Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Sound and Vibration 275 (2004) 431–433
JOURNAL OF SOUND AND VIBRATION
www.elsevier.com/locate/jsvi

Letter to the Editor

Comments on "Cryptanalysis of a novel cryptosystem based on chaotic oscillators and feedback inversion"

S.M. Shahruz*

Berkeley Engineering Research Institute, P.O. Box 9984, Berkeley, CA 94709, USA

Received 8 October 2003

1. Introduction

When Ref. [1] was submitted for publication, due to the proprietary nature of the work, only a brief description of the proposed cryptosystem was given. The description in Ref. [1] provides only a glimpse of the actual cryptosystem designed and implemented. Many recipes that make the proposed cryptosystem secure and implementable were not given in this reference. Since the proposed cryptosystem is no longer in use, details of its design and implementation are disclosed here. What is disclosed will answer some of the points raised in Ref. [2].

2. Resisting attacks

The example in Ref. [1], which uses a chaotic Duffing's oscillator, is an illustrative example to show how to build a cryptosystem based on dynamical systems and feedback inversion. In general, there is no need to use a chaotic system; any single-input single-output (SISO) non-linear (even linear) system can be used. For robust implementation, discrete time (sampled data) systems should be used. A typical system is

$$N: \begin{cases} x(k+1) = f(x(k), u(k); P), & x(0) =: x_0, \\ y(k) = h(x(k); Q), \end{cases} \tag{1}$$

where the state vector $x(k) \in \mathbb{R}^n$, the input $u(k) \in \mathbb{R}$, and the output $y(k) \in \mathbb{R}$ for all $k \in \{0, 1, 2, \ldots, K\}$; the initial state vector $x_0 \in \mathbb{R}^n$, the vectors of system parameters $P \in \mathbb{R}^p$ and $Q \in \mathbb{R}^q$; the function $f: \mathbb{R}^n \times \mathbb{R} \times \mathbb{R}^p \to \mathbb{R}^n$ and the output map $h: \mathbb{R}^n \times \mathbb{R}^q \to \mathbb{R}$. System N is time-invariant; however, it can be chosen a time-varying system.

System N is a part of the encryption system, where the *non-zero* initial state vector and the parameters in P and Q are some of the keys of the cryptosystem. The other parts of the encryption

*Tel.: +1-510-642-3248.
E-mail address: shahruz@eecs.berkeley.edu (S.M. Shahruz).

doi:10.1016/j.jsv.2003.11.008

system are two signal generators S_1 and S_2 that generate sequences of random real numbers $k \mapsto w_1(k)$ and $k \mapsto w_2(k)$, respectively. The random sequences $w_1(\cdot)$ and $w_2(\cdot)$ are also the system keys and are never chosen periodic sequences.

The input to the system is

$$u(k) = p(k) + w_1(k), \tag{2}$$

for all $k \in \{0, 1, 2, \ldots, K\}$, where $p(\cdot)$ is the plaintext and $w_1(\cdot)$ is the random sequence generated by the signal generator S_1. The plaintext is chosen to be a string (sequence) of symbols from the binary alphabet and is converted to a train of pulses of amplitude zero or one. The input $u(\cdot)$ is thus a sequence of random real numbers that is applied to system N. The output of N is thus a sequence of random real numbers as well. The output of the system is added to the random sequence $w_2(\cdot)$ to form the ciphertext given by

$$c(k) = y(k) + w_2(k), \tag{3}$$

for all $k \in \{0, 1, 2, \ldots, K\}$. It is emphasized that for tighter security the sequence $w_2(\cdot)$ is never set identically equal to zero.

With this setup, it becomes clear that it is not necessary to use a chaotic system as a means of tightening the security of the cryptosystem. The security of the system relies on the system keys: parameters $P \in \mathbb{R}^p$ and $Q \in \mathbb{R}^q$, the initial state vector $x_0 \in \mathbb{R}^n$, and the random sequences $w_1(\cdot)$ and $w_2(\cdot)$. By choosing an adequately large number of keys, the cryptosystem will be secure (see, e.g., Ref. [3]).

3. Implementation issues

In Ref. [2], it is argued that the cryptosystem in Ref. [1] is difficult to implement. In the following, it is briefly explained that there are no difficulties in implementing the proposed cryptosystem by answering some of the points raised in Ref. [2].

(1) By choosing a discrete time system, the system output and the ciphertext are sequences of (random) real numbers and hence the transmission is not analog.

(2) When each packet of the ciphertext ($c(k)$, where $k \in 0, 1, 2, \ldots, K$) is received by the decryption system, it is buffered. Then, the decryption system operates on the ciphertext by synchronously running the feedback system and the signal generators in it.

(3) Signal attenuation and corruption of ciphertext by noise are problems of all cryptosystems; they are not exclusive to the cryptosystem in Ref. [1].

(4) The issues of digital transmission and discretization of the ciphertext are irrelevant when a discrete time system is used.

4. Conclusions

The cryptosystem proposed in Ref. [1] is a new system designed based on dynamical systems. The proposed cryptosystem does not necessarily use chaotic dynamical systems. In particular, its security does not rely on the chaotic behavior of the dynamical system used in its encryption system. The security of the proposed cryptosystem relies on the system keys, including: system

parameters, system initial state vector, two sequences of random real numbers generated by the signal generators. There is no major problem in implementation of the proposed cryptosystem when discrete time systems are used.

References

[1] S.M. Shahruz, A.K. Pradeep, R. Gurumoorthy, Design of a novel cryptosystem based on chaotic oscillators and feedback inversion, *Journal of Sound and Vibration* 250 (2003) 762–771.

[2] G. Álvarez Marañón, L. Hernández Encinas, F. Montoya Vitini, J. Muñoz Masqué, Cryptanalysis of a novel cryptosystem based on chaotic oscillators and feedback inversion, *Journal of Sound and Vibration* 275 (2004) 423–430.

[3] A.K. Lenstra, E.R. Verhuel, Selecting cryptographic key sizes, *Journal of Cryptology* 14 (2001) 255–293.