Int. J. Contemp. Math. Sciences, Vol. 7, 2012, no. 7, 327 - 335

On the Security of Golden Cryptosystems

M. Tahghighi[1], S. Turaev[1], A. Jaafar[1], R. Mahmod[1] and M. Md. Said[2]

[1]Faculty of Computer Science and Information Technology
University Putra Malaysia
43400 UPM Serdang, Selangor, Malaysia
mtahghighi@yahoo.com, {sherzod, azmi, ramlan}@fsktm.upm.edu.my

[2]Institute for Mathematical Research
University Putra Malaysia
43400 UPM Serdang, Selangor, Malaysia
mrushdan@putra.upm.edu.my

Abstract

In this paper we have investigated the security of different variants the golden cryptography, and showed that all the variants of the cryptosystem are not secure against chosen-plaintext attack.

Mathematics Subject Classification: 11B39, 11T71, 11C20

Keywords: Fibonacci numbers and functions, Golden matrices, Cryptography, Cryptanalysis

1 Introduction

Fibonacci numbers or Fibonacci sequences, closely connected to Golden Section, appear in various fields such as nature, architecture, physics, etc., and are used in modeling phenomena appearing in economy, computer science, physics, etc. The recent intensive studies of Fibonacci numbers have resulted different extensions of Fibonacci numbers. For instance, k-Fibonacci numbers, hyperbolic Fibonacci functions, Fibonacci Q-matrices, Golden matrices, and so on. The simplicity and beauty of Fibonacci numbers allow developing matrix cryptosystems, which are useful in digital communications, i.e., digital TV, digital telephony, digital measurement, etc. One of such cryptosystems, called golden cryptography based on golden matrices, which are a generalization of Fibonacci Q-matrices for continuous domain, was introduced by Stakhov in [7]. Later, in his another paper, he improved golden cryptosystem by using golden G_k-matrices based on the k-Fibonacci hyperbolic functions (see [8]). Another

interesting cryptosystem based on Hadamard product of golden matrices was introduced by Nally in [4]. There are also other simple cryptographic methods (for instance, see [9], [2]) based on extensions of golden matrices.

Any cryptosystem has a practical value if it is secure against different types of cryptanalytic attacks such as *ciphertext-only* attack (cryptanalysis has to based on only the sample of ciphertext), *known-plaintext* attack (the cryptanalyst knows in advance some pairs of plaintexts and the corresponding ciphertexts), *chosen-plaintext* attack (the cryptanalyst can obtain the ciphertexts corresponding to an arbitrary set of plaintexts of his own choosing).

Unfortunately, the above-mentioned cryptosystems are not resistable against some cryptanalytic attacks. Rey and Sánchez (see [6]) showed that the cryptosystem proposed in [7] is not secure, i.e., it is not robust against chosen-plaintext attack. In this paper, we show that the improved version of golden cryptography developed in [8] and the cryptosystem defined in [4] are also insecure against chosen-plaintext attack.

The paper is organized as follows: in Section 2 we cite some necessary notions and notations which are used in sequal. In Section 3 we show that the cryptographic method based on Hadamard product of golden matrices (in Subsection 3.1) and the generalized golden cryptography are not secure against the chosen-plaintext attack (in Subsection 3.2).

2 Preliminaries

The reader is assumed to be familiar with basic notations of cryptography and cryptanalysis, for details refer to [5].

2.1 Golden matrices

For some real number x, the *golden matrices* are defined as

$$Q^{2x} = \begin{pmatrix} cFs(2x+1) & sFs(2x) \\ sFs(2x) & cFs(2x-1) \end{pmatrix}, \tag{1}$$

$$Q^{2x+1} = \begin{pmatrix} sFs(2x+2) & cFs(2x+1) \\ cFs(2x+1) & sFs(2x) \end{pmatrix}, \tag{2}$$

where

$$sFs(x) = \frac{\tau^x - \tau^{-x}}{\sqrt{5}} \quad \text{and} \quad cFs(x) = \frac{\tau^x + \tau^{-x}}{\sqrt{5}}$$

are the symmetrical hyperbolic Fibonacci sine and the symmetrical hyperbolic Fibonacci cosine with $\tau = \frac{1+\sqrt{5}}{\sqrt{2}}$ (the Golden Proportion). For the detailed information on golden matrices, we refer the reader to [7].

The *Hadamard product* of golden matrices is defined as

$$Q^{2x} \circ Q^{-2x} = \begin{pmatrix} cFs(2x+1)cFs(2x-1) & -[sFs(2x)]^2 \\ -[sFs(2x)]^2 & cFs(2x+1)cFs(2x-1) \end{pmatrix}, \quad (3)$$

$$Q^{2x+1} \circ Q^{-2x-1} = \begin{pmatrix} -sFs(2x+2)sFs(2x) & [cFs(2x+1)]^2 \\ [cFs(2x+1)]^2 & -sFs(2x+2)sFs(2x) \end{pmatrix}. \quad (4)$$

The inverses of the matrices (3) and (4) are defined as

$$(Q^{2x} \circ Q^{-2x})^{-1} = \frac{1}{1+2q_1} \begin{pmatrix} 1+q_1 & q_1 \\ q_1 & 1+q_1 \end{pmatrix}, \quad (5)$$

$$(Q^{2x+1} \circ Q^{-2x-1})^{-1} = \frac{1}{1-2q_2} \begin{pmatrix} 1-q_2 & -q_2 \\ -q_2 & 1-q_2 \end{pmatrix}, \quad (6)$$

where $q_1 = [sFs(2x)]^2$ and $q_2 = [cFs(2x+1)]^2$. The detailed information on the Hadamard product of golden matrices can be found in [3, 4].

For some positive integer k and real number x, the *generalized golden matrices of the order* k is defined as

$$G_k^{2x} = \begin{pmatrix} cF_k(2x+1) & sF_k(2x) \\ sF_k(2x) & cF_k(2x-1) \end{pmatrix}, \quad (7)$$

$$G_k^{2x+1} = \begin{pmatrix} sF_k(2x+2) & cF_k(2x+1) \\ cF_k(2x+1) & sF_k(2x) \end{pmatrix}, \quad (8)$$

where

$$sF_k(x) = \frac{\sigma_k^x - \sigma_k^{-x}}{\sigma_k + \sigma_k^{-1}} \text{ and } cF_k(x) = \frac{\sigma_k^x + \sigma_k^{-x}}{\sigma_k + \sigma_k^{-1}}, \ \sigma_k = \frac{k + \sqrt{k^2+4}}{2},$$

are *k-Fibonacci hyperbolic sine* and *cosine*, respectively.

The inverse matrices of (7) and (8) are defined as

$$G_k^{-2x} = \begin{pmatrix} cF_k(2x-1) & -sF_k(2x) \\ -sF_k(2x) & cF_k(2x+1) \end{pmatrix}, \quad (9)$$

$$G_k^{-2x-1} = \begin{pmatrix} -sF_k(2x) & cF_k(2x+1) \\ cF_k(2x+1) & -sF_k(2x+2) \end{pmatrix}. \quad (10)$$

The detailed information on the k-Fibonacci hyperbolic functions and the

corresponding golden matrices is given in [1, 8].

2.2 Golden cryptographic methods

The basic idea of the cryptographic methods proposed in [4, 8] is as follows:

- a plaintext $a_1, a_2, a_3, a_4, \ldots$ is presented in the form of 2×2 matrices
$$M = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \ldots$$
- For some $i = 1, 2, \ldots, 24$, the permutation $\pi(i)$ of a_1, a_2, a_3, a_4, i.e., $a_{\pi(1)}$, $a_{\pi(2)}$, $a_{\pi(3)}$, $a_{\pi(4)}$ is designated.
- The matrix (3) or (4) (the matrix (7) or (8)), which called the *enciphering matrix*, and its inverse matrix (5) or (6) (its inverse matrix (9) or (10)), respectively, which is called the *deciphering matrix*, are chosen.
- The ciphertext $E_1(x)$ or $E_2(x)$ is obtained by using matrix multiplication of the plaintext M and the matrix $Q^{2x} \circ Q^{-2x}$ or $Q^{2x+1} \circ Q^{-2x-1}$ (the ciphertext $E_1(x, k)$ or $E_2(x, k)$ is obtained by using matrix multiplication of the plaintext M and the matrix G_k^{2x} or G_k^{2x+1}), i.e.,
$$E_1(x) = M \times Q^{2x} \circ Q^{-2x} \quad \text{or} \quad E_2(x) = M \times Q^{2x+1} \circ Q^{-2x-1}$$
$$(E_1(x, k) = M \times G_k^{2x} \quad \text{or} \quad E_2(x, k) = M \times G_k^{2x+1}).$$
- In order to recover the original plaintext M, the corresponding inverse matrix $(Q^{2x} \circ Q^{-2x})^{-1}$ or $(Q^{2x+1} \circ Q^{-2x-1})^{-1}$ (the corresponding inverse matrix G_k^{-2x} or G_k^{-2x-1}) is used, i.e.,
$$M = E_1(x) \times (Q^{2x} \circ Q^{-2x})^{-1} \text{ or } M = E_2(x) \times (Q^{2x+1} \circ Q^{-2x-1})^{-1}$$
$$(M = E_1(x, k) \times G_k^{-2x} \text{ or } M = E_2(x, k) \times G_k^{-2x-1}).$$

3 Results

In the following subsections we show that the above-mentioned cryptographic methods do not resist against the chosen-plaintext attack.

3.1 The chosen-plaintext attack against the cryptographic method with Hadamard product of golden matrices

We choose the pairs of plaintexts and ciphertexts $\{M_i, E_i(x)\}$, $i = 1, 2, 3, 4$, where

$$M_1 = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, M_2 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, M_3 = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, M_4 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (11)$$

Without loss of generality, we can assume that the enciphering matrix is $Q^{2x} \circ Q^{-2x}$. Then 24 possible permutations of the initial matrix are reduced to the following 4 matrices:

$$E_1(x) = M_1 \times Q^{2x} \circ Q^{-2x} = \begin{pmatrix} -e_2 & e_2 \\ e_1 & e_1 \end{pmatrix},$$

$$E_2(x) = M_2 \times Q^{2x} \circ Q^{-2x} = \begin{pmatrix} e_2 & -e_2 \\ e_1 & e_1 \end{pmatrix},$$

$$E_3(x) = M_3 \times Q^{2x} \circ Q^{-2x} = \begin{pmatrix} e_1 & e_1 \\ -e_2 & e_2 \end{pmatrix},$$

$$E_4(x) = M_4 \times Q^{2x} \circ Q^{-2x} = \begin{pmatrix} e_1 & e_1 \\ e_2 & -e_2 \end{pmatrix},$$

where

$$e_1 = cFs(2x+1)cF(2x-1) - [sFs(2x)]^2,$$
$$e_2 = cFs(2x+1)cF(2x-1) + [sFs(2x)]^2.$$

Thus, for the known real variables t_1 and t_2, we obtain the system

$$\begin{cases} Fs(2x+1)cF(2x-1) - [sFs(2x)]^2 = t_1 \\ cFs(2x+1)cF(2x-1) + [sFs(2x)]^2 = t_2. \end{cases} \quad (12)$$

of non-linear equations. By the definition of $sF(x)$ and $cFs(x)$,

$$\begin{cases} \frac{(\tau^{2x+1}+\tau^{-2x-1})}{5} - \frac{(\tau^{2x}-\tau^{-2x})^2}{5} = t_1 \\ \frac{(\tau^{2x+1}+\tau^{-2x-1})}{5} + \frac{(\tau^{2x}-\tau^{-2x})^2}{5} = t_2. \end{cases} \quad (13)$$

The substraction of the first equation from the second equation in (13) leads to the equation

$$2(\tau^{2x} - \tau^{-2x})^2 = 5(t_2 - t_1). \tag{14}$$

Further, by some calculations, we obtain the equation

$$y^2 + (2.5(t_1 - t_2) - 2)y + 1 = 0, \tag{15}$$

where $y = \tau^{4x}$. The solutions of the equation (15) are

$$y = \frac{2 - 2.5(t_1 - t_2) \pm \sqrt{6.25(t_1 - t_2)^2 + 5(t_1 - t_2)}}{2}.$$

Thus, by the simple calculations one can easily find the secret key

$$x = \frac{1}{4}\log_\tau \left(\frac{2 - 2.5(t_1 - t_2) \pm \sqrt{6.25(t_1 - t_2)^2 + 5(t_1 - t_2)}}{2} \right)$$

of the cryptosystem, which means that the cryptographic method based on the Hadamard product of golden matrices is not resistable against the chosen-plaintext attack.

3.2 The chosen-plaintext attack against the generalized golden cryptographic method

We choose the following plaintext matrices

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad M_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \tag{16}$$

and the enciphering matrix G_k^{2x} (without loss of generality). The selection of the plaintexts as the matrices in (16) reduces possible 24 variants of the permuted initial matrix the following 4 ciphertexts

$$E_1(x,k) = M_1 \times G_k^{2x} = \begin{pmatrix} cF_k(2x+1) & sF_k(2x) \\ 0 & 0 \end{pmatrix},$$

$$E_2(x,k) = M_2 \times G_k^{2x} = \begin{pmatrix} sF_k(2x) & cF_k(2x+1) \\ 0 & 0 \end{pmatrix},$$

$$E_3(x,k) = M_3 \times G_k^{2x} = \begin{pmatrix} 0 & 0 \\ cF_k(2x+1) & sF_k(2x) \end{pmatrix},$$

$$E_4(x,k) = M_4 \times G_k^{2x} = \begin{pmatrix} 0 & 0 \\ sF_k(2x) & cF_k(2x+1) \end{pmatrix}.$$

Thus, the key of the cryptosystem can be found by the solution of the following system

$$\begin{cases} sF_k(2x) = t_1 \\ cF_k(2x+1) = t_2 \\ cF_k(2x-1) = t_3 \end{cases} \tag{17}$$

of non-linear equations, where t_1, t_2 and t_3 are known real numbers. Further, we prove that the solutions of the system (17) can be found by using simple calculations.

By the definitions of $sF_k(x)$ and $cF_k(x)$, the system (17) can be written as

$$\begin{cases} \sigma_k^{2x} - \sigma_k^{-2x} = t_1(\sigma_k + \sigma_k^{-1}) \\ \sigma_k^{2x+1} + \sigma_k^{-2x-1} = t_2(\sigma_k + \sigma_k^{-1}) \\ \sigma_k^{2x-1} + \sigma_k^{-2x+1} = t_3(\sigma_k + \sigma_k^{-1}). \end{cases} \tag{18}$$

If we multiply the first equation of the system (18) by σ_k^{-1}, and add it to the second equation, the equation

$$\sigma_k^{2x-1} + \sigma_k^{2x+1} = (\sigma_k + \sigma_k^{-1})(t_1\sigma_k^{-1} + t_2)$$

is resulted. Further

$$\sigma_k^{2x}(\sigma_k + \sigma_k^{-1}) = (\sigma_k + \sigma_k^{-1})(t_1\sigma_k^{-1} + t_2),$$

and finally

$$\sigma_k^{2x} = (t_1\sigma_k^{-1} + t_2). \tag{19}$$

On the other hand, if we multiply the first equation of (18) by σ_k, and add the obtained equation and the third equation, then

$$\sigma_k^{2x-1} + \sigma_k^{2x+1} = (\sigma_k + \sigma_k^{-1})(t_1\sigma_k + t_3).$$

By the similar calculations above, we obtain

$$\sigma_k^{2x} = (t_1\sigma_k + t_3). \tag{20}$$

From the equations (19) and (20),

$$t_1\sigma_k^{-1} + t_2 = t_1\sigma_k + t_3,$$

and

$$t_1\sigma_k^2 + (t_3 - t_2)\sigma_k - t_1 = 0.$$

Since $D = (t_3 - t_2)^2 + 4t_1^2 \geq 0$,

$$\sigma_k = \frac{t_2 - t_3 \pm \sqrt{(t_3 - t_2)^2 + 4t_1^2}}{2t_1}. \tag{21}$$

Thus the value of σ_k can be easily calculated from the known variables t_1, t_2 and t_3.

As

$$\sigma_k = \frac{k + \sqrt{k^2 + 4}}{2},$$

it is easy to see that

$$k = \frac{\sigma_k^2 - 1}{\sigma_k}. \tag{22}$$

From (20) (or from 19), we can calculate the value of x, i.e.,

$$x = \frac{1}{2}\log_{\sigma_k}(t_1\sigma_k + t_3) \text{ (or } x = \frac{1}{2}\log_{\sigma_k}(t_1\sigma_k^{-1} + t_2)). \tag{23}$$

Thus the secret key $\{k, x\}$ is obtained, which shows that the generalized golden cryptosystem is also vulnerable to the chosen-plaintext attack.

4 Conclusions

We have showed that the generalized golden cryptography and the golden cryptography with Hadamard products are not resistable against the chosen-plaintext attack. We have not mentioned the security of the cryptographic methods proposed in [2] and [9] intentionally, as they are very simple and it is very easy to show their insecurity against the chosen-plaintext attack. We leave the proofs of this statement to an eager reader.

Acknowledgements

This work was partially supported by University Putra Malaysia via RUGS 05-01-10-0896RU.

References

[1] S. Falcón and Á. Plaza, The k-Fibonacci hyperbolic functions, *Chaos, Solutions and Fractals*, Vol. **38** (2008), 409–420.

[2] Ernatuti, R. Salim, Sulistyo, The applications of "ELC numbers" to golden cryptography, *The Fifth International Conference on Information and Communication technology and Systems*, 2009, 329–334.

[3] A. Nally, On the Hadamard product of Fibonacci Q^n matrix and Fibonacci Q^{-n} matrix, *Int. J. Contemp. Math Sciences,* Vol. **1**, No. **16** (2006), 753 – 761.

[4] A. Nally, On the Hadamard product of golden matrices, *Int. J. Contemp. Math Sciences,* Vol. **2**, No. **11** (2007), 537 – 544.

[5] A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography, CRC Press*, Boca Raton, 1996.

[6] A. Rey and G. Sánchez, On the security of the "golden cryptography, *International Jounal of Network Security*, Vol. **7**, No. **3** (2008), 448–450.

[7] A. Stakhov, The "golden matrices and a new kind of cryptography, *Chaos, Solutions and Fractals*, Vol. 32 (2007), 1138–1146.

[8] A. Stakhov, Gazale formulas, a new class of the hyperbolic Fibonacci and Lucas functions, and the improved method of the "golden" cryptography, *Moscow: Academy of Trinitarism,* **77-6567**, publication **14098** (2006), 1138–1146.

[9] K.R. Sudha, A. Chandra Sekhar, Prasad Reddy PVGD, Cryptography protection of digital signals using some recurrence relations, *Int. J. of Comp. Sci. and Network Security*, Vol. **7**, No. **5** (2007), 203–207.

Received: April, 2011