Military Technical College
Kobry Elkobbah,
Cairo, Egypt

2nd International Conference on
Electrical Engineering
ICEENG 99

# PRIVATE-KEY BLOCK CRYPTOSYSTEM USING TWO-DIMENSIONAL CHAOTIC MAP

Alaa Fahmy[1] Salah El Agooz[1] Mohamed A. H. Eleiwa[1]

## ABSTRACT

In contradiction to one-dimensional mapping, higher-dimensional mapping may be conservative (volume preserving) as well as dissipative (volume contracting), invertible as well as non-invertible, depending on the parameter in the model. In this paper, we use two-dimensional chaotic maps, specifically Henon map [1], for compression as well as encryption. The Henon map is used to construct a private-key block cryptosystem.

## 1. INTRODUCTION

In this way, we emphasize how to make use of chaos in cryptography. The unique character of chaotic dynamics may be seen most clearly by imagining the system to be started twice, but from slightly different initial conditions. For non-chaotic system this small initial difference leads only to an error in prediction that grows linearly with time. For chaotic systems, on the other hand, the error grows exponentially in time. Therefore, the state of the system is essentially unknown after a very short time.

## 2. TWO-DIMENSIONAL CHAOTIC MAP (HENON MAP)

Henon [1] first studied the two-dimensional map of the plane

$$\mathbf{H}_{\mathbf{b}}:\ \mathbf{x}_{\mathbf{n+1}} = 1 - \mathbf{a}\mathbf{x}_{\mathbf{n}}^{2} + \mathbf{y}_{\mathbf{n}}\ , \qquad \mathbf{y}_{\mathbf{n+1}} = \mathbf{b}\mathbf{x}_{\mathbf{n}}. \tag{1}$$

Henon map is the simplest extension of the logistic map [2] (one-dimensional map) to two-dimensional map. This map is one-to-one mapping that transforms the (x, y) plane into itself. Its jacobian is given by:

$$\mathbf{J} = \partial\,(\mathbf{x}_{\mathbf{n+1}},\mathbf{y}_{\mathbf{n+1}}) / \partial\,(\mathbf{x}_{\mathbf{n}},\mathbf{y}_{\mathbf{n}}) = \begin{vmatrix} -2\mathbf{a}\mathbf{x}_{\mathbf{n}} & 1 \\ & \\ \mathbf{b} & 0 \end{vmatrix} = -\,\mathbf{b}. \tag{2}$$

[1] PH.D., Electrical Engineering Dept., Military Technical College, Cairo, Egypt.

When the determinant | J | = b= 1, the map preserves the area and thus imitates a conservative dynamical process. If | b | <1, the contraction of the area may be thought to be due to the presence of dissipation. If b = 0, we recover the logistic map. Thus, Henon map can be decomposed into three separate maps, which can be written as:

$$\mathbf{H}_b = \mathbf{H}_3 \circ \mathbf{H}_2 \circ \mathbf{H}_1. \tag{3}$$

The map $H_1$: (x, y) → (x, 1- $ax^2$ +y) is an area preserving, non-linear bending. The map $H_2$: (x, y) → (bx, y) is a contraction in the "x" direction. While, the map $H_3$ : (x, y) → (y, x) maps the bent and contracted area back onto itself. The effect of repeated bending and contracting is to produce an attracting set, that is a strange attractor as shown in Fig.1. With b = 0.3 the contraction in one iteration is mild enough that the sheaves of the strange attractor are visible. Also, Fig.1 reveals that, the Henon map does not define a single curve but a bundle of curves.

The contracting properties are determined solely by the parameter "b". Figure 2 illustrates the contraction of the strange attractor for b = 0.1. The Henon map is invertible as long as b ≠ 0, in contrast to the logistic map [2] . The non-invertibility is necessary for chaos in one-dimensional map but not for maps on higher dimensional spaces. The Henon map has two fixed points, given by [1]:

$$\mathbf{x} = [\,(\mathbf{b}-1) \pm \sqrt{(1-\mathbf{b})^2 + 4\mathbf{a}}\,]/2\mathbf{a}, \qquad \mathbf{y} = \mathbf{bx}. \tag{4}$$

The inverse of Henon map is given by:

$$\mathbf{H}_b^{-1} : \mathbf{x}_{n-1} = \mathbf{y}_n / \mathbf{b}, \qquad \mathbf{y}_{n-1} = \mathbf{x}_n + \mathbf{a}(\mathbf{y}_n / \mathbf{b})^2 - 1. \tag{5}$$

## 3. PRIVATE-KEY BLOCK CRYPTOSYSTEM

We utilize the 2-dimensional chaotic map to construct a private-key cryptosystem. In this way, the inverse map $H_b^{-1}$ is used for encryption process, and the forward map $H_b$ is used for decryption process. To construct a private-key cryptosystem, we follow the general procedures presented in [2]. These procedures are briefly mentioned below.

### 3.1 Secret Key

Both the sender and receiver use the parameter S as a secret key. The secret key is a 32-digits or ≈ 106- bits. The fixed points of $H_b$ are real for:

$$\mathbf{a} \succ \mathbf{a}_0 = -(1-\mathbf{b})^2 / 4. \tag{6}$$

When this is the case, one point is always linearly stable, while the other is unstable for:

$$\mathbf{a} \succ \mathbf{a}_1 = 3\,(1-\mathbf{b})^2 / 4. \tag{7}$$

Derrida [3] have showed that at a ≈ 0.3675 to be the beginning of period doubling and the transition to chaos at $a_\infty \approx 1.058048$. The secret key S comprises of the two parameter (a,b). The value of "a" lies within the range $a_0<a<a_2$, where, typically, $a_2 \approx$ 1.55 [1].

## 3.2 Encryption

The encryption process consists of the following steps:
(i) Use the ASCII code to convert the alphabetic plaintext M, into a binary form Z.
(ii) Divide the encoded plaintext Z into N blocks of fixed size B ≈ 64 bits.

$$\mathbf{Z} = \{\mathbf{z}_1 . \mathbf{z}_2 ,......,\mathbf{z}_N\}, \tag{8}$$

where the bits of each block are written as:

$$\mathbf{z}_i = \mathbf{m}_1, \mathbf{m}_2 ,.....,\mathbf{m}_B, \qquad \mathbf{i} = 1,2,....,\mathbf{N}. \tag{9}$$

(iii) Pad Z, if necessary, so that its length becomes a multiple of the block size B.
(iv) Use the transformation

$$\mathbf{F} : \mathbf{z}_i \rightarrow \mathbf{r}_i , \tag{10}$$

to transform the binary block $z_i$ into decimal number $r_i$, with P digits accuracy (P=20-digits), where

$$\mathbf{r}_i = \sum_{j=1}^{B} \mathbf{m}_j * 2^{-j}, \qquad \mathbf{i} = 1,2,....\mathbf{N}. \tag{11}$$

(v) Set $r_i$ as an initial condition $(x_0,y_0)$.
(vi) Calculate the ciphertext block $C_i$ by iterating $H_b^{-1}$ n-times (n = 66)

$$\mathbf{C}_i = \mathbf{H}_b^{-n} ((\mathbf{x}_0 , \mathbf{y}_0) = \mathbf{r}_i ). \tag{12}$$

As suggested in [4], the ciphertext block $C_i$ requires some more digits for correct decryption.
(vii) Convert the decimal number $C_i$ into a binary one $E_i$ and send it to the receiver.
(viii) Repeat the steps (iv-vii) for each plaintext block to get the binary ciphertext blocks.

$$\mathbf{E} = \{ \mathbf{E}_1 , \mathbf{E}_2 ,.....\mathbf{E}_N \}. \tag{13}$$

## 3.3 Decryption

The decryption process begins with receiving the binary ciphertext block $E_i$. The following steps are performed to recover the original plaintext M.
(i) Convert the ciphertext block $E_i$ into decimal number $C_i$.

(ii) Set $C_i$ as an initial condition $(x_0,y_0)$.
(iii) Calculate the recovered plaintext block $r_i$ by iterating $H_b$ n-times (n = 66)

$$\mathbf{r}_i = \mathbf{H}_b^n\ ((\ \mathbf{x}_0,\mathbf{y}_0) = \mathbf{C}_i\ ). \qquad \textbf{(14)}$$

(iv) Use the transformation **(15)**

$$\mathbf{F}^{-1} : \mathbf{r}_i \rightarrow \mathbf{z}_i,$$

to transform the decimal number $r_i$ into a binary block $z_i$.
(v) Use the ASCII code to convert the binary plaintext block $z_i$ into an alphabetic form.
(vi) Repeat the steps (i-v) for each ciphertext block to recover the original plaintext M (in alphabetic form).

## 4. RESULTS AND DISCUSSIONS

Given a set of points (x,y), representing a face in the (x,y) plane, Figs.3-4 illustrate the encryption and decryption of these points using Henon map. The number of iterations should be $P/\log_{10}2$, where P denotes, the number of plaintext's digits. The compression ratio after one iteration is "b". Since the mapping $H_b$ is a one-to-one map, there is a unique trajectory through any given point. In other word, each plaintext has a unique ciphertext. For a $<a_0$ or a> $a_2$, all initial points always escape to infinity, and there exist no attractors. Consequently, the ciphertext escape to infinity and the decryption becomes impossible.

In principle, ciphertexts generated by eq. (12) can be reconstructed in reverse order as long as the key is known) when the last ciphertext is used as the origin for the iterations of eq. (1). Since the last ciphertext generated by the inverse of two-dimensional chaotic map does not contain information dating farther back than $P/\log_{10}2$ steps, the reconstruction of the ciphertexts (and consequently the original plaintext) from the last one cannot be carried beyond that point. For correct decryption, the ciphertext size should be greater than $\xi$ [4] where,

$$\xi = \mathbf{n}\log_{10}2 + \log_{10}3 + \mathbf{P}. \qquad \textbf{(16)}$$

Therefore, for a plaintext with P=20-digits and the times of composite of inverse map n=66, the ciphertext size should be greater than 40.35. The constructed private-key block cryptosystem, using two-dimensional chaotic map, is based on simple repeated iterations. It is required n-times multiplication. Since the memory of computer has finite size, it is necessary to set a computation size. In this way, for a 20-digits plaintext, the number of iterations are set to n=66. Since the secret key consists of 106-bits, there are also $2^{106}$ possible keys.

## 5. CONCLUSION

This paper introduces the use of two-dimensional chaotic map to construct a private key block cryptosystem. It is used for compression as well as for encryption. The forward map $H_b$ was used for decryption, while the inverse map $H_b^{-1}$ was used for encryption. The ciphertext generated by the inverse of two-dimensional chaotic map, does not contain information dating farther back than $P/\log_{10}2$ steps (P is the number of accuracy digits). For a plaintext with $P = 20$-digits and the times of composite of inverse map $n = 66$, the ciphertext size should be greater than 40.3 and it is independent of the secret key. The key size is 106- bits, i.e., double the key size used in one-dimensional chaotic map (54-bits).

## REFERENCES

[1] M. Henon, "A Two-dimensional Mapping With a Strange Attractor," Comm. Math. Phys., Vol.50, pp. 69-77, 1976.

[2] Alaa Fahmy, "Private key cryptosystem using one-dimensional chaotic map, " Proceedings of the 8th ASAT conference, 4-5 May, 1999.

[3] B. Derrida, A. Gervois, and Y. Pomeau, Journal Phys. 12A, 269, 1979.

[4] Whitfield Diffie and Martin E.Hellman, "Privacy and Authentication: An Introduction to Cryptography," Proceedings of the IEEE, Vol.67, No.3, March 1979.

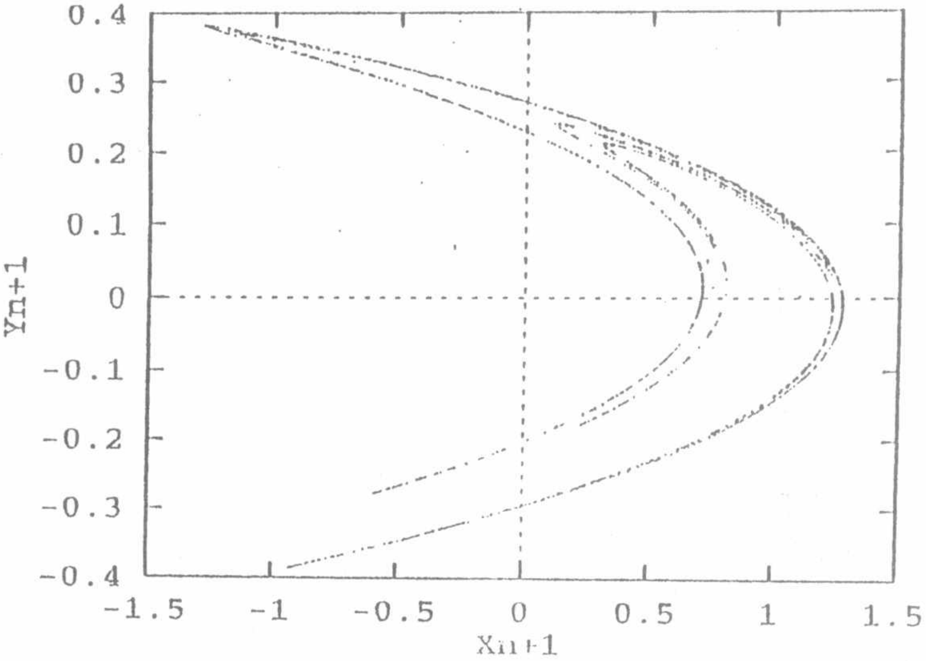

Fig.1 The Chaotic attractor of Henon map for b=0.3

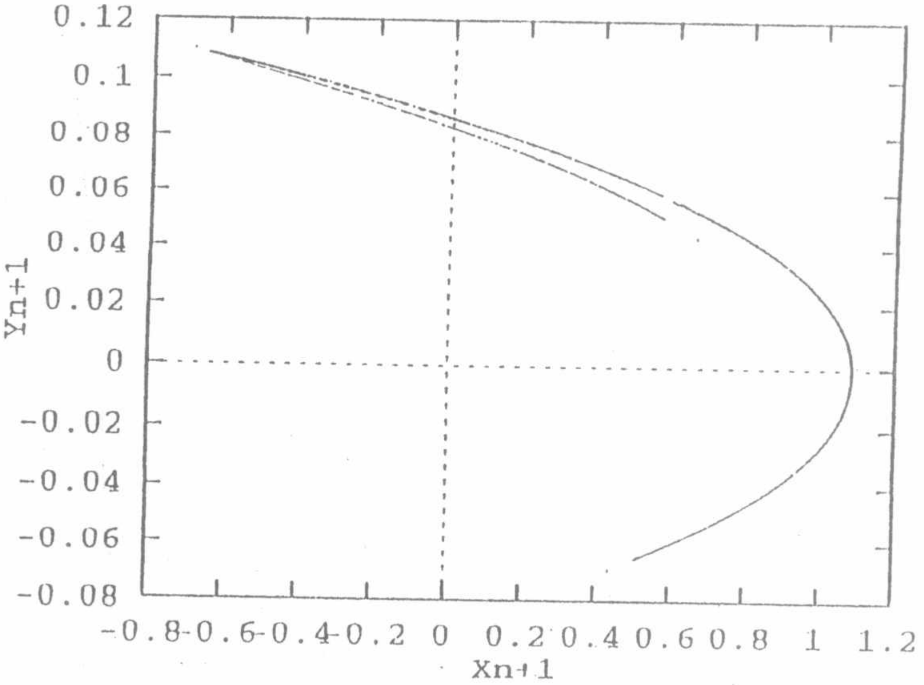

Fig.2 The chaotic attractor with compression ratio b=0.1

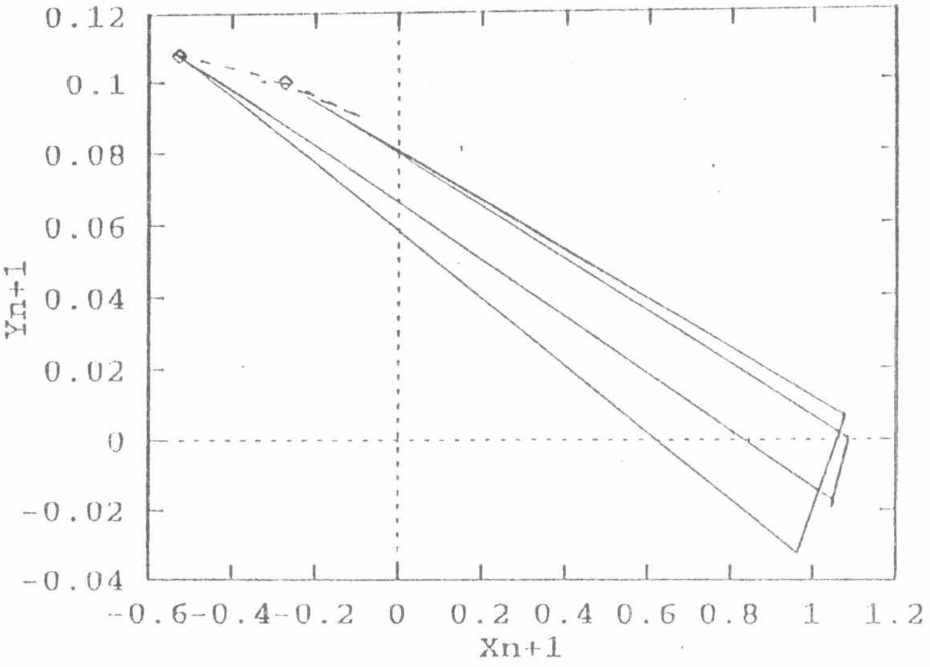

Fig.3 Encryption using Henon map

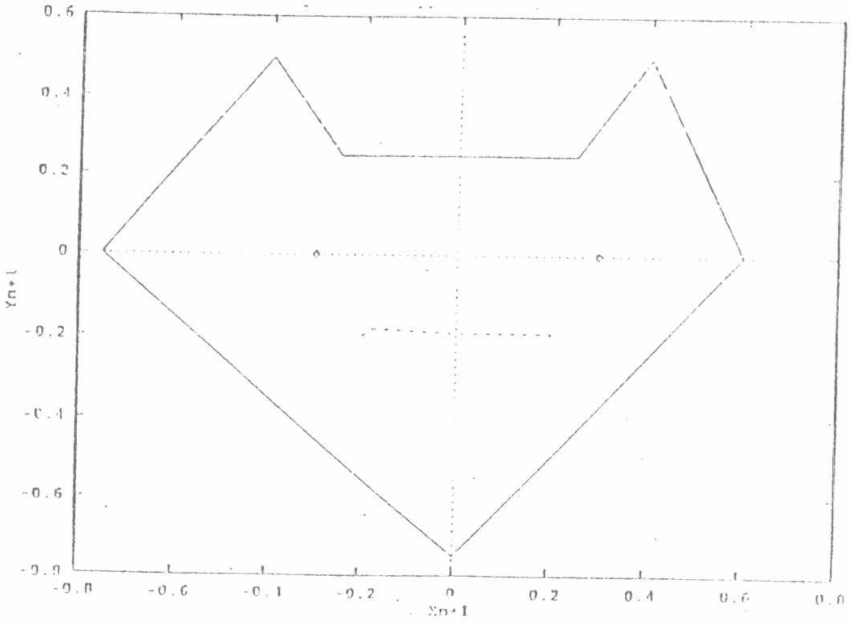

Fig. 4 Decryption using Henon map