International Journal of Innovative Computing, Information and Control
Volume **3**, Number **2**, April **2007**

 ISSN 1349-4198
pp. 449–456

DESIGNING OF CHAOTIC SYSTEM OUTPUT SEQUENCE CIRCUIT BASED ON FPGA AND ITS APPLICATIONS IN NETWORK ENCRYPTION CARD

Qun Ding[1,2], Jing Pang[2], Jinqing Fang[3] and Xiyuan Peng[1]

[1]Department of Automatic Test and Control
Harbin Institute of Technology
Harbin 150001, P. R. China
ding-qun@263.net; pxy@hit.edu.cn

[2]Electronic Engineering School
Heilongjiang University
Harbin 150080, P. R. China
Pangjing2002@126.com

[3]China Institute of Atomic Energy
Beijing University of Technology
Beijing 102413, P. R. China
fjq96@126.com

Received January 2006; revised June 2006

Abstract. *Taking the Lorenz chaotic equation as an example, FPGA (Field Programmable Gate Array) technology is applied to obtain chaotic sequence in this paper. Based on the design of a digital integrator and quantification circuit, we get Lorenz chaotic output sequence by DSP Builder tool. This design method may improve arithmetic precision according to the need of the system and resource efficiency. Experiment shows the output sequence of the designed system has good self-correlation. This method can be applied to other continuous chaotic systems and may be applied to chaotic system for information security and secrecy communication field.*
Keywords: FPGA, Lorenz system, Chaos encryption, Self-correlation

1. **Introduction.** With the development of technology, a great change has taken place in the internal structure of communication equipment, computer and test instrument and so on. And discrete components and single chip structures are developing into large scale integrated chip structure and modularization structure. Although system control and complexity of operation are improved continuously, and system function is constantly enhanced, the hardware configuration of systems is becoming simpler and simpler instead and has the eminent characteristics of digital equipment, high stability, high operation accuracy, low failure rate, small volume and so on. Especially when it is combined with computer technique the degree of automation will be highly enhanced. This kind of electronic equipment constituted by a large-scale integrated circuit will be applied more and more and exhibit its superiority in modern economic constructs.

In the information security field, encryption equipment is composed of circuits and arithmetic. It is a modern developing trend of hardware encryption, namely, download the