On the Security of “Golden” Cryptography

Ángel Martín del Rey[1] and Gerardo Rodríguez Sánchez[2]
(Corresponding author: Ángel Martín del Rey)

GICSIMAD, Department of Applied Mathematics, Universidad de Salamanca
Avda. de los Hornos Caleros 50, 05003-Ávila, Spain[1] (Email: {delrey, gerardo}@usal.es)
Avda. Cardenal Cisneros 34, 49022-Zamora, Spain[2]

(Received May 30, 2007; revised and accepted Dec. 5, 2007)

Abstract

In this paper the security of “golden” cryptography, which has been proposed recently, is tackled. Specifically, it is shown that the security of such cryptosystem is trivially compromised as it does not pass one of the basic cryptanalytic attacks: the chosen plaintext attack.

Keywords: Cryptanalysis, cryptography, fibonacci matrix

1 Introduction and Preliminaries

In [3] a new kind of cryptography is created: the “golden” cryptography. It is based on the use of “golden” matrices which are the generalization of the classical Fibonacci Q-matrix for continuous domain.

Specifically, if τ is the golden proportion and x is a continuous variable, the “golden” matrices are defined as follows:

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

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

where

$$\mathrm{sFs}\,(x) = \frac{\tau^x - \tau^{-x}}{\sqrt{5}}, \quad \mathrm{cFs}\,(x) = \frac{\tau^x + \tau^{-x}}{\sqrt{5}}, \quad (3)$$

are the symmetrical hyperbolic Fibonacci sine and the symmetrical hyperbolic Fibonacci cosine, respectively. Symmetrical hyperbolic Fibonacci functions are connected to Fibonacci numbers as follows:

$$F_n = \begin{cases} \mathrm{sFs}\,(n), & \text{if } n = 2k \\ \mathrm{cFs}\,(n), & \text{if } n = 2k+1 \end{cases}$$

where $n, k \in \mathbb{Z}$. Moreover, the inverse matrices of “golden” Matrices (1) and (2) are:

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

For a more detailed description of such functions we refer the reader to [2, 3].

The cryptographic protocol to encrypt messages proposed in [3] is as follows: Let

$$M = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \mathcal{M}_2\,(\mathbb{R}),$$

be the plaintext and set P_i one of the $4! = 24$ possible permutations of the coefficients of the matrix M. If we choose the “golden” Matrices (1) and (2) as the enciphering matrices, then the cryptograms obtained are $E_1\,(x) = M \times Q^{2x}$ or $E_2\,(x) = M \times Q^{2x+1}$, depending on the enciphering matrix used. Note that the secret key is the pair (P_i, x). To recover the original message M, one has to use the corresponding inverse matrix as the deciphering matrix: $M = E_1\,(x) \times Q^{-2x}$ or $M = E_2\,(x) \times Q^{-(2x+1)}$.

A fundamental premise in Cryptography (see, for example, [1, 4]) is that the cryptanalyst knows the cryptosystem being used (Kerckhoffs’ principle); that is, when two parties (the sender and the receiver) want to communicate securely using a cryptosystem, the only thing that they keep secret is the secret key. Obviously, one can gain additional security by keeping the cryptographic protocol secret but one should not base the security of the entire protocol on this approach.

At the very least, a cryptosystem is considered secure if it resists the following basic types of attacks (see, for example, [1]):

- *Ciphertext only attack.* The cryptanalyst tries to obtain the secret key or plaintext by only observing the cryptogram. Any encryption scheme vulnerable to this attack is considered to be completely insecure.
- *Known-plaintext attack.* The cryptanalyst has several plaintexts and their corresponding cryptograms and tries to recover the secret key from them.
- *Chosen-plaintext attack.* The cryptanalyst is able to choose the plaintext and to obtain the corresponding cryptogram. Subsequently, the adversary uses some

information deduced in order to obtain the secret key used.

- *Chosen-ciphertext attack.* The cryptanalyst selects the cryptogram (or ciphertext) and is then given the corresponding plaintext. This type of attacks are specially suitable for asymmetric cryptography.

In this work, only chosen-plaintext attack is considered as known-plaintext attack and ciphertext only attack are particular cases of the first one.

In the next section, it is shown that the cryptographic protocol proposed in [3] is not secure against chosen-plaintext attack.

2 The Chosen-Plaintext Attack of the Protocol

Let us consider the following four known pairs of plaintext/cryptogram:

$$\{M_1, E_1(x)\}, \{M_2, E_2(x)\}, \{M_3, E_3(x)\}, \{M_4, E_4(x)\},$$

such that

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

Without loss of generality, we can also soppose that the enciphering matrix is Q^{2x}. Then:

$$\begin{aligned} E_1(x) &= M_1 \times Q^{2x} = \begin{pmatrix} \mathrm{cFs}(2x+1) & \mathrm{sFs}(2x) \\ 0 & 0 \end{pmatrix} \\ E_2(x) &= M_2 \times Q^{2x} = \begin{pmatrix} \mathrm{sFs}(2x) & \mathrm{cFs}(2x-1) \\ 0 & 0 \end{pmatrix} \\ E_3(x) &= M_3 \times Q^{2x} = \begin{pmatrix} 0 & 0 \\ \mathrm{cFs}(2x+1) & \mathrm{sFs}(2x) \end{pmatrix} \\ E_4(x) &= M_4 \times Q^{2x} = \begin{pmatrix} 0 & 0 \\ \mathrm{sFs}(2x) & \mathrm{cFs}(2x-1) \end{pmatrix} \end{aligned}$$

That is, the following system of non-linear equations is obtained:

$$\left\{ \begin{array}{l} \mathrm{sFs}(2x) = k_1 \\ \mathrm{cFs}(2x+1) = k_2 \\ \mathrm{cFs}(2x-1) = k_3 \end{array} \right. \tag{4}$$

where $k_1, k_2, k_3 \in \mathbb{R}$ are known variables.

We choose these matrices, M_1, M_2, M_3 and M_4, since if all coefficients of the plaintext are 0 except for only one, which is 1, then the $4! = 24$ possible variants of the permuted initial matrix are reduced to these four matrices. Consequently, the effect of the permutation is computationally irrelevant.

Using Equation (3), the first equation of the System (4) yields:

$$z^2 - k_1\sqrt{5}z - 1 = 0,$$

where $z = \tau^{2x}$. Their solutions are:

$$z = \frac{k_1\sqrt{5} \pm \sqrt{5k_1^2 + 4}}{2},$$

and, as a simple calculus shows, the real value for x is:

$$x = \frac{1}{2}\log_\tau\left(\sqrt{\frac{k_1\sqrt{5} + \sqrt{5k_1^2 + 4}}{2}}\right)$$

which also satisfies the second and third equations of the system. As a consequence, the secret key x is obtained.

3 Conclusions

In this paper it is shown that the cryptosystem proposed in [3] and based on the use of golden matrices is not secure. Specifically, it is not robust against chosen-plaintext attack which is an essential cryptanalytic attack.

Acknowledgements

This work has been partially supported by the Consejería de Educación y Cultura of Junta de Castilla y León (Spain) under grant SA110A06, and by Ministerio de Educación y Ciencia (Spain), under grant TSI2007-62657.

References

[1] A. Menezes, P. C. V. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, Boca Raton, Florida: CRC Press, 1996.

[2] A. P. Stakhov, and B. Rozin, “On a new class of hyperbolic function,” *Chaos, Solitons and Fractals*, vol. 23, pp. 379-389, 2004.

[3] A. P. Stakhov, “The “golden” matrices and a new kind of cryptography,” *Chaos, Solitons and Fractals*, vol. 32, pp. 1138-1146, 2007.

[4] D. R. Stinson, *Cryptography: Theory and Practice*, Second Edition, Boca Raton, Florida: Chapman & Hall/CRC, 2002.

Ángel Martín del Rey obtained his Ph. D. in Mathematics from National University of Distance Learning (UNED) in 2000. From 1997 until 2001 he was assistant professor of the Department of Applied Mathematics, University of Salamanca, and since 2002 he has been associated professor of the same department. His current research interests include image processing, cellular automata, cryptography and information security.

Gerardo Rodríguez Sánchez obtained his Ph. D. in Mathematics from Universidad de Salamanca in 1996. He is full professor of Applied Mathematics Department in Universidad de Salamanca. He has participated in 17 projects of investigation financed by autonomic, national and European organizations public and is co-author of 34 publications of national and international character, including 3 educational books. His current research interests include image processing, cellular automata and cryptography.