Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC-PapersOnLine 48-18 (2015) 257–261

Pseudo random number generator based on the generalized Lorenz chaotic system

Volodymyr Lynnyk * **Noboru Sakamoto** **
Sergej Čelikovský ***

* *Institute of Information Theory and Automation, The Czech Academy of Sciences, Prague, Czech Republic, (e-mail: voldemar@utia.cas.cz).*
** *Department of Aerospace Engineering, Graduate School of Engineering, Nagoya University, Furo-cho, Chikusa-ku, Nagoya, Japan, (e-mail: sakamoto@nuae.nagoya-u.ac.jp)*
*** *Institute of Information Theory and Automation, The Czech Academy of Sciences, Prague, Czech Republic, (e-mail: celikovs@utia.cas.cz)*

Abstract: An approach to generate the pseudo random number sequences from a single generalized Lorenz system (GLS) is proposed in this paper. New algorithms are introduced for the binary sequence generation based on the GLS. Basic statistical tests and security analysis of the pseudo random number generators (PRNG) based on the GLS are also provided. The results show that PRNG based on GLS can be good candidates for using in applications in secure communication.

Keywords: Chaos, chaotic behaviour, random number generators, pseudo random sequences, generalized Lorenz system.

1. INTRODUCTION

In recent years, chaos has been attracting interests of many researchers in the fields of physics, mathematics, computer engineering. Furthermore, chaos has been attracting the attention of the grass roots and collocation of "point of bifurcation" became widespread in the article of newspapers more often than before. Chaos theory is used by scientists for explaining and prediction of the behaviour of the systems in the real word. As a matter of fact, the well-known features of the chaotic systems like strong dependence on the initial conditions, topological transitivity, wide spread spectrum of its signal, etc., directly suggest the idea to use suitable chaos generators to build a new generation of secure encryption methods Kocarev et al. (1992); Cuomo et al. (1993); Yang et al. (1997); Čelikovský et al. (2006); Lynnyk and Čelikovský (2010); Baptista (1998). In modern life, many people use credit cards for shopping, social networks for communications, internet banking for paying the bills, internet phone and of Short Message Service (SMS) communication etc. Generally, all this activity are protected by the secure encryption methods.

In the classical cryptography there are two kinds of the encryption schemes based on the different key distribution techniques. One of them is the symmetric cryptosystem (secret-key cryptosystem) that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. Symmetric cryptosystems can use either stream ciphers or block ciphers Mao (2004). For the distribution of the secure keys in symmetric cryptosystems the face-to-face meeting, trusted courier, or existing secure encryption channel are used. The first two enumerated methods are not very realistic ones and are often impractical, while the third method depends on the security of the previous key exchange. For the key exchange Diffie Hellman method can be used as well, Diffie and Hellman (1976). Diffie Hellman key exchange is a specific method of securely exchanging cryptographic keys over a public channel and it is the first specific example of asymmetric (public-key) cryptosystem. This is the second kind of cryptosystems, which uses two separate keys, one of which is secret and one of which is public, Diffie and Hellman (1976). For the generation of the key sequence in the symmetric and asymmetric cryptosystems a random number generator (RNG) or pseudo random number generator (PRNG) are used. In computing, a RNG is called the hardware true random number generator (TRNG). TRNG is an apparatus that generates random numbers from a physical process, rather than a computer program. Such devices are often based on microscopic phenomena that generate low-level, statistically random "noise" signals, such as thermal noise, the photoelectric effect, and other quantum phenomena LLC (2010). Moreover, the quality of the cameras integrated in mobile telephones has improved significantly so that now they are sensitive to light at the few-photon level. Sanguinetti et al. (2014) demonstrate how these properties can be used to generate the random numbers of a quantum origin. RNG can be used for the generation of the true random numbers (seed), which is used in the PRNG for the generation of the pseudo random numbers. Any cryptosystem with super strong encryption algorithm can be broken, if it uses a poor key-selection algorithm. Therefore, Intel corporation integrated a TRNG which primarily samples thermal noise by amplifying the voltage measured across undriven resistors in Intel 82802 Firmware Hub in 1999

10.1016/j.ifacol.2015.11.046

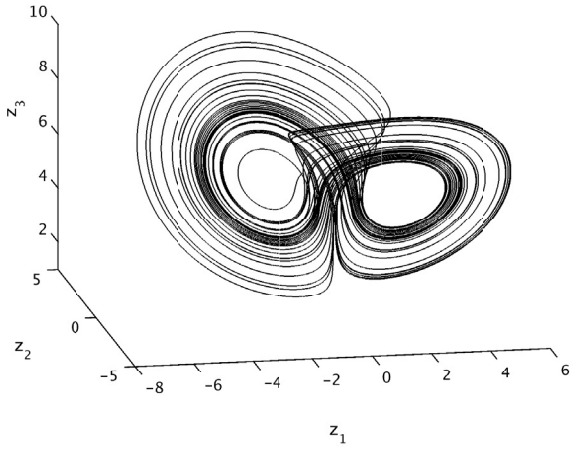

Fig. 1. The attractor of the generalized Lorenz system with parameters $\lambda_1 = 8$, $\lambda_2 = -16$, $\lambda_3 = -1$, $\tau = 0.1$.

Jun and Kocher (1999). Afterwards, this TRNG has a problem with increased power consumption, speed of the generation of the random numbers and compatibility with manufacturing process (connected with the reducing of the size of the transistors in processors). Later on, a Digital Random Number Generator (DRNG), described in Srinivasan et al. (2009, 2010) and integrated in Ivo Bridge processors family was constructed for Intel corporation. Also, TRNG is inrtegrated in the processors VIA C3, which is put forward by the VIA company Cryptography Research (2003).

In Oishi and Inoue (1982) researchers designed a first PRNG based on the chaotic system. Last two decades, PRNG based on the chaotic systems has been the focus of research for many investigators Fridrich (1998); Kwok and Tang (2007); Lei et al. (2006); Li et al. (2005); Stojanovski and Kocarev (2001); Yalcin et al. (2004); Nian-Sheng (2011). In Chen et al. (2001) a RNG based on the Chua circuit is hardware realized. Hu et al. (2013) have proposed a PRNG based on the Chen chaotic system. Later on, Özkaynak and Yavuz (2013) showed that generated pseudo random number sequences have been obtained by using the brute force attack on a reduced key space.

In this paper, two pseudo-random number generators are proposed by using the generalized Lorenz system (GLS). One of the PRNG is based on the sum of three coordinates of the chaotic orbits of GLS. The another one is based on the combination of three coordinates of the chaotic orbits of GLS. Statistical tests and security analysis show that proposed algorithm has a good pseudo random characteristics, highly sensitivity to change of the key and strength against brute force attack.

The rest of the paper is organized as follows. In Section 2, we briefly repeat some known facts about the generalized Lorenz system. Section 3 introduced the PRNG algorithms for the generalized Lorenz system which are analysed in Section 4. Final section gives some conclusion and outlooks for future research.

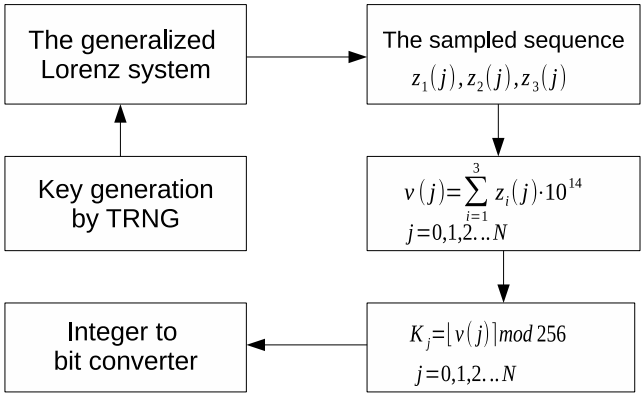

Fig. 2. Scheme of the PRNG based on the generalized Lorenz chaotic system.

2. THE GENERALIZED LORENZ SYSTEM

First, let us recall some previously published results on the generalized Lorenz system classification. Further details may be found in Čelikovský and Chen (2002, 2005). The following general nonlinear system of ordinary differential equations in R^3 is called a *generalized Lorenz system* (GLS):

$$\dot{x} = \begin{bmatrix} A & 0 \\ 0 & \lambda_3 \end{bmatrix} x + \begin{bmatrix} 0 \\ -x_1 x_3 \\ x_1 x_2 \end{bmatrix}, \; A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \tag{1}$$

where $x = [x_1 \;\; x_2 \;\; x_3]^\top$, $\lambda_3 \in R$, and A has eigenvalues $\lambda_1, \lambda_2 \in R$, such that

$$-\lambda_2 > \lambda_1 > -\lambda_3 > 0. \tag{2}$$

The inequality (2) goes back to the well-known Shilnikov's chaos analysis near the homoclinicity and can be viewed as the necessary condition for the chaos existence, see more detailed discussion in Čelikovský and Chen (2002). GLS is said to be *nontrivial* if it has at least one solution that goes neither to zero nor to infinity nor to a limit cycle. The following result, enabling the efficient synthesis of a rich variety of chaotic behaviours for GLS, has been obtained in Čelikovský and Chen (2002): For the nontrivial generalized Lorenz system (1)-(2), there exists a nonsingular linear change of coordinates, $z = Tx$, which takes (1) into the following *generalized Lorenz canonical form*:

$$\dot{z} = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} z + cz \begin{bmatrix} 0 & 0 & -1 \\ 0 & 0 & -1 \\ 1 & \tau & 0 \end{bmatrix} z, \tag{3}$$

where $z = [z_1, z_2, z_3]^\top$, $c = [1, -1, 0]$ and parameter $\tau \in (-1, \infty)$.

Actually, the parameter τ plays important role of single scalar bifurcation parameter, while remaining parameters has only qualitative influence being eigenvalues of the approximate linearization of GLS at the origin. These qualitative parameters are just required to satisfy robust condition (2), so that fine tuning may be done using the single scalar parameter τ only. In such a way, the parameter range to be used in the PRNG later on is further extended. In Čelikovský and Chen (2005) complete and nice classification of all related systems is given showing