Chaos, Solitons and Fractals 104 (2017) 655–667

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

Nonlinear Science, and Nonequilibrium and Complex Phenomena

journal homepage: www.elsevier.com/locate/chaos

The design and implementation of hybrid RSA algorithm using a novel chaos based RNG

Ünal Çavuşoğlu[a,*], Akif Akgül[b], Ahmet Zengin[a], Ihsan Pehlivan[b]

[a] *Department of Computer Eng., Faculty Of Computer and Information Sciences, Sakarya University, Serdivan, Sakarya 54187, Turkey*
[b] *Department of Electrical and Electronics Eng., Faculty Of Technology, Sakarya University, Serdivan, Sakarya 54187, Turkey*

ARTICLE INFO

Article history:
Received 21 March 2017
Revised 23 August 2017
Accepted 11 September 2017

Keywords:
Information security
Encryption algorithm
Chaos
RSA
RNG

ABSTRACT

The number of attempts to break modern encryption methods increases day by day and therefore the need for the design of systems to ensure higher security has occurred. This study aims, an encryption algorithm that combines the strong of asymmetric encryption algorithm and the rich dynamic behaviors of chaotic systems is developed. In this study, firstly a new chaotic system design with high dynamic features is performed and then circuit realization and analyses are made. A chaos based RNG (random number generator) is designed with the help of the new developed chaotic system, NIST and FIPS tests are run. Chaos based hybrid RSA (CRSA) encryption algorithm design in which RNG and RSA algorithms are used together is performed. Text and image encryption is carried out with the algorithm and security analyses of these applications are made. Security analyses results are compared with classical RSA algorithm. It is observed that the developed CRSA algorithm provided better results than RSA algorithm in security tests.

1. Introduction

Due to the developing technology and wider use of computers in today's world, there has been a dramatic increase in the amount of data shared via internet. Maintenance of the security of such data has, without any doubt, become a top issue recently. Everyday there are more and more attacks to capture important data on the internet and thus there are more efforts for the security of such data. These efforts mostly include the design of new encryption algorithms and security systems. Encryption algorithms are usually divided into two categories as symmetric and asymmetric. Symmetric encryption algorithms are AES [1], DES [2], RC5 [3], RC6 [4], Blowfish [5]. Asymmetric encryption algorithms are RSA [6], ECC [7], Diffie Helman [8]. RSA is an asymmetric based and open key encryption algorithm [6,9]. RSA algorithm is very commonly used in data encryption and digital signature applications. One of the most significant methods used in studies for the maintenance of data security is the use of chaotic systems in encryption [10–12]. Because of the sensitive dependence on initial conditions and control parameters of the chaotic systems, it has been argued that the science of chaos and cryptology are closely coupled [13]. Thanks to such features, chaotic systems contain two most important components of the encryption; confusion and diffusion [14].

The literature of the field contains numerous studies with chaos based encryption and RNG. Bassem et al. [15], Wang et al. [16], Liu et al. [17], Fouda et al. [18], Brindha and Gounden [19] proposed a new chaotic encryption algorithm in their studies. Shuai et al. [20] proposed a new chaos based block encryption algorithm to provide security communication on wireless sensor networks. Mohammed et al. [21] designed an algorithm that increases security and QOS on SRTP (secure real time protocol) protocol by using chaotic systems. Kocarev and Goce [22] proposed a chaos based algorithm design while Tong et al. [23] proposed a new chaos based encryption algorithm for wireless sensor networks. Zhao and Sun [24] performed a chaos based image encryption using the logistic chaotic map. Silva et al. [25] created a developed data flow encryption algorithm, they called eLoBa (enhanced Lorenz based), that uses Lorenz chaotic map. In their common article, Ginting and Rocky [26] designed a mixed encryption algorithm in which RC4 encryption algorithm and logistic chaotic map are used for the encryption of digital images. In their study, Hraoui et al. [27] designed a chaos based encryption algorithm that makes use of the logistic chaotic map to be used in image encryption. Jolfaei and Abdolrasoul [28] designed an image encryption algorithm that includes baker's chaotic map and S-AES block encryption algorithm. Over the last few years, many studies on RNGs have been conducted [29–36].

[*] Corresponding author.
E-mail address: unalc@sakarya.edu.tr (Ü. Çavuşoğlu).

https://doi.org/10.1016/j.chaos.2017.09.025
0960-0779/© 2017 Published by Elsevier Ltd.

Literature of the field concerning encryption algorithms and RNG designs usually includes only studies including modern encryption methods or chaotic systems. Encryption algorithms performed with only chaotic systems may be broken and thus security deficiencies are possible [37,38]. That is why system design that includes both modern encryption methods and chaotic systems is an alternative solution for high security encryption. Making use of chaotic systems, whose dynamic structure is well-known by everybody, in encryption studies creates a certain disadvantage [39,40]. A unique RNG design based on a new chaotic system with a complicated dynamic structure will avoid such a disadvantage and the new RNG designed will be appropriate for high security encryption. The objective here is to create a new chaotic system, a new random number generator design and a new hybrid encryption algorithm and thus to design a unique and strong encryption system to fill the gaps in the security literature.

The design of a structure to enable a stronger encryption with the help of the CRSA algorithm is intended in this study. For the first step of the study, the design of the new chaotic system to be employed in chaos based RNG design is realized and analyses of the chaotic system and circuit realization of the new chaotic system are performed. As the next step, chaos based RNG is designed by means of the new chaotic system and NIST and FIPS randomness tests [41], which are of the highest standards, FIPS Tests are run on bit series produced by RNG to be utilized in encryption. CRSA algorithm that included the usage of both chaos based RNG and RSA algorithms is designed and its design is explained in detail. Text and image encryption applications are realized with the CRSA algorithm developed and the security analyses of this encryption application are made. Results of the applications are compared with the results of the RSA algorithm.

The second section of the article covers the new chaotic system design and chaotic system analyses; the third section covers chaos based RNG design and NIST and FIPS tests; the fourth section covers the circuit realization of the new chaotic system, its simulation and CRSA algorithm design and application; the fifth section covers security analyses and the last section covers the results.

2. New chaotic system and analysis

As chaotic systems are sensitive dependent on initial conditions and control parameters [42–44], they are utilized in designing random number generators in encryption. There are many new chaotic systems in the literature. Especially new chaotic systems with hidden equilibrium points and no equilibrium points are presented [45–51]. Chaos based cryptology is based on the complex dynamics of nonlinear systems. In this part, the design of the chaotic system to be used in RNG design is completed and analyses of this system are made.

2.1. The design of new chaotic system

The design of the chaotic system to be used in RNG design is completed. The fact that the chaotic system has high dynamic features is significant in terms of the randomness of the numbers to be generated. For the design of the new chaotic system, terms are added on equation sets compiled and some changes are added on parameters. Eq. (1) shows the equation that belongs to the new chaotic system (NCS) developed. Initial conditions of the system are $x(0) = 1, y(0) = -1, z(0) = 0.01$.

$$\begin{aligned} \dot{x} &= cy - x - bz \\ \dot{y} &= axz - xy - bx \\ \dot{z} &= dxy + b \end{aligned} \tag{1}$$

When system parameters are $a = 1$, $b = 1$, $c = 2$ and $d = -3$, they present chaotic features. Different chaotic systems can be achieved in different system parameters. Eq. (2) exhibits the chaotic system with parameters.

$$\begin{aligned} \dot{x} &= 2y - x - z \\ \dot{y} &= xz - xy - x \\ \dot{z} &= -3xy + 1 \end{aligned} \tag{2}$$

2.1.1. The phase portraits of new chaotic system

For a three dimensional system, chaotic attractors of the system, in other words the phase portraits, can be examined in four different ways like x-y, x-z, y-z and x-y-z. These processes can be easily carried out by computers thanks to developing technology. Chaotic system data is entered with Matlab [52] odesolve.m program and phase portraits expected in the program output can easily be obtained. Same processes can be gathered as Matlab Simulink, electronic circuit realization simulation program or oscilloscope outputs from electronic circuits. Phase portraits of new chaotic system are first examined with Matlab odesolve.m program. Figure x shows the x-y, y-z, x-z and x-y-z phase portrait outputs of the chaotic system with initial values as x = 0, y = 0 and z = 0. Matlab outputs of phase portraits are given in a comparative way with outputs obtained from ORCAD [53] program and real environment circuit application in Part 4.1. As Fig. 8 exhibits, the new chaotic system has rich dynamic behaviors.

2.1.2. Equilibrium points analysis

As a result of the chaotic systems equilibrium points analysis; E1, E2 equilibrium points are derived as complex numbers given below [54]. When system parameters are a = 1, b = 1, c = 2, d = −3 :

$$\begin{aligned} E_1 &= (0.263763, 1.263763, 2.263763) \\ E_2 &= (-1.263763, -0.263763, 0.736238) \end{aligned} \tag{3}$$

The local behaviour of the system around these real number equilibrium points can be investigated by using the following Jacobian matrix:

$$J = \begin{bmatrix} -1 & 2 & -1 \\ z-y-1 & -x & x \\ -3y & -3x & 0 \end{bmatrix} \tag{4}$$

$$J(E_1) = \begin{bmatrix} -1 & 2 & -1 \\ 0 & -0.2637 & 0.2637 \\ -3.789 & -0.7911 & 0 \end{bmatrix} \tag{5}$$

To obtain its eigenvalues, let $\det(\lambda I - J(E_2)) = 0$. Then, the characteristic equation has the following form:

$\lambda_1 = 2.6739 \quad \lambda_2 = 0.9178 \quad \lambda_3 = 0.4924$ for E_2:

$$J(E_2) = \begin{bmatrix} -1 & 2 & -1 \\ -0.0001 & -1.2637 & 1.2637 \\ 0.7911 & 3.7911 & 0 \end{bmatrix} \tag{6}$$

To obtain its eigenvalues, let $\det(\lambda I - J(E_1)) = 0$. Then, the characteristic equation has the following form:

$\lambda_1 = 1.6224 \quad \lambda_2 = 1.4889 \quad \lambda_3 = 2.3973$

Since the linearization matrices J(E1), J(E2) have eigenvalues with positive real parts, it follows from Lyapunov stability theory that the equilibrium points E1, E2 unstable, and this implies chaos in the dissipative system. So, the trajectories of new system (Eq. (1)) diverge from the two equilibrium points and orbit onto the strange attractor of the system (Eq. (1)).

2.1.3. Time series analysis / sensitivity to initial conditions

That even a tiny change in the initial condition values of the system creates different outputs provides important clues regarding chaotic behaviour feature. Fig. 1 shows 'x' initial