International Journal of Pure and Applied Mathematics
Volume 107 No. 1 2016, 49-57
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: 10.12732/ijpam.v107i1.5
ijpam.eu

A NEW KIND OF DIGITAL SIGNATURE SCHEME USING GOLDEN MATRICES BASED ON FACTORING PROBLEM

Feras Bani-Ahmad[1], "Mohd Taib" Shatnawi[2], Nedal Tahat[3], Safaa Shatnawi[4]

[1,3]Department of Mathematics Faculty of Science
The Hashemite UniversityZarqa 13133, JORDAN
[2]Al-Balqa Applied University, Al-Huson University
College P.O. Box 50, Al-Huson, 21510, Irbid, JORDAN
[4]School of Mathematical Sciences
National University of Malaysia
43600, UKM Bangui Selangor, MALAYSIA

Abstract: A.P. Stakhov in [12] proposed the concepts golden matrices and new kind of cryptography. In this paper, we propose a new kind of digital signature scheme based on factoring problem and the golden matrices, called the golden digital signature. The method is very fast and simple for technical realization and can be used for signature protection of digital signals (telecommunication and measurement system).

Key Words: signature scheme, golden matrices, factoring problem, golden digital signature

1. Introduction

In the last decades the theory of Fibonacci numbers [1], [3] was complemented by the theory of the so-called Fibonacci $Q-$matrix [2], [3]. The latter is a square

Received: December 15, 2015
Published: March 23, 2016

2×2 matrix of the following form

$$Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \tag{1}$$

In [3] the following property of the n^{th} power of the $Q - matrix$ was proved

$$Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \tag{2}$$

$$det(Q^n) = F_{n+1}F_{n-1} - F_n^2 = (-1)^n \tag{3}$$

Where $n = 0, \mp 1, \mp 2, \mp 3, F_{n-1}, F_n, F_{n+1}$ are Fibonacci numbers given by the following recurrence relation:

$$F_{n+1} = F_n + F_{n-1} \tag{4}$$

with the initial terms $F_1 = F_2 = 1$

Rule (4), can be used to extend the sequence backwards, thus $F_{-n} = (-1)^{n+1}F_n$

In [7] , represent matrix (2) is showed in the following form

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

or

$$Q^n = Q^{n-1} + Q^{n-2}$$

It is proved in [8] the following property of the matrix,

$$Q^nQ^m = Q^mQ^n = Q^{nm}$$

Alexey Stakhov, Ivan Tkachenko and Boris Rozin developed recently a theory of the hyperbolic Fibonacci and Lucas functions [9, 10, 11] Let us consider so-called symmetrical hyperbolic Fibonacci functions introduced in [11] Symmetrical hyperbolic Fibonacci sine:

$$sF_s = \frac{\tau^x - \tau^{-x}}{\sqrt{5}} \tag{5}$$

Symmetrical hyperbolic cosine:

$$cF_s = \frac{\tau^x + \tau^{-x}}{\sqrt{5}} \tag{6}$$

Where $sF_s = \frac{\tau^{\mathsf{x}} - \tau^{-\mathsf{x}}}{\sqrt{5}}$ (the Golden Proportion).

Note that the symmetrical hyperbolic Fibonacci functions are connected to the Fibonacci numbers by the following correlations:

$$F_n = \begin{cases} sF_s(x) & \text{if } n = \text{2k} \\ cF_s(x) & \text{if } n = \text{2k+1} \end{cases} \tag{7}$$

It was proved in [11] that the following identities connect the symmetrical hyperbolic Fibonacci functions.

$$[sF_s(x)]^2 - cF_s(x+1)cF_s(x-1) = -1 \tag{8}$$

$$[cF_s(x)]^2 - sF_s(x+1)cF_s(x-1) = 1 \tag{9}$$

Note that the identities (8) and (9) are a generalization of the Cassini formula (3) for continuous domain. Stakhov [12] 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 (5) and (6). The golden matrices that are the functions of the continuous variable x are the following form.

$$Q^{2x} = \begin{pmatrix} cF_s(2x+1) & sF_s(2x) \\ sF_s(2x) & cF_s(2x-1) \end{pmatrix} \tag{10}$$

$$Q^{2x+1} = \begin{pmatrix} sF_s(2x+2) & cF_s(2x+1) \\ cF_s(2x+1) & sF_s(2x) \end{pmatrix} \tag{11}$$

Stakhov [12] obtained inverse matrices of (10) and (11). The inverse golden matrices that are the functions of the continuous variable x are the following form.

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

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

Furthermore, in [12] the golden matrices were used for creation of a new kind of cryptography called the golden cryptography. In this paper, we propose a new kind of digital signature based on factoring and golden matrices.

2. The New Digital Signature

In this section, we propose a new signature scheme based on factoring problem and golden matrices.

2.1. Algorithm for Signing and Verification Message

Select two large primes p, q and $n = pq$. The signer picks randomly an integer e from $0, 1, 2, ..., n-1$ such that $gcd(e, \phi(n)) = 1$. Calculate d such that $ed \equiv 1\,(\mathrm{mod}\phi(n))$. Thus the public key and secret keys respectively given by e and d.
What we have introduced above, namely the "golden" direct and inverse matrices and allow us to develop the following application to digital signature.

Let the initial message be a digital signal, which is any sequence of real numbers:

$$a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, ... \in Z_n^* \tag{14}$$

Separate real numbers of the sequence (14) are called readings. There are many examples of the "digital signals" (14): digital telephony, digital TV, digital measurement systems and so on.

The problem of protecting the "digital signal" (14) from the hackers is solved usually with application of digital signature methods. Consider a new signature method based on the "golden" matrices. To this end let us choose the first four readings a_1, a_2, a_3, a_4 of (14) and form them a square 2×2-matrix M:

$$M = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \text{ Where } a_2 = a_1 + 1, a_3 = a_1 + 2, a_4 = a_1 - 1 \tag{15}$$

Table 1: Signing / verification algorithm

Signing	Verification
Computes $A = Q^{2x}$ $s_1(x) = M^d A$	$[s_1(x)A^{-1}]^e = M(mod\, n)$
$B = Q^(2x+1)$ $s_2(x) = M^d B$	$[s_2(x)B^{-1}]^e = M(mod\, n)$

Note that the initial matrix M can be considered as message

Note that there are 24 variants (permutations) to form the matrix (15) 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 a_1, a_2, a_3, a_4 is a choice of the permutation P_i.

Let us consider now the following signing /verification algorithms based on matrix multiplication (see table 1). Here is the plaintext (15) that is formed according to the permutation P_i;$s_1(x), s_2(x)$ are signatures; $A = Q^{2x}, B = Q^{2x+1}$ are the signature matrices (10) and (11); $A^{-1} = Q^{-2x}, B^{-1} = Q^{-(2x+1)}$ are the verification matrices (12) and (13). 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 . In general the key consists of two parts: public key e , private keys (x, d)

The signature on message M is $(A, B, s_1(x), s_2(x))$. where M^d is matrix to the power d , also $[s_1(x)A^{-1}]^e = M(mod\, n)$ is matrix to the power e

The above equations are true for valid signature since:

Let us prove that the signature method given with table 1 ensures one -valued transformation of the message into the signature s and then the signature s into the message M .Let us consider this transformation for the case when we choose the" golden" matrix (10) as the digital matrix .For the given value of the digital signature key $x = x_1$ the "golden" digital can be represented as follows:

suppose $M^d = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \, mod\, n$

$$M^d \times Q^{2x} = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \times \begin{pmatrix} cF_s(2x_1+1) & sF_s(2x_1) \\ sF_s(2x_1) & cF_s(2x_1-1) \end{pmatrix}$$

$$= \begin{pmatrix} c_1cF_s(2x_1+1) + c_2sF_s(2x_1) & c_1sF_s(2x_1) + c_2cF_s(2x_1-1) \\ c_3cF_s(2x_1+1) + c_4sF_s(2x_1) & c_3sF_s(2x_1) + c_4cF_s(2x_1-1) \end{pmatrix}$$

$$= \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix} = s_1(x) \tag{16}$$

where

$$\begin{aligned} s_{11} &= c_1cF_s(2x_1+1) + c_2sF_s(2x_1) && (17)\\ s_{12} &= c_1sF_s(2x_1) + c_2cF_s(2x_1-1) && (18)\\ s_{21} &= c_3cF_s(2x_1+1) + c_4sF_s(2x_1) && (19)\\ s_{22} &= c_3sF_s(2x_1) + c_4cF_s(2x_1-1) && (20) \end{aligned}$$

Let us consider the "golden" verification for case:

$$[s_1(x)A^{-1}]^e = \left(\begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix} \begin{pmatrix} cF_s(2x_1-1) & -sF_s(2x_1) \\ -sF_s(2x_1) & cF_s(2x_1+1) \end{pmatrix}\right)^e$$

$$= \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix}^e = v \tag{21}$$

where

$$\begin{aligned} v_{11} &= s_{11}cF_s(2x_1-1) - s_{12}sF_s(2x_1) && (22)\\ v_{12} &= -s_{11}sF_s(2x_1) + s_{12}cF_s(2x_1+1) && (23)\\ v_{21} &= s_{21}(2x_1-1) - s_{22}sF_s(2x_1) && (24)\\ v_{22} &= -s_{21}sF_s(2x_1) + s_{22}cF_s(2x_1+1) && (25) \end{aligned}$$

For calculation of the matrix elements given by (22)-(25) we can use the expression (17)-(20). Then we have:

$$\begin{aligned} v_{11} = \left[c_1 cF_s(2x_1+1) + c_2 sF_s(2x_1)\right] cF_s(2x_1-1) \\ - \left[c_1 sF_s(2x_1) + c_2 cF_s(2x_1-1)\right] sF_s(2x_1) \\ = c_1 \left[cF_s(2x_1+1) cF_s(2x_1-1) - (sF_s(2x_1))^2\right] \\ + c_2 \left[sF_s(2x_1) cF_s(2x_1-1) - cF_s(2x_1-1) sF_s(2x_1)\right] \end{aligned} \tag{26}$$

Using the fundamental identity (8) we can write the expression (26) as follows:

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

In the same manner after corresponding transformations we can write:

$$\begin{aligned} v_{12} &= c_2 \\ v_{21} &= c_3 \\ v_{22} &= c_4 \end{aligned}$$

Then we have

$$\begin{aligned} v &= \left[s(x_1) \times Q^{-2x_1}\right]^e \\ &= \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix}^e \\ &= \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}^e \\ &= \left(\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}^d\right)^e \\ &= M^{de} \\ &= M \bmod n \end{aligned}$$

So

$$\left[s(x_1) \times Q^{-2x_1}\right]^e = [M^d]^e = M \bmod n$$

3. Simple Example

Let $p = 47, q = 59, n = 4759, \phi(n) = 2668, e = 17$ such that $\gcd(17, 2668) = 1$ and $17 \times d = 1 \bmod 2668$ then $d = 157, x_1 = 20$

Compute

$$A = Q^{2x} = Q^{40} = \begin{pmatrix} 165580141 & 102334155 \\ 102334155 & 63245986 \end{pmatrix}$$

$$A^{-1} = Q^{-40} = \begin{pmatrix} 63245986 & -102334155 \\ -102334155 & 165580141 \end{pmatrix}$$

Let $M = \begin{pmatrix} 3 & 4 \\ 5 & 2 \end{pmatrix}$

$$M^d = \begin{pmatrix} 3 & 4 \\ 5 & 2 \end{pmatrix}^{157} \pmod{2773} = \begin{pmatrix} 1478 & 2012 \\ 2515 & 975 \end{pmatrix} \pmod{2773}$$

$$s_1(x) = M^d A = \begin{pmatrix} 1478 & 2012 \\ 2515 & 975 \end{pmatrix} \times \begin{pmatrix} 165580141 & 102334155 \\ 102334155 & 63245986 \end{pmatrix}$$

$$= \begin{pmatrix} 1559 & 1640 \\ 2585 & 19 \end{pmatrix} \pmod{2773}$$

Verification:

$$\left[s_1(x)A^{-1}\right]^e = \left[\begin{pmatrix} 1559 & 1640 \\ 2585 & 19 \end{pmatrix} \times \begin{pmatrix} 63245986 & -102334155 \\ -102334155 & 165580141 \end{pmatrix}\right]^{17}$$

$$= \begin{pmatrix} 1478 & 2012 \\ 2515 & 975 \end{pmatrix}^{17} \pmod{2773}$$

$$= \begin{pmatrix} 3 & 4 \\ 5 & 2 \end{pmatrix} \pmod{2773} = M$$

4. Performance Evaluation

We use the following notation to analyze the performance of the scheme :

- T_s this means that a full signature time
- $T_v$this means that a full verification time
- T_{ad} is the time of modular addition
- T_m is the time modular multiplication
- T_{exp} is the time for a modular exponentiation

According to (16) the signature consists in calculation of four elements $s_{11}, s_{12}, s_{21}, s_{22}$ of the matrix (16) .According to (17) – (20) a calculation of every element include eight multiplication and four additions. This means that a full signature time T_s is equal:

$$T_s = 4T_{ad} + 8T_m + T_{exp} \tag{27}$$

By analogy, if we consider the expressions (21) – (25) we can write the expressions for a full verification time:

$$T_v = 4T_{ad} + 8T_m + T_{exp} \tag{28}$$

Analysis of the expressions (27) and (28) 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.

5. Conclusion

In this paper, we presented a new signature scheme based on factor- ing 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 a new kind of digital signature called the golden digital signature. The proposed scheme is fast signature. This means that the golden signature can be used for signature protection of digital in scale of time

References

[1] EL.MS. Naschie,Statistical geometry of a cantor diocretum and semiconductors , *Comput.Math. Appl* ,29(12),(1995),103-10.

[2] H. Gould, A History of the Fibonacci Q-matrix and a higher- dimensional problem,*Fibonacci Quart*,19,(1981),2507.

[3] VE. Hoggat , Fibonacci and Lucas numbers, *Palo Alto, CA : Houghton-Mifflin* ,(1969).

[4] R. A. Horn and Johnson , Matrix Analysis,*Cambridge Univer- sity Press, New York*,(1985).

[5] H. Minc, Permanents,*Encyclopaedia of Mathematics and Its Applications* ,Vol.6, Addison-Wesley(1978).

[6] A. P. Stakhov, V. Massingue and A. Sluchenkova, *Introduc- tion into Fibonacci coding and cryptography* ,Kharkov, Osnova,(1999).

[7] A.P. Stakhov, Fibonacci matrices, a generalization of the Cassini formula and a new coding theory, *Chaos, Solitons and Fractals*, (2006);30:5666.

[8] A.P. Stakhov, A generalization of the Fibonacci Q-matrix Rep. *Nat. Acad. Sci., Ukraine*,(9),(2006),46-9.

[9] A.P. Stakhov and IS. Tkachenko, Hyperbolic Fibonacci trigonometry Rep. *Ukr. Acad. Sci*, 208(7),(1993) 9-14.

[10] A.P. Stakhov,Hyperbolic Fibonacci and Lucas functions,*A new mathematics for the living nature*, Vinnitsa, ITI , (2003).

[11] A.P. Stakhov and B. Rozin, On a new class of Hyperbolic func- tion, On a new class of Hyperbolic function,*Chaos, Solitons and Fractals*, 23, (2004),379-389

[12] A.P. Stakhov , The golden matrices and a new kind of cryp- tography, *Chaos, Solitons and Fractals*, (2006).