A RANDOM SEQUENCE GENERATOR BASED ON CHAOTIC CIRCUITS*

Chen Jianxiao  Ran Lixin  Chen Kangsheng
(Dept. of Info. and Electron. Eng., Zhejiang University, Hangzhou 310027)

Abstract  In this paper, a random sequence generator based on chaotic circuits is presented. Fundamental principle and experimental circuit have been carried out in case of Chua's circuit. The statistical results are in good agreement with probability characteristics of random sequence.

Key words  Random sequence generator; Chaos; Chua's circuit

I. Introduction

The apparently random phenomena of chaos have become increasingly observed in the behavior of myriad nonlinear deterministic systems. Nowadays, more and more researchers are concentrating their attentions on various applications of chaos; a lot of papers about chaos applications have been reported[1-3]. In this paper, a new method for fabricating random sequence generator is presented. Based on Chua's circuit, the probability characteristics of random sequence generator are also given.

II. Principle

It has been well known that chaotic signal has broadband, noise-like, continuous power spectrum, and is very sensitive to initial conditions. Small disturbance to the chaotic circuit will lead to large variation of output signals, which is named "butterfly effect". Therefore, to a physical chaotic circuit, it is actually impossible for us to foretell output signal instance after a time interval long enough, even if we have known precision initial conditions of chaotic circuit. That is, if the chaotic signals were sampled in a rate slow enough and the output was set to 1 or 0 according to the amplitudes or the phases of the chaotic signals, a random sequence can be obtained.

For example, Chua's circuit is a third-order autonomous circuit, consisting of a linear inductor $L$, two linear capacitors ($C_1, C_2$), a linear resistor $R$, and a voltage-controlled nonlinear resistor $N_R$. The driving-point characteristic of the nonlinear resistor $N_R$ refers to Fig.1(b).

According to Fig.1, if we select $i_L, V_{C1}, V_{C2}$ as status variables, the state equations for

*Supported by the Doctoral Fund of the State Education Committee of China and the Nature Science Foundation of Zhejiang Province
Chua's circuit are given by

\[
\begin{align*}
\frac{dV_{C1}}{dt} &= \frac{G}{C_1} (V_{C2} - V_{C1}) - \frac{1}{C_1} f(V_{C1}) \\
\frac{dV_{C2}}{dt} &= \frac{G}{C_2} (V_{C2} - V_{C1}) - \frac{1}{C_2} i_L \\
\frac{di_L}{dt} &= -\frac{1}{L} V_{C2}
\end{align*}
\]

(1)

where \( G = 1/R \).

\[
f(V_{C1}) = \begin{cases} 
G_b V_{C1} + (G_b - G_a)E, & V_R < -E \\
G_a V_{C1}, & -E \leq V_R \leq E \\
G_b + (G_a - G_b)E, & V_R > E
\end{cases}
\]

(2)

As Ref.[4], the following circuit parameters have been used in laboratory experiment: \( L=18\,\text{mH}, \ C_1=10\,\text{nF}, \ C_2=100\,\text{nF}, \ G_a = -50/66\,\text{mS}, \ G_b = -9/22\,\text{mS}, \ E \approx 1\,\text{V} \). Keeping these circuit parameters stable, when \( R \) changes from \( 2k\Omega \) to 0, Chua's circuit will come through equilibrium point, Hopf bifurcation, limit cycle, Rossler type attractor and double-scroll attractor. Fig.2(a) shows the phase plane of Chua's double-scroll attractor \( V_{C1}-V_{C2} \), which \( R = 1.73k\Omega \). Notice that \( V_{C1} \) signal has variant signs in different scroll. Since butterfly effect of chaos, we can not foretell in which scroll will the trajectory be located after a time interval long enough. So, if we sample the \( V_{C1} \) signal with a low rate and set output as 1 or 0 according to the sign of \( V_{C1} \), we will obtain a random sequence.

### III. Experimental Circuit

Random sequence generator model based on Chua's circuit is shown in Fig.3. Chaotic signal \( V_{C1} \) of Chua's circuit was separated by buffer, quantified by 1 bit, finally binary sequence can be obtained when output circuit was controlled by sample pulse clock.

During the experiment, output data were sampled by computer parallel port, sample sequence length 100,000, sampling interval 0.5s. In order to get the binary sequence with same probability distribution, we should modulate the value of Chua's circuit power supply.