tag{5}$$

$$Q^k Q^l = Q^l Q^k = Q^{l+k} \tag{6}$$

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

$$F_k = \begin{cases} sF_s(k), & for\ k = 2x \\ cF_s(k), & for\ k = 2x+1 \end{cases} \tag{7}$$

Corresponding Author: M.G. Vara Prasad*[2]
[2]Department of Mathematics. NSRIT, Visakhapatnam, India.

Symmetrical hyperbolic Fibonacci sine: $sF_s(k) = \frac{\tau^k - \tau^{-k}}{\sqrt{5}}$ (8)

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

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

By using (3) generalization of the Cassini formula

$$[sF_s(k)]^2 - cF_s(k+1)cF_s(k-1) = -1 \tag{10}$$

$$[cF_s(k)]^2 - sF_s(k+1)sF_s(k-1) = 1 \tag{11}$$

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.

$$Q^{2x} = \begin{pmatrix} cF_s(2x+1) & sF_s(2x) \\ sF_s(2x) & cF_s(2x-1) \end{pmatrix} \tag{12}$$

$$Q^{2x+1} = \begin{pmatrix} sF_s(2x+2) & cF_s(2x+1) \\ cF_s(2x+1) & sF_s(2x) \end{pmatrix} \tag{13}$$

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.

$$Q^{-2x} = \begin{pmatrix} cF_s(2x-1) & -sF_s(2x) \\ -sF_s(2x) & cF_s(2x+1) \end{pmatrix} \tag{14}$$

$$Q^{-(2x+1)} = \begin{pmatrix} -sF_s(2x) & cF_s(2x+1) \\ cF_s(2x+1) & -sF_s(2x+2) \end{pmatrix} \tag{15}$$

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

k	0	1	2	3	4
${Q_1}^k$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}$
${Q_1}^{-k}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$	$\begin{pmatrix} -1 & 2 \\ 2 & -3 \end{pmatrix}$	$\begin{pmatrix} 2 & -3 \\ -3 & 5 \end{pmatrix}$

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 ∈ GL_2 (Z_n) be a matrix made up of nonnegative integers less than n.

Let g_p = |GL_2 (Z_n) | = $(p^2 - 1)(p^2 - p)$, g_q = |GL_2 (Z_n) | = $(q^2 - 1)(q^2 - q)$ and define $g = g_p g_q$. Further let e, d ∈ 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.

$$m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8, m_9 \ldots\ldots\ldots \in {Z_n}^* \tag{16}$$

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.

$$\text{Let } M = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} \tag{17}$$

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.

$$\text{Signing: } S_1(x) = M^d \mathrm{Q}^{2x} \pmod{n} \tag{18}$$

$$S_2(x) = \mathrm{M}^{\mathrm{d}} \mathrm{Q}^{2x+1} \pmod{n} \tag{19}$$

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:

$$\text{Verification:} [S_1(x)\mathrm{Q}^{-2x}]^e = M (mod\ n) \tag{20}$$

$$[S_2(x)\mathrm{Q}^{-(2x+1)}]^e = M (mod\ n) \tag{21}$$

Where Q^{-2x} (14) and $\mathrm{Q}^{-(2x+1)}$ (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 $x = a$ the "golden" digital can be represented as follows:

Signing:

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

Now $\mathrm{M}^{\mathrm{d}}\mathrm{Q}^{2x} = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \begin{pmatrix} cF_s(2a+1) & sF_s(2a) \\ sF_s(2a) & cF_s(2a-1) \end{pmatrix}$

$$= \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix} \pmod{n} = S_1(a) \tag{22}$$

where

$$s_{11} = c_1 cF_s(2a+1) + c_2 sF_s(2a) \tag{23}$$

$$s_{12} = c_1 sF_s(2a) + c_2 cF_s(2a-1) \tag{24}$$

$$s_{21} = c_3 cF_s(2a+1) + c_4 sF_s(2a) \tag{25}$$

$$s_{22} = c_3 sF_s(2a) + c_4 cF_s(2a-1) \tag{26}$$

Verification:

$$[S_1(a)\mathrm{Q}^{-2a}]^e = \left(\begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix} \begin{pmatrix} cF_s(2a-1) & -sF_s(2a) \\ -sF_s(2a) & cF_s(2a+1) \end{pmatrix} \right)^e$$

$$= \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix}^e (mod\ n) \tag{27}$$

where

$$v_{11} = s_{11} cF_s(2a-1) - s_{12} sF_s(2a) \tag{28}$$

$$v_{12} = -s_{11} sF_s(2a) + s_{12} cF_s(2a+1) \tag{29}$$

$$v_{21} = s_{21} cF_s(2a-1) - s_{22} sF_s(2a) \tag{30}$$

$$v_{22} = -s_{21} sF_s(2a) + s_{22} cF_s(2a+1) \tag{31}$$

For calculation of the matrix element given by (28) we can use the (23) and (24). Then we get

$$\begin{aligned} v_{11} &= [c_1 cF_s(2a+1) + c_2 sF_s(2a)]cF_s(2a-1) - [c_1 sF_s(2a) + c_2 cF_s(2a-1)]sF_s(2a) \\ &= c_1[cF_s(2a+1)cF_s(2a-1) - [sF_s(2a)]^2] + c_2[sF_s(2a)cF_s(2a-1) - cF_s(2a-1)sF_s(2a)] \end{aligned} \tag{32}$$

Using the identity (8) we can write the expression (32) as follows:

$$v_{11} = c_1 \times 1 + c_2 \times 0 = c_1$$

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

$$[S_1(a)Q^{-2a}\ ]^e = \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix}^e (mod\ n)$$
$$= \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}^e (mod\ n)$$
$$= \left(\begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}^d\right)^e (mod\ n)$$
$$= \mathrm{M}^{\mathrm{de}} (mod\ n)$$
$$= \mathrm{M}\ (mod\ n)$$
$$[S_1(a)Q^{-2a}\ ]^e = \mathrm{M}\ (mod\ n) \tag{33}$$

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
$g = g_p g_q$= 967680, e= 199 such that g.c.d (199, 967680) =1 and 199×d=1(mod 967680) then d=34039, choose x=10

$\mathrm{Q}^{2x} = \mathrm{Q}^{20} = \begin{pmatrix} 10946 & 6765 \\ 6765 & 4181 \end{pmatrix}$ and $\mathrm{Q}^{-2x} = \mathrm{Q}^{-20} = \begin{pmatrix} 4181 & -6765 \\ -6765 & 10946 \end{pmatrix}$

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

$\therefore$ M=$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$

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

Signature:

$$\mathrm{M}^{\mathrm{d}}\mathrm{Q}^{2x} = \mathrm{M}^{34039}\mathrm{Q}^{20} = \begin{pmatrix} 8 & 15 \\ 24 & 32 \end{pmatrix}\begin{pmatrix} 10946 & 6765 \\ 6765 & 4181 \end{pmatrix}(\ mod\ 35)$$
$$= \begin{pmatrix} 8 & 5 \\ 34 & 17 \end{pmatrix}(\ mod\ 35)$$

Verification:

$$[S_1(a)Q^{-2a}\ ]^e = [S_1(10)Q^{-20}\ ]^{199}$$
$$= \left(\begin{pmatrix} 8 & 5 \\ 34 & 17 \end{pmatrix}\begin{pmatrix} 4181 & -6765 \\ -6765 & 10946 \end{pmatrix}\right)^{199} (mod\ \ 35)$$
$$= \begin{pmatrix} 8 & 15 \\ 24 & 32 \end{pmatrix}^{199} (mod\ \ 35)$$
$$= \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}(mod\ \ 35) = \mathrm{M}$$

6 PERFORMANCE EVALUATION

We use the following notation to analyze the performance of the proposed technique:
$\mathrm{T_{sign}}$ is the full signature time, $\mathrm{T_{ver}}$ is full verification time, $\mathrm{T_{exp}}$ is the time for a modular exponentiation, $\mathrm{T_{add}}$ is the time of modular addition, $\mathrm{T_{mul}}$ is the time modular multiplication.

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

$$\mathrm{T_{sign}} = 4\mathrm{T_{add}} + 8\mathrm{T_{mul}} + \mathrm{T_{exp}} \tag{34}$$

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

$$\mathrm{T_{ver}} = 4\mathrm{T_{add}} + 8\mathrm{T_{mul}} + \mathrm{T_{exp}} \tag{35}$$

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

1. H.Gould A history of the Fibonacci Q-matrix and a higher-dimensional problem. The Fibonacci Quart 1981(19):250–7.
2. VE. Hoggat , Fibonacci and Lucas numbers, Palo Alto, CA: Houghton-Mifflin, (1969).
3. A.P. Stakhov Massingue V, Sluchenkova A. Introduction into Fibonacci coding and cryptography. Kharkov: Osnova; 1999.
4. A.P. Stakhov. A generalization of the Fibonacci Q-matrix. Rep Natl Acad Sci Ukr 1999(9):46–59.
5. A.P. Stakhov and IS. Tkachenko, Hyperbolic Fibonacci trigonometry Rep. Ukr. Acad. Sci, 208(7), (1993), 9-14.
6. A. P. Stakhov, The golden matrices and a new kind of cryptography, Chaos, Solitions and Fractals 32(2007), 1138-1146.
7. Hoggat VE. Fibonacci and Lucas numbers. Palo Alto, CA: Houghton-Mifflin; 1969.
8. Hohn FE. Elementary matrix algebra. New York: Macmillan Company; 1973.
9. Chih-Chwen ChuangJames George Dunham, Matrix Extensions of the RSA Algorithm CRYPTO1990: Advances in Cryptology-CRYPT0' 90, 140-155
10. Andrew Pangia, A Matrix Extension of the RSA Cryptosystem,2014
11. A.P. Stakhov and B. Rozin, On a new class of Hyperbolic function, On a new class of Hyperbolic function,Chaos, Solitons and Fractals, 23, (2004),379-389.
12. A.P. Stakhov, Hyperbolic Fibonacci and Lucas functions,A new mathematics for the living nature, Vinnitsa, ITI (2003).
13. F. Bani-ahmad, M.T. Shatnawi, N. Tahat, S. Shatnawi, A new kind of digital signature scheme using golden matrices based on factoring problem, International journal of pure and applied mathematics, Vol 107 No. 1

Source of support: Nil, Conflict of interest: None Declared.