Journal of Sound and Vibration (2002) **250**(4), 762–771
doi:10.1006/jsvi.2001.3780, available online at http://www.idealibrary.com on IDEAL®

DESIGN OF A NOVEL CRYPTOSYSTEM BASED ON CHAOTIC OSCILLATORS AND FEEDBACK INVERSION

S. M. Shahruz

Berkeley Engineering Research Institute, P.O. Box 9984, *Berkeley* 94709, *U.S.A.*
E-mail: shahruz@robotics.eecs.berkeley.edu

AND

A. K. Pradeep and R. Gurumoorthy

Board Vantage, 2030 *Addison Street*, *Suite* 640, *Berkeley* 94704, *U.S.A.*

(*Received* 20 *June* 2001)

1. INTRODUCTION

In this note, a novel symmetric (also known as private-key or secret-key) cryptosystem is designed based on chaotic oscillators such as Duffing's or a generalized Van der Pol's oscillator.

Cryptography is one of the oldest human practices for communicating secretly with intended parties; see, e.g., references [1–3] for history and non-technical description of cryptography. In recent decades, cryptography has become exceedingly prevalent in information technology since: (1) there has been an explosive increase in the transmission of information by different wired and wireless means; (2) such transmissions require security and privacy. For instance, currently, computers have become major components of information technology for communications, electronic mail, on-line banking and shopping, transmission of financial and medical reports, to name a few. Also, wireless communication systems have become another important component of information technology and provide connectivity at local and global scales.

Information technology has thus created a great demand for security and privacy of information transmission and data storage. Security and privacy are provided by cryptosystems, which for instance, keep the transmitted data secret and tamper-proof, protect information from unintended parties aiming to eavesdrop, prevent fraud, and ensure the privacy of citizens. Due to their crucial role, cryptosystems have become major elements of information technology.

Cryptosystems are mostly designed based on mathematical theories. Some cryptosystems, however, are designed based on the theory of dynamical systems. In this note, the latter approach is taken to design a novel cryptosystem based on chaotic oscillating systems and the inversion of such systems by a feedback loop. The organization of the note is as follows. In section 2, the basic structure of cryptosystems is described briefly. In section 3, a cryptosystem is proposed. In section 4, two examples are given to illustrate the superb performance of the proposed cryptosystem.

0022-460X/02/090762 + 10 $35.00/0

2. A BRIEF DESCRIPTION OF CRYPTOSYSTEMS

The basic structure of symmetric cryptosystems is shown in Figure 1. The components and operation of this system are as follows (see, e.g., references [4–8]).

The message to be transmitted is called the *plaintext message* or simply *plaintext* and is denoted by p. In order to represent a plaintext *symbols* are needed. A finite non-empty set of symbols is called an *alphabet of definition* or simply an *alphabet*. Examples of alphabet are: (1) the set $\{0, 1\}$, known as the binary alphabet; (2) the set $\{0, 1, 2, \ldots, 9\}$; (3) the set of English alphabet; (4) the set of ASCII symbols which are used for encoding (see, e.g., references [4–9]). A plaintext is a *string* (*sequence*) of symbols from an alphabet. The set of all plaintexts is called the *plaintext space* and is denoted by P (or called the *message space* and is denoted by M).

A plaintext p is encrypted to a *ciphertext* by an *encryption function* or *encryption transformation* E subject to a set of *keys* k from the *key space* K. Thus, the ciphertext, denoted by c, can formally be written as

$$c = E_k(p). \tag{1}$$

The ciphertext is a string of symbols from an alphabet possibly different from that used for the plaintext. The set of all ciphertexts is called the *ciphertext space* and is denoted by C.

The ciphertext is transmitted to the receiver, which is the intended recipient of messages. The receiver decrypts the ciphertext by using a *decryption function* or *decryption transformation* D subject to the same set of keys $k \in K$. The decryption of the plaintext p can be formally presented by

$$D_k(c) = D_k(E_k(p)) = p. \tag{2}$$

That is, $D_k = E_k^{-1}$.

In the cryptosystem just described, the same keys are used for both encryption and decryption. This type of cryptosystem is called the symmetric or private- or secret-key cryptosystem. In designing cryptosystems, in general, there are two important rules: (1) the encryption function should transform the plaintext p to a ciphertext c which would be infeasible (ideally, impossible) to decrypt without the right keys; (2) the inverse of the encryption function, namely the decryption function, should exist and recover the plaintext accurately.

Most cryptosystems are designed based on pure mathematical theories such as number theory, modular arithmetics, algebra, and elliptic curves; see, e.g., references [4–10]. In this note, a symmetric cryptosystem is designed based on chaotic oscillators, such as Duffing's or a generalized Van der Pol's oscillator. It should be remarked that cryptosystems based on chaotic systems have been designed by some researchers (see, e.g., references [11–16]). Such designs are mostly based on the synchronization of two chaotic systems. The cryptosystem presented in this note is entirely new. In particular, the decryption of the ciphertext is based on a feedback loop which inverts linear or non-linear systems. The proposed inversion is easily implementable and recovers plaintexts very fast and accurately.

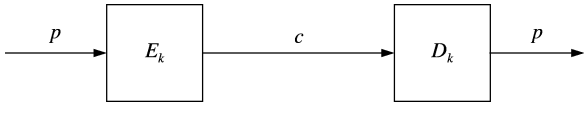

Figure 1. Basic structure of symmetric cryptosystems: p and c are, respectively, the plaintext and ciphertext; E_k and D_k are, respectively, the encryption and decryption functions subject to the set of keys k.

3. A NOVEL CRYPTOSYSTEM

The cryptosystem presented in this note is depicted in Figure 2. This system consists of the following components.

3.1. ENCRYPTION SYSTEM

A major part of the encryption system is a non-linear time-varying system $N: L_{\infty e}(\mathbb{R}_+) \to L_{\infty e}(\mathbb{R}_+)$. ($L_{\infty e}(\mathbb{R}_+)$ denotes the extended L_∞-space on $\mathbb{R}_+$; see, e.g., references [17, 18] for the definition of such spaces; hereafter, $(\mathbb{R}_+)$ is deleted in the notation of spaces). The system N can be any general non-linear system represented by non-linear differential or integral equations. Other parts of the cryptosystem are the signal generators S_1 and S_2 that generate the time functions $t \mapsto w_1(t)$ and $t \mapsto w_2(t)$, respectively. The signal generator S_1 can be, for instance, a non-linear system that generates chaotic outputs, or an oscillator that generates periodic functions. The signal generator S_2 is a non-linear system that generates chaotic outputs, or a random signal generator.

The (private) keys of the cryptosystem in Figure 2 are the system N, its parameters, and the signal generators S_1 and S_2.

The message to be transmitted is first converted to a plaintext. The plaintext is chosen to be a string (sequence) or symbols from the binary alphabet and is converted to a train of pulses of suitable width and of amplitude zero or one. This train of pulses, which is now a function of time, is denoted by $t \mapsto p(t)$. The function $p(\cdot)$ is added to $w_1(\cdot)$ to form

$$u(t) = p(t) + w_1(t), \tag{3}$$

for all $t \geqslant 0$. The function $u(\cdot)$ is then applied to the system N. The output of N is added to $w_2(\cdot)$ to form the ciphertext given by

$$c(t) = (Nu)(t) + w_2(t), \tag{4}$$

for all $t \geqslant 0$. Thus, the encryption function of the proposed cryptosystem consists of the dynamics (evolution) of N and the addition of the output of this system to the chaotic or random output of the signal generator S_2. By appropriate choice of the system N and the signal generator S_1, the output of N can be chaotic, which would be difficult to decrypt if it

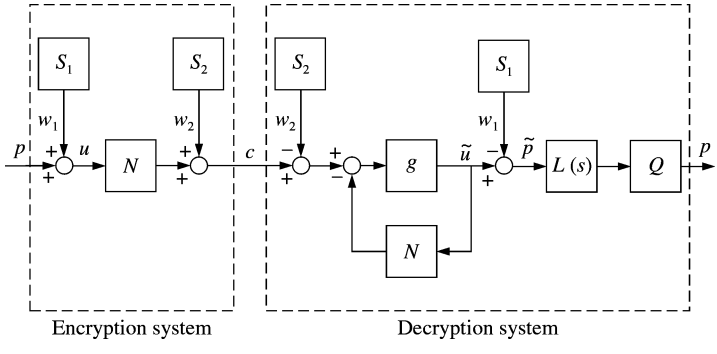

Figure 2. Details of the proposed cryptosystem: N is a non-linear time-varying system; S_1 and S_2 are signal generators; g is a (large) constant gain; $L(s)$ is a low-pass filter; Q is a quantizer.

is intercepted by an unintended party. Moreover, the addition of the chaotic or random output of the signal generator S_2 to the output of N enhances the security of the cryptosystem. The injection of the plaintext $p(\cdot)$ into the chaotic system N can be viewed as the chaotic modulation of the plaintext, whereas the addition of the output of N to that of the signal generator S_2 is the chaotic or random masking of the plaintext already encrypted by N.

The ciphertext is transmitted to the intended party to use the decryption system to recover the plaintext.

3.2. DECRYPTION SYSTEM

Although it is easy to choose an encryption system, it may be difficult to design a decryption system that would invert the encryption function. The inversion should be possible, implementable, and accurate. The crucial part of the inversion of the encryption function in this note is based on a general result from the theory of feedback systems described as follows. Consider the system in Figure 3, denoted by $S(g, N)$. In this system, g in the feedforward loop is a constant gain and N in the feedback loop is a non-linear system. The following result holds for $S(g, N)$.

Assertion 3.1. Consider the system $S(g, N)$. Let the map $g\ (I + g\,N)^{-1}\colon L_{\infty e} \to L_{\infty e}$ be bounded for all $g \in (g_1, g_2)$, where $I\colon L_{\infty e} \to L_{\infty e}$ is the identity map, $g_1 > 0$, and $g_2 \gg 1$ are constant real numbers. For sufficiently large g, the output of $S(g, N)$ is given as

$$y(t) \approx (N^{-1}\, r)(t), \tag{5}$$

for all $t \geqslant 0$. That is, $S(g, N)$ inverts the non-linear system N.

Proof. The output of the system $S(g, N)$ is given by

$$y(t) = ((g^{-1} + N)^{-1}\, r)(t), \tag{6}$$

for all $t \geqslant 0$. For large g, the output $y(\cdot)$ in equation (6) can be approximated by the function in equation (5). □

Remark. When it is possible to invert a non-linear system N by the system $S(g, N)$, the gain g should not be chosen very large. The reason is that the output of $S(g, N)$ is usually noisy and very large g will make it noisier.

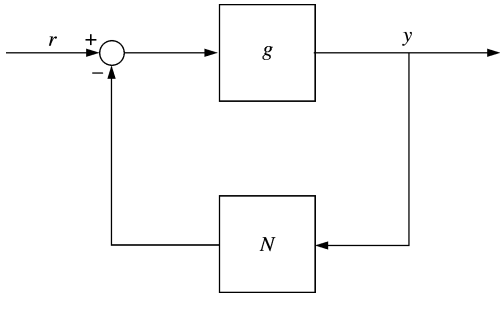

Figure 3. The feedback system $S(g, N)$. For sufficiently large gain g, the input–output map of this system is approximately equal to N^{-1}.

The result of Assertion 3.1 readily explains the decryption system in Figure 2. The decryption system consists of the signal generator S_1 and S_2 and a feedback system similar to the system $S(g, N)$, where N is the non-linear system used in the encryption system. The difference between the ciphertext $c(\cdot)$ and the output of the signal generator S_2 is the input to $S(g, N)$. The output of $S(g, N)$ is $\tilde{u}(\cdot)$, which is a good, but noisy approximation of $u(\cdot) = p(\cdot) + w_1(\cdot)$. Subtracting $w_1(\cdot)$ from $\tilde{u}(\cdot)$ yields $\tilde{p}(\cdot)$, which is a good, but noisy approximation of $p(\cdot)$. By using the low-pass filter $L(s)$ and the quantizer Q, the plaintext $p(\cdot)$ is recovered by the receiver. Note that the keys, namely, the system N and its parameters and the signal generators S_1 and S_2, are the same in both encryption and decryption systems. It is remarked that the filter $L(s)$ should be designed carefully in order to be able to recover the plaintext accurately. For instance, when the plaintext is fed to the encryption system at high rates, i.e., when the pulses in $p(\cdot)$ have small widths, the filter $L(s)$ should have fast dynamics.

Thus far, the cryptosystem proposed in this note has been described. In the next section, examples are presented to illustrate the superb performance of this cryptosystem.

4. EXAMPLES

In this section, two examples are given to illustrate the design of cryptosystem based on chaotic oscillators in detail.

4.1. EXAMPLE: DUFFING'S OSCILLATOR

Let the non-linear system N in Figure 2 be a Duffing's oscillator (see, e.g., references [19–21]) represented by

$$N\colon \ddot{x}(t) + \delta\dot{x}(t) - \alpha x(t) + \beta x^3(t) = u(t), \quad x(0) = 0, \quad \dot{x}(0) = 0, \tag{7}$$

for all $t \geqslant 0$, where $u(t) \in \mathbb{R}$ and $x(t) \in \mathbb{R}$ are, respectively, the input to and the output of the oscillator, and the parameters δ, α, and β are constant real numbers. The system N and its parameters are some of the keys of the cryptosystem. Other keys of this system are the signal generators S_1 and S_2. For this example, the signal generator S_1 generates the periodic function $w_1(t) = A\cos\omega t$ of amplitude A and frequency ω for all $t \geqslant 0$. The signal generator S_2 is turned off ($w_2 \equiv 0$).

The input to the system N is

$$u(t) = p(t) + A\cos\omega t, \tag{8}$$

for all $t \geqslant 0$, where $p(t)$ is the train of pulses of amplitude zero or one shown in Figure 4(a), which incorporates the plaintext, and $\cos\omega t$ is generated by the signal generator S_1. If the input to N were only $t \mapsto A\cos\omega t$ and the parameters δ, α, β, A, and ω were chosen appropriately, then $x(\cdot)$, the output of N, would have been chaotic. One such set of parameters is (see, e.g., references [19–21])

$$\alpha = 10, \qquad \beta = 100, \quad \delta = 1, \quad A = 1{\cdot}5, \quad \omega = 3{\cdot}76. \tag{9}$$

Using the parameter values in equation (9) and the input in equation (8), the ciphertext $c(t) = x(t)$ for all $t \geqslant 0$ is obtained. The ciphertext is chaotic as shown in Figure 4(b). This

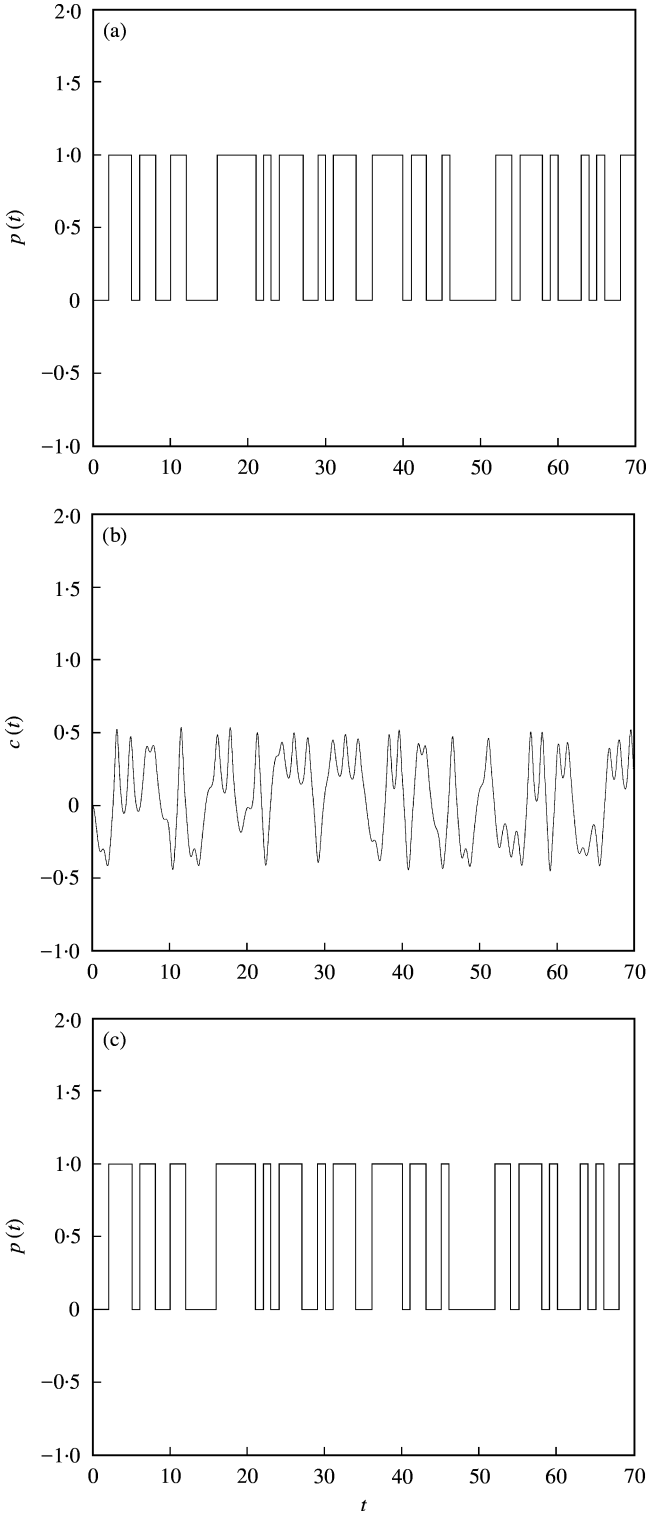

Figure 4. Time histories of: (a) plaintext $t \mapsto p\,(t)$; (b) ciphertext $t \mapsto c(t)$; (c) plaintext $t \mapsto p(t)$ recovered by the decryption system. Note the chaotic behaviour of the ciphertext.

ciphertext is transmitted to the receiver to use the decryption system to recover the plaintext. The decryption system has the same keys as those of the encryption system. Additional components of the decryption system are

$$g = 10\,000, \qquad L(s) = \frac{20}{s + 20}, \tag{10}$$

and the quantizer Q. The decryption system operates upon the ciphertext and recovers the plaintext shown in Figure 4(c). It is evident that the plaintext is fully and accurately recovered.

4.2. EXAMPLE: A GENERALIZED VAN DER POL'S OSCILLATOR

Let the non-linear system N in Figure 2 be a generalized Van der Pol's oscillator (see, e.g., references [22, 23]) represented by

$$N\colon \ddot{x}(t) + \delta\,(x^2(t) - 1)\,\dot{x}(t) + \beta x^3(t) = u(t), \quad x(0) = 0, \quad \dot{x}(0) = 0, \tag{11}$$

for all $t \geqslant 0$, where $u(t) \in \mathbb{R}$ and $x(t) \in \mathbb{R}$ are, respectively, the input to and the output of the oscillator, and the system parameters are

$$\delta = 0{\cdot}2, \quad \beta = 1. \tag{12}$$

The input to the system N is the same as that in equation (8), where the time function $t \mapsto p(t)$ is the train of pulses shown in Figure 5(a), and $t \mapsto A\cos\omega t$ is generated by the signal generator S_1, with

$$A = 17, \quad \omega = 4. \tag{13}$$

For parameter values in equations (12) and (13), the output of the system N is chaotic in the absence of the plaintext $t \mapsto p(t)$ in equation (8); see, e.g., references [22, 23]. For this example, the signal generator S_2 generates a random output to be added to that of the system N to form the ciphertext $t \mapsto c(t)$ shown in Figure 5(b). The ciphertext is transmitted to the receiver to use the decryption system to recover the plaintext. The decryption system has the same keys as those of the encryption system. Additional components of the decryption system are

$$g = 30\,000, \qquad L(s) = \frac{150}{s^2 + 10\,s + 150}, \tag{14}$$

and the quantizer Q. The decryption system recovers the plaintext fully and accurately as it is shown in Figure 5(c).

Remark. As shown in sections 4.1 and 4.2, by appropriate choice of the non-linear system N and the signal generators S_1 and S_2, the encryption system can generate chaotic or random ciphertexts. There is a variety of non-linear and random systems and signal generators that can be chosen for N, S_1, and S_2 to generate chaotic ciphertexts; see, e.g.,

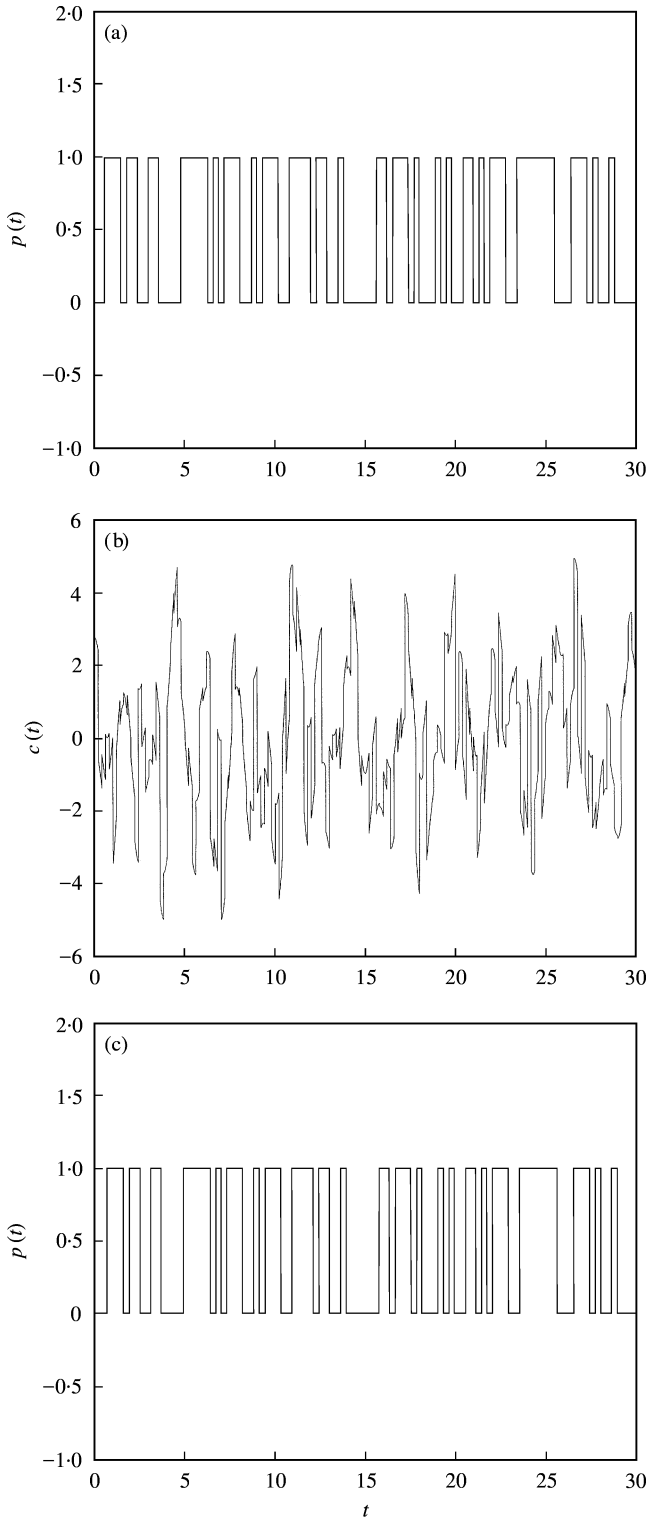

Figure 5. Time histories of: (a) plaintext $t \mapsto p\,(t)$; (b) ciphertext $t \mapsto c(t)$; (c) plaintext $t \mapsto p(t)$ recovered by the decryption system. Note the chaotic and random behaviour of the ciphertext.

references [23–29]. In choosing N care should be taken since the success of a designed cryptosystem relies on the invertibility of N by the feedback system $S(g, N)$.

5. CONCLUSIONS

In this note, a novel symmetric cryptosystem is proposed. The encryption system of the proposed system consists of a non-linear chaotic oscillator and two signal generators. The non-linear oscillator, its parameters, and the signal generators are the private keys of the cryptosystem. The plaintext is a train of pulses of suitable width and of amplitude zero or one which is operated upon by the encryption system. The encryption function consists of the dynamics (evolution) of the non-linear oscillator and the addition of a chaotic or a random signal to the output of the oscillator. The decryption system uses the same keys as those of the encryption system. A feedback loop is used in the decryption system to invert the non-linear dynamics of the chaotic oscillator. Moreover, the decryption system has a low-pass filter and a quantizer to recover the plaintext fully and accurately. By appropriate choice of the non-linear oscillator, the signal generators, and the low-pass filter, it is possible to have a cryptosystem capable of transmitting information securely and recovering it accurately. Two examples, which use Duffing's and a generalized Van der Pol's oscillators, are given to illustrate the superb performance of the proposed cryptosystem.

REFERENCES

1. D. KAHN 1967 *The Codebreakers*: *The Story of Secret Writing*. New York, NY: Macmillan.
2. D. E. NEWTON 1997 *Encyclopedia of Cryptology*. Santa Barbara, CA: ABC-CLIO.
3. S. SINGH 2000 *The Code Book*: *The Evolution of Secrecy from Ancient Egypt to Quantum Cryptography*. New York, NY: Anchor Books.
4. B. SCHNEIER 1996 *Applied Cryptography*: *Protocols*, *Algorithms*, *and Source Code in C*. New York, NY: John Wiley; second edition.
5. A. J. MENEZES, P. C. VAN OORSCHOT and S. A. VANSTONE 1997 *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press.
6. J. C. A. VAN DER LUBBE 1998 *Basic Methods of Cryptography*. Cambridge, UK: Cambridge University Press.
7. J. A. BUCHMANN 2001 *Introduction of Cryptography*. New York, NY: Springer-Verlag.
8. R. A. MOLLIN 2001 *An Introduction to Cryptography*. Boca Raton, FL: Chapman & Hall/CRC.
9. S. C. COUTINHO 1999 *The Mathematics of Ciphers*: *Number Theory and RSA Cryptography*. Natick, MA: A. K. Peters, Ltd.
10. I. F. BLAKE, G. SEROUSSI and N. P. SMART 1999 *Elliptic Curves in Cryptography*. Cambridge, UK: Cambridge University Press.
11. K. M. CUOMO and A.V. OPPENHEIM 1993 *Physical Review Letters* **71**, 65–68. Circuit implementation of synchronized chaos with applications to communications.
12. K. M. CUOMO, A. V. OPPENHEIM and S. H. STROGATZ 1993 *IEEE Transactions on Circuits and Systems—II*: *Analog and Digital Signal Processing* **40**, 626–633. Synchronization of Lorenz-based chaotic circuits with applications to communications.
13. C. W. WU 1995 *Ph.D. Dissertation*, *Department of Electrical Engineering and Computer Sciences*, *University of California*, *Berkeley*, *California*. Some aspects of order in circuits and systems.
14. T.-L. LIAO and N.-S. HUANG 1999 *IEEE Transactions on Circuits and Systems—I*: *Fundamental Theory and Applications* **46**, 1144–1150. An observer-based approach for chaotic synchronization with applications to secure communications.
15. M. P. KENNEDY, R. ROVATTI and G. SETTI (editors) 2000 *Chaotic Electronics in Telecommunications*. Boca Raton, FL: CRC Press.
16. K.-Y. LIAN, T.-S. CHIANG, C.-S. CHIU and P. LIU 2001 *IEEE Transactions on Systems*, *Man*, *and Cybernetics—Part B*: *Cybernetics* **31**, 66–82. Synthesis of fuzzy model-based designs to synchronization and secure communications for chaotic systems.

17. C. A. DESOER and M. VIDYASAGAR 1975 *Feedback Systems*: *Input–Output Properties*. New York, NY: Academic Press.
18. M. VIDYASAGAR 1993 *Nonlinear Systems Analysis*. Englewood Cliffs, NJ: Prentice-Hall; second edition.
19. F. C. MOON 1987 *Chaotic Vibrations*: *An Introduction for Applied Scientists and Engineers*. New York, NY: John Wiley.
20. J. GUCKENHEIMER and P. HOLMES 1983 *Nonlinear Oscillations*, *Dynamical Systems*, *and Bifurcations of Vector Fields*. New York, NY: Springer-Verlag; fourth printing, 1993.
21. S. H. STROGATZ 1994 *Nonlinear Dynamics and Chaos*: *With Applications to Physics*, *Biology*, *Chemistry*, *and Engineering*. Reading, MA: Addison-Wesley.
22. W.-H. STEEB and A. KUNICK 1987 *International Journal of Non-Linear Mechanics* **22**, 349–361. Chaos in limit cycle systems with external periodic excitations.
23. T. KAPITANIAK 2000 *Chaos for Engineers*: *Theory*, *Applications*, *and Control*. New York, NY: Springer-Verlag; second edition.
24. M. A. VAN WYK and W.-H. STEEB 1997 *Chaos in Electronics*. Dordrecht, The Netherlands: Kluwer Academic Publishers.
25. G. CHEN and X. DONG 1998 *From Chaos to Order*: *Methodologies*, *Perspectives and Applications*. Singapore: World Scientific.
26. T. KAPITANIAK and S. R. BISHOP 1999 *The Illustrated Dictionary of Nonlinear Dynamics and Chaos*. New York, NY: John Wiley.
27. G. CHEN (editor) 2000 *Controlling Chaos and Bifurcations in Engineering Systems*. Boca Raton, FL: CRC Press.
28. A. S. ELWAKIL and M. P. KENNEDY 2001 *IEEE Transactions on Circuits and Systems—I*: *Fundamental Theory and Applications* **48**, 289–307. Construction of classes of circuit-independent chaotic oscillators using passive-only nonlinear devices.
29. R. BERNARDINI and G. CORTELAZZO 2001 *IEEE Transactions on Circuits and Systems—I*: *Fundamental Theory and Applications* **48**, 552–564. Tools for designing chaotic systems for secure random number generation.