Cryptanalysis of a discrete-time synchronous chaotic encryption system

David Arroyo [a,*], Gonzalo Alvarez [a,*], Shujun Li [b], Chengqing Li [c] and Juana Nunez [a]

[a] *Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas, Serrano 144, 28006 Madrid, Spain*

[b] *FernUniversität in Hagen, Lehrgebiet Informationstechnik, Universitätsstraße 27, 58084 Hagen, Germany*

[c] *Department of Electronic Engineering, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong SAR, China*

Abstract

Recently a chaotic cryptosystem based on discrete-time synchronization has been proposed. Some weaknesses of that new encryption system are addressed and exploited in order to successfully cryptanalyze the system.

Key words: Chaotic encryption, Hénon map, known-plaintext attack, cryptanalysis
PACS: 05.45.Ac, 47.20.Ky.

1 Introduction

During the last two decades chaotic systems have been broadly used in cryptographic applications [1–5] exploiting its ergodicity, sensitivity to initial con-

[*] Corresponding authors: David Arroyo (david.arroyo@iec.csic.es), Gonzalo Alvarez (http://www.gonzaloalvarez.com).

ditions, mixing property, and simple analytic description but high complex behavior. However, many of the proposed schemes show important security weaknesses as a result of a bad or nonexistent key definition and bad or nonexistent key space specification [6–14].

In this letter the cryptosystem proposed in [15] is analyzed and some deficiencies are pointed out. This cryptosystem is built upon the Hénon map, defined as

$$\begin{aligned} x_{k+1} &= 1 - a \cdot x_k^2 + y_k, \\ y_{k+1} &= b \cdot x_k \ . \end{aligned} \tag{1}$$

The plaintext is divided into blocks $\{m_k\}_{k=0}^{N-1}$, where each block has M bits. The encryption of the plain-blocks is carried out for $k = 0 \sim N-1$ in turn. For the k-th plain-block m_k, the corresponding cipher-block is x_{k+1}, which is calculated through Eq. (1) by setting

$$a = \psi\left(m_k\right) \cdot \mu_1\left(y_k\right), \tag{2}$$

$$b = \mu_2\left(y_k\right), \tag{3}$$

where $\psi(x)$ is a bijective function assuring that a is a valid parameter of Eq. (1) and $\mu_i(x)$, $i \in \{1,2\}$, are piecewise linear functions defined as

$$\mu_i(x) = \begin{cases} b_{i,1}(x), & \text{if } a_{i,1}(x) < |x| \leq a_{i,2}(x), \\ \cdots & \cdots \\ b_{i,j}(x), & \text{if } a_{i,j}(x) < |x| \leq a_{i,j+1}(x), \\ \cdots & \cdots \\ b_{i,L}(x), & \text{if } a_{i,L}(x) < |x| \leq a_{i,L+1}(x), \end{cases} \tag{4}$$

where $a_{i,j}(x)$ is any function making one and only one condition on the right hand of Eq. (4) satisfied for any x, and $b_{i,j}(x)$ is any function making a and b valid control parameters of Eq. (1).

At the receiver, the decryption of m_k is carried out synchronously in the following two steps:

- Generate intermediate variable $\psi(m_k)$ by Eq. (5);

$$\psi\left(m_k\right) = \frac{1 - x_{k+1} + y_k}{\mu_1\left(y_k\right) \cdot x_k^2}, \tag{5}$$

$$y_{k+1} = \mu_2\left(y_k\right) x_k \ . \tag{6}$$

- Get $m_k = \psi^{-1}(\psi(m_k))$, where $\psi^{-1}(x)$ is the inverse function of $\psi(x)$.

As claimed in [15, Sec. 2], the secret key of the cryptosystem includes the following three subkeys:

(1) The initial condition of the second component of the Hénon map, i.e., y_0.
(2) The M-ary switching key (MSK) mechanism which is the function $\psi(x)$.
(3) The pseudo-random switching key (PRSK) mechanism which is given by the functions $\mu_1(x)$ and $\mu_2(x)$.

Based on the above general form of the proposed cryptosystem, the original authors present a concrete configuration: $M = 48$, $\psi(x)$, $\mu_1(x)$ and $\mu_2(x)$ are set in Eqs. (7), (8), (9) respectively.

$$\psi\left(x\right) = A + Bx = 1.77 \cdot 10^{-2} + 1.39 \cdot 10^{-15} \cdot x, \tag{7}$$

$$\mu_1(x) = \begin{cases} 1.27 + \frac{x}{10.2}, & \text{if } |x| \le 0.1 + \frac{x}{1.3}, \\ 1.28 + \frac{x}{10.2}, & \text{if } 0.1 + \frac{x}{1.3} < |x| \le 0.2 + \frac{x}{1.3}, \\ 1.29 + \frac{x}{10.2}, & \text{if } 0.2 + \frac{x}{1.3} < |x| \le 0.3 + \frac{x}{1.3}, \\ 1.30 + \frac{x}{10.2}, & \text{otherwise.} \end{cases} \tag{8}$$

$$\mu_2(x) = \begin{cases} 0.29 + \frac{x}{10}, & \text{if } |x| \le 0.1 + \frac{x}{1.1}, \\ 0.30 + \frac{x}{10}, & \text{if } 0.1 + \frac{x}{1.1} < |x| \le 0.2 + \frac{x}{1.1}, \\ 0.31 + \frac{x}{10}, & \text{if } 0.2 + \frac{x}{1.1} < |x| \le 0.3 + \frac{x}{1.1}, \\ 0.32 + \frac{x}{10}, & \text{otherwise.} \end{cases} \tag{9}$$

Obviously, Eqs. (8), (9) are equivalent to Eqs. (10), (11) respectively.

$$\mu_1(x) = \begin{cases} 1.27 + \frac{x}{10.2}, & \text{if } \frac{-13}{230} \le x \le \frac{13}{30}, \\ 1.28 + \frac{x}{10.2}, & \text{if } \frac{-13}{115} \le x < \frac{-13}{230}; \frac{13}{30} < x \le \frac{13}{15}, \\ 1.29 + \frac{x}{10.2}, & \text{if } \frac{-39}{230} \le x < \frac{-13}{115}; \frac{13}{15} < x \le \frac{13}{10}, \\ 1.30 + \frac{x}{10.2}, & \text{otherwise.} \end{cases} \tag{10}$$

$$\mu_2(x) = \begin{cases} 0.29 + \frac{x}{10}, & \text{if } \frac{-11}{210} \le x \le \frac{11}{10}, \\ 0.30 + \frac{x}{10}, & \text{if } \frac{11}{10} < x \le \frac{22}{10}; \frac{-11}{105} \le x < \frac{-11}{210}, \\ 0.31 + \frac{x}{10}, & \text{if } \frac{22}{10} < x \le \frac{33}{10}; \frac{-11}{70} < x < \frac{-11}{105}, \\ 0.32 + \frac{x}{10}, & \text{otherwise.} \end{cases} \tag{11}$$

This paper focuses on the security analysis of the cryptosystem under the above specific configuration. For more details about its working, the reader is referred to [15]. The rest of the paper is organized as follows. In the next section some design problems of the cryptosystem are emphasized. In the following section different attacks are described. Finally, some concluding remarks and conclusions are given.

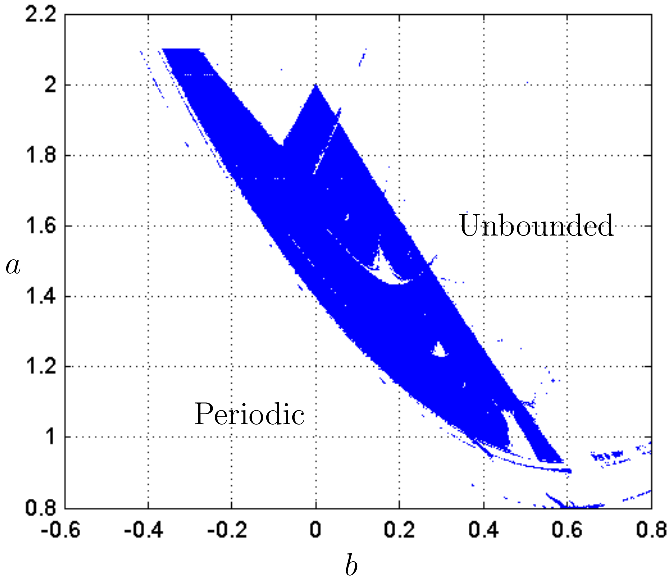


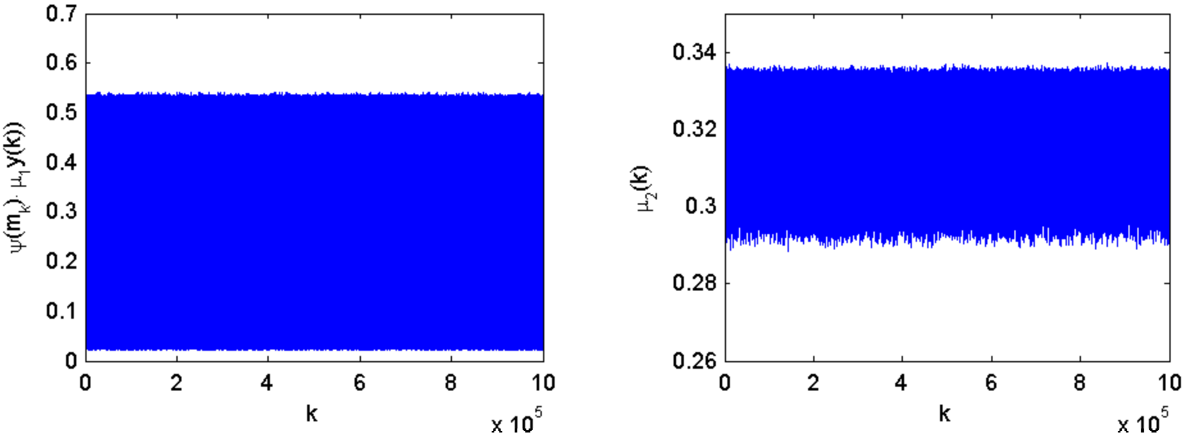
Fig. 1. Chaotic region for the Hénon map.

2 Design weaknessses

2.1 Loss of chaoticity of the Hénon map

As remarked in [16, Rules 4 and 5], a well designed cryptosystem is characterized by a precise definition of the secret key and a cryptographically large key space. In [15] the secret key depends on the selection of the functions that build either the MSK or PRSK mechanisms. However, there is no clue in [15] about how to find those functions. It is only demanded that the equations in Eq. (1) are always bounded. This is a big problem when considering the key exchange and the cryptosystem hardware implementation [16, Rules 1 and 3]. The cryptosystem's security analysis of [15, Sec. 6] demonstrates that the decryption process demands that the PRSK and MSK settings are exactly the same as the ones used during the encryption step. Indeed, it makes difficult to guess the key value, but it also implies the secret key exchange has to be very precise. Provided that the design for MSK is left open and PRSK is designed using real numbers, the key exchange in the cryptosystem proposed in [15] is going to be very complex.

Moreover, it is not easy to find proper functions so that the system described by Eq. (1) shows a chaotic behavior. Furthermore, the functions given in [15] as an example for $M = 48$, i.e, Eqs. (7), (8) and (9), do not allow the cryptosystem to work in the chaotic region of the Hénon map. A common method to determine whether a dynamical system with the given control parameters is chaotic is to calculate its maximum Lyapunov exponent. Figure 1 depicts the set of points (a, b) for which the maximal Lyapunov exponent of the Hénon map is positive.



(a)

(b)

Fig. 2. Pseudo-random switching key analysis: a) a values for random plaintext; b) b values for random plaintext.

When a random plaintext generated by the rand() function of Matlab is encrypted with Eqs. (1), (7), (8), (9), $M = 48$, $x(0) = 0.4$ and $y(0) = 0.5$, the product $\psi(m_k) \cdot \mu_1(y_k)$ is always out of the chaotic region (see Fig. 2).

Figure 3 shows that, after a number of transient values, the ciphertext reaches a constant value or a pair of constant values. This is a result of the cryptosystem being always working in periodic windows of the Hénon map. The condition for other definitions of $\psi(x)$, $\mu_1(x)$ and $\mu_2(x)$ may be better, but it is difficult to make the system remain always in the chaotic region of the Hénon map. The best solution would be to use other maps with a broader chaotic region.

2.2 Deficient compression performance

In [15] it is mentioned that the cryptosystem under study gives a ciphertext that requires a smaller storage size than the one for the plaintext, since each message block of M bits is encrypted into a single-precision floating-point number (a number that is 32-bits long). Therefore, if M is greater than 32 it is expected to reduce the storage size for the resulting ciphertext comparing to the one for the plaintext. However, this is not true.

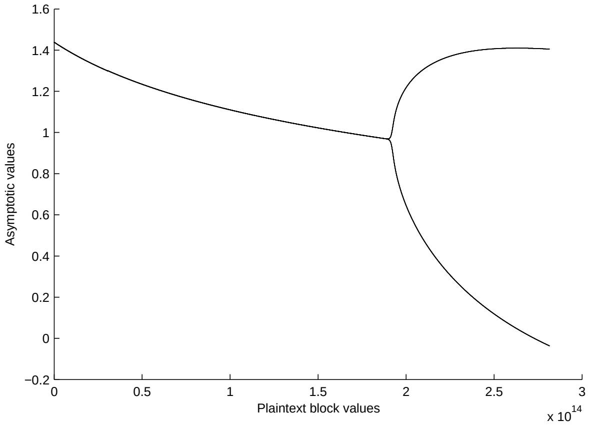


Fig. 3. Ciphertext values for plaintext blocks with a fixed value.

The function $\psi(x)$ has to be a bijective function, i.e., each output value of this function is associated to one and only one input value. If m_k is a 32-bit value it means that there are 2^{32} possible values for $\psi(m_k)$. The plaintext block m_k is M-bits long and consequently there are 2^M possible values for m_k. Therefore, if $M > 32$ then $\psi(m_k)$ is not a bijective function. This problem was verified dealing with the cryptosystem referred by Eqs. (1), (7), (8), (9), $M = 48$, $x_0 = 0.4$ and $y_0 = 0.5$. A random 10^6-block plaintext was encrypted and decrypted being all the operations computed with single-precision floating-point numbers, i.e., every number was 32-bit long. The decrypted text was compared to the original plaintext and there was a 28% of bits different from the original ones. The bit error rate is approximately one third, as expected given that 32 bits are used to represent 48-bit values. The authors of [15] might have been using double-precision floating-point (64-bit) numbers in their experiments, thus overlooking this fact.

2.3 Decryption errors due to finite precision computations

The decryption of the ciphertext x_k involves the inversion of $\psi(m_k)$. In the sample implementation given in [15], $\psi(m_k)$ is determined by Eq. (7) and the 48-bit plaintext block is recovered by inverting Eq. (7):

$$m_k = \frac{\psi\left(m_k\right) - A}{B}, \tag{12}$$

where $\psi\left(m_k\right)$ has been calculated from the ciphertext by using Eq. (5). If the value recovered from Eq. (5) is not exactly the one used during the encryption process for m_k, then the value given by Eq. (12) is not an integer. This happens if all the mathematical operations are in finite precision, as it occurs in the encryption scheme under examination. It was actually verified that the result of Eq. (12) is never an integer. Thus the value returned by the decryption process needs to be rounded in order to recover the original information. This was not mentioned in [15] and poses the following problem: some blocks of the original plaintext are incorrectly recovered from the ciphertext, i.e., it exists a residual bit error rate derived from the fact that every computation is in finite precision, as shown in Fig. 4. The cryptosystem's security analysis made in [15, Sec. 6] emphasizes that a cryptanalyst will require identifying a number of $\psi(k)$ output values with high certainty and precision. Figure 4 informs that this high certainty and precision requirement concerns not only the cryptanalyst but also the receiver.

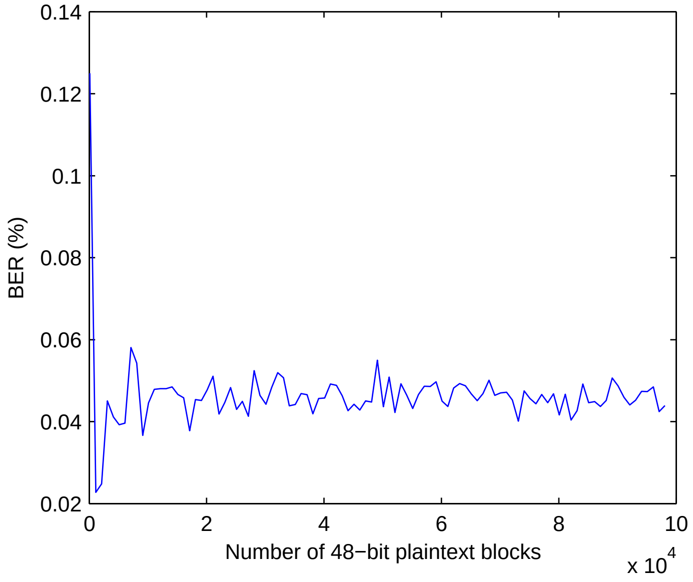


Fig. 4. Bit Error Rate for $M = 48$ and different plaintext lengths.

3 Partial key recovery attack

In the context of a secure and robust encryption system it is assumed that the partial knowledge of the key does not reveal information about the rest of the key and, as a result, the cryptosytem performance is not harmed [16, Rule 7]. However, in the scenario drawn by [15], partial knowledge of the key can be used to obtain the rest of the key. Along the section we describe a known-plaintext attack [17, p. 25], where it is possible to reconstruct the supporting PRSK mechanism functions and y_0, assuming that the attacker has access to $\psi(m_k)$ for every possible value of m_k.

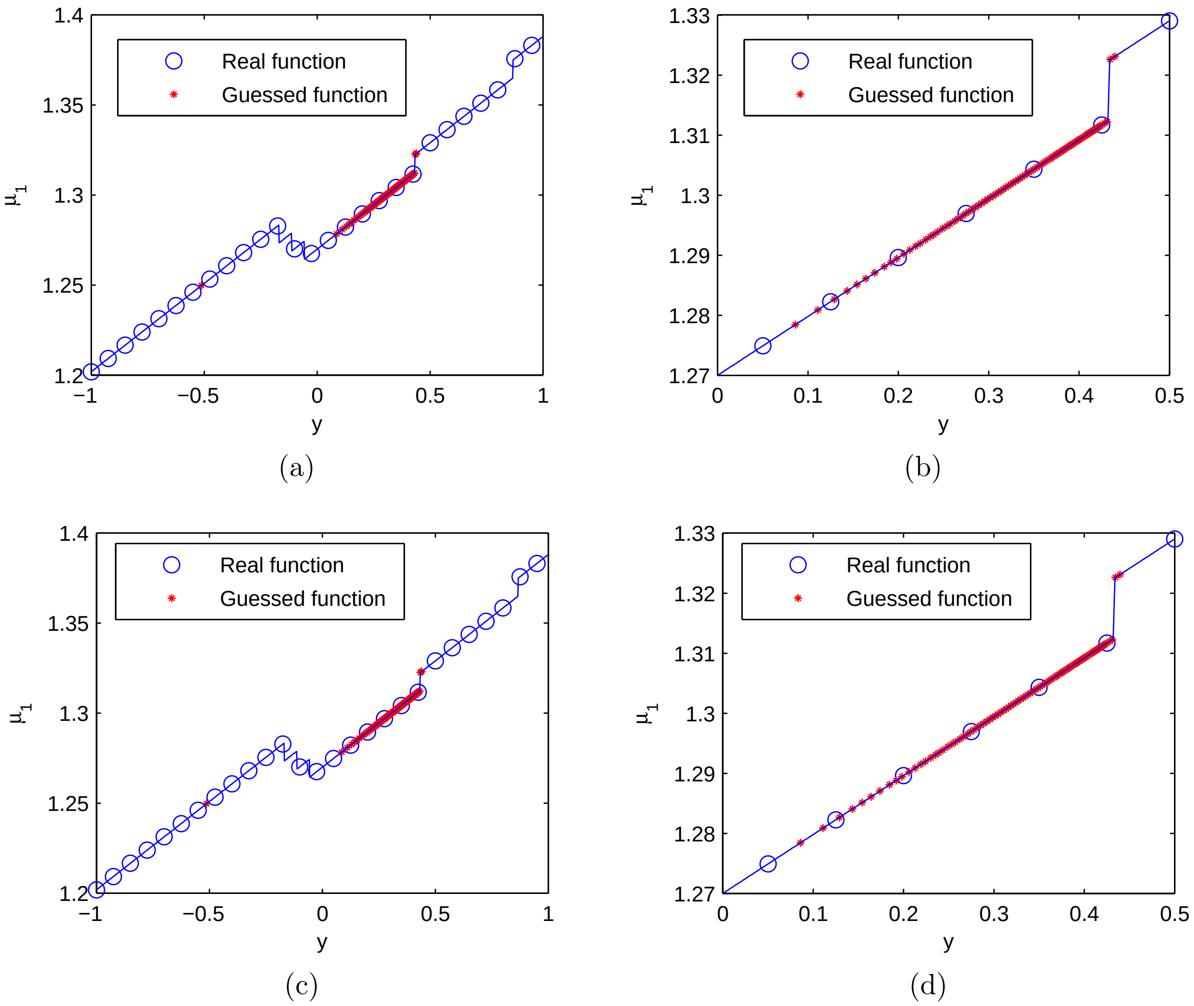
Given two plaintexts $\{m_{1,k}\}_{k=0}^{N-1}$, $\{m_{2,k}\}_{k=0}^{N-1}$, then

$$x_{1,1} = 1 - \psi(m_{1,0}) \cdot \mu_1(y_0) \cdot x_0^2 + y_0, \tag{13}$$
$$x_{2,1} = 1 - \psi(m_{2,0}) \cdot \mu_1(y_0) \cdot x_0^2 + y_0 \tag{14}$$

and

$$x_{1,k+1} = 1 - \psi(m_{1,k}) \cdot \mu_1(y_k) \cdot x_{1,k}^2 + y_k, \tag{15}$$
$$x_{2,k+1} = 1 - \psi(m_{2,k}) \cdot \mu_1(y_k) \cdot x_{2,k}^2 + y_k, \tag{16}$$
$$y_k = \mu_2(y_{k-1}) \cdot x_{k-1}, \tag{17}$$

where $k \geq 1$.



(a) (b) (c) (d)

Fig. 5. Recovered and original functions for the PRSK mechanism when they are designed as in [15]: a) $\mu_1(y)$ for $y_0 = 0.9402036$; b) image zoom for $\mu_1(y)$ and $y_0 = 0.9402036$; c) $\mu_1(y)$ for $y_0 = -0.5123493$; and d) image zoom for $\mu_1(y)$ and $y_0 = -0.5123493$.

Subtracting Eq. (13) from Eq. (14), one obtains:

$$\begin{aligned} x_{2,1} - x_{1,1} &= \psi(m_{1,0}) \cdot \mu_1(y_0) \cdot x_0^2 - \psi(m_{2,0}) \cdot \mu_1(y_0) \cdot x_0^2 \\ &= (\psi(m_{1,0}) - \psi(m_{2,0})) \cdot \mu_1(y_0) \cdot x_0^2. \end{aligned} \tag{18}$$

In the following discussion, it is shown how to recover the secret key, assuming that $\psi(x)$ is known.

From Eq. (18), one has

$$r_1 = \frac{x_{2,1} - x_{1,1}}{\psi(m_{1,0}) - \psi(m_{2,0})}. \tag{19}$$

Because the encryption is generally carried out in floating point operation, the quantization error is very small in most cases and can be ignored. As a result, $r_1 = \mu_1(y_0) \cdot x_0^2$, which implies that $y_0 = x_{1,1} - 1 + \psi(m_{1,0}) \cdot r_1$, and $\mu_1(y_0) = \frac{r_1}{x_0^2}$.

Subtracting Eq. (15) from Eq. (16):

$$\widetilde{\mu}_1(y_k) = \frac{x_{2,k+1} - x_{1,k+1}}{\psi(m_{1,k}) \cdot x_{1,k}^2 - \psi(m_{2,k}) \cdot x_{2,k}^2} \tag{20}$$

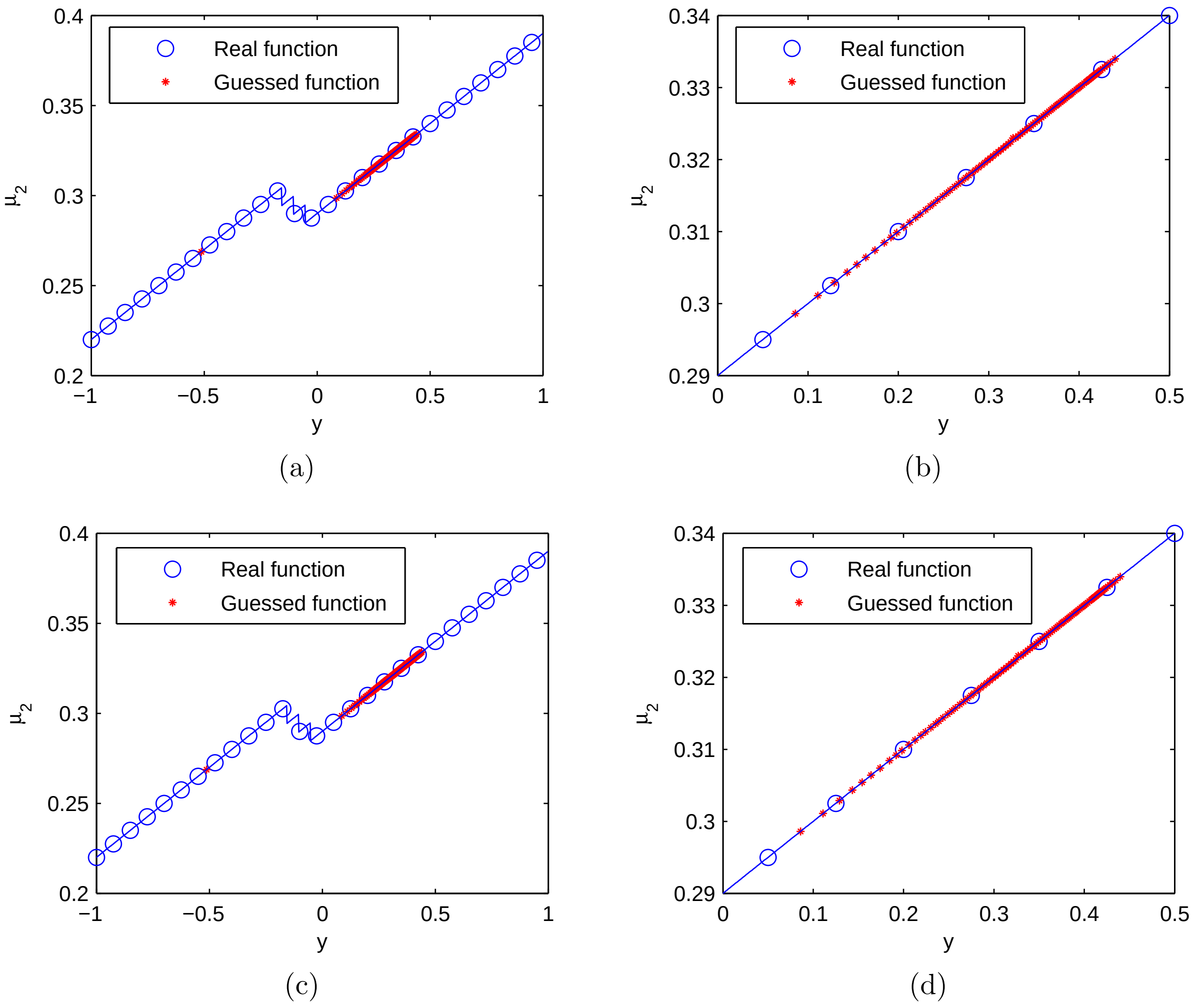
From Eq. (17):

$$\widetilde{\mu}_2(y_{k-1}) = \frac{x_{1,k+1} - 1 + \psi(m_{1,k}) \cdot \widetilde{\mu}_1(y_k) \cdot x_{1,k}^2}{x_{k-1}}. \tag{21}$$

As mentioned above, by ignoring the quantization error, we have $\widetilde{\mu}_1(y_k) = \mu_1(y_k)$ and $\widetilde{\mu}_2(y_{k-1}) = \mu_2(y_{k-1})$.

Repeating this procedure for $k = 1, \ldots, N$ it is possible to reconstruct $\mu_1(y_k)$ and $\mu_2(y_k)$.

In order to prove the proposed known-plaintext attack, 10000 points for $\mu_1(y_k)$ and $\mu_2(y_k)$ were calculated for $x_0 = 0.4,\ y_0 = 0.9402036$ and $x_0 = 0.4,\ y_0 = -0.5123493$. In Figs. 5 and 6 it is shown how it was possible to infer $\mu_1(y_k)$, $\mu_2(y_k)$ shape. This is due to the fact that the first component of the Hénon map employed in the encryption process is sent through the communication channel without applying any masking transformation. However, there exists an underlying quantization error in the recovering method due to the fact that all the mathematical operations are done in finite precision. It was verified that $\Delta(\mu_1) \sim 10^{-6}$ and $\Delta(\mu_2) \sim 10^{-7}$. Therefore, the exact μ_1 and μ_2 reconstruction demands an exhaustive search. On the other hand, Figs. 5 and 6 also show that during the encryption process $\mu_1(y_k)$ and $\mu_2(y_k)$ do not go



(a) (b)

(c) (d)

Fig. 6. Recovered and original functions for the PRSK mechanism when they are designed as in [15]: a) $\mu_2(y)$ for $y_0 = 0.9402036$; b) image zoom for $\mu_2(y)$ and $y_0 = 0.9402036$; c) $\mu_2(y)$ for $y_0 = -0.5123493$; and d) image zoom for $\mu_2(y)$ and $y_0 = -0.5123493$.

through all the possible values of the functions referred by Eqs. (8) and (9). In other words, it was verified that, during the encryption process, y_k never goes through all the possible input values for both functions. This is the reason why $\mu_1(x)$ and $\mu_2(x)$ can not be totally recovered, which has no impact on the efficiency of the cryptanalysis.

This attack has been carried out in a scenario where the attacker knows $\psi(x)$. Nevertheless, the cryptosystem allows other kinds of known-plaintext attacks where $\psi(x)$ is not known. For instance, Eq. (18) clearly reveals a leak of information from $\psi(x)$: one can assure that $\psi(x)$ is a linear function if the value of $x_{2,1} - x_{1,1}$ keep unchanged for different $(m_{1,0}, m_{2,0})$ pairs, where $(m_{1,0} - m_{2,0})$ is kept fixed. To be more precise, in view of Eqs. (5) and (6), different values of $\psi(x)$ may be calculated if the rest of the subkeys are known. The details of this attack are not given because it is an analogue of the one just described and because the weakness of the cryptosystem has been profusely proved.

4 Conclusions

In this paper some security and design problems of a chaotic cryptosystem based on discrete-time synchronization have been pointed out. First of all, it has been remarked the lack of a description about the key space and it has been also emphasized the difficulty of finding new keys in a cryptosystem as the one referred in [15]. Finally it has been shown that it is possible to break the cryptosystem when the keys are selected as in [15] using a known plaintext attack and assuming a partial knowledge of the key.

This analysis reveals that the choice of chaotic map is all important. Maps with irregular chaotic regions as those depicted in Fig. 1 should be avoided, in favor of maps with more uniform distributions. In this way the chaotic behavior for a wider range of parameters can be guaranteed. As has been shown, entering into periodic windows has negative impact on the algorithm's security.

Another important point to be emphasized is that both the key and key space should be thoroughly described and should be designed in a way as to facilitate the selection of valid keys.

Acknowledgments

The work described in this letter was partially supported by Ministerio de Educación y Ciencia of Spain, Research Grant SEG2004-02418. Shujun Li was supported by the Alexander von Humboldt Foundation, Germany.

References

[1] S. Li, Analyses and new designs of digital chaotic ciphers, Ph.D. thesis, School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China, available online at `http://www.hooklee.com/pub.html` (June 2003).

[2] T. Yang, A survey of chaotic secure communication systems, Int. J. Comp. Cognition 2 (2) (2004) 81–130.

[3] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Chaotic cryptosystems, in: L. D. Sanson (Ed.), Proc. 33rd Annual 1999 International Carnahan Conference on Security Technology, IEEE, 1999, pp. 332–338.

[4] L. Kocarev, Chaos-based cryptography: A brief overview, IEEE Circuits Syst. Mag. 1 (2001) 6–21.

[5] J. Amigo, L. Kocarev, J. Szczepanski, Theory and practice of chaotic cryptography, Phys. Lett. A 366 (3) (2007) 211–216.

[6] G. Alvarez, S. Li, Breaking an encryption scheme based on chaotic baker map, Phys. Lett. A 352 (1-2) (2006) 78–82.

[7] S. Li, G. Chen, K.-W. Wong, X. Mou, Y. Cai, Baptista-type chaotic cryptosystems: Problems and countermeasures, Phys. Lett. A 332 (5-6) (2004) 368–375.

[8] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of dynamic look-up table based chaotic cryptosystems, Phys. Lett. A 326 (3-4) (2003) 211–218.

[9] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of a discrete chaotic cryptosystem using external key, Phys. Lett. A 319 (3-4) (2003) 334–339.

[10] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of an ergodic chaotic cipher, Phys. Lett. A 311 (2-3) (2003) 172–179.

[11] S. Li, X. Mou, Z. Ji, J. Zhang, Y. Cai, Performance analysis of jakimoski-kocarev attack on a class of chaotic cryptosystems, Phys. Lett. A 307 (1) (2003) 22–28.

[12] G. Jakimoski, L. Kocarev, Analysis of some recently proposed chaos-based encryption algorithms, Phys. Lett. A 291 (6) (2001) 381–384.

[13] S. Li, X. Mou, Y. Cai, Improving security of a chaotic encryption approach, Phys. Lett. A 290 (3-4) (2001) 127–133.

[14] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of a chaotic encryption system, Phys. Lett. A 276 (1) (2000) 191–196.

[15] C. Y. Chee, D. Xu, Chaotic encryption using dicrete-time synchronous chaos, Physics Letters A 348 (3-6) (2006) 284–292.

[16] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, International Journal of Bifurcation and Chaos 16 (8) (2006) 2129–2151.

[17] D. Stinson, Cryptography: Theory and Practice, CRC Press, 1995.