Dynamics of Continuous, Discrete and Impulsive Systems
Series **B:** *Applications & Algorithms* **10 (2003)** 929-953

MODULAR ARITHMETIC, SYNCHRONIZED CHAOS AND SECURE COMMUNICATION

William F. Langford and Steven E. Sladewski

Department of Mathematics and Statistics
University of Guelph, Guelph ON Canada N1G 2W1
E-mail: wlangfor@uoguelph.ca

Abstract. A chaotic dynamical system has trajectories which appear to have random behaviour, even though the system is completely deterministic. Locally, nearby trajectories separate exponentially in time. Yet, Pecora and Carroll (1990) were able to show that two chaotic dynamical systems can be synchronized with a single scalar signal. This inspired proposals to use "synchronized chaos" as a masking scheme for secure communication. However, phase space reconstruction techniques, based on the underlying deterministic property of the chaotic system, have led to algorithms for unmasking the hidden signal. In this work, we present a communication scheme that works through a modular arithmetic filter. This filter removes the structure exploited by existing unmasking algorithms, yet a receiver possessing the secret "key" (composed of parameter values) is still able to synchronize with the sender and decode the communication.
Keywords. Synchronized chaos, modular arithmetic, unmasking, secure communication.
AMS (MOS) 2000 subject classification: 37D45, 37E30, 37M10.

1 Introduction

In 1990 Pecora and Carroll [21] announced a method for the *synchronization* of two chaotic systems, using only one-way coupling with a single scalar variable. This result was surprising, because it is inherent in the very nature of chaos that two chaotic systems, no matter how close to identical in their deterministic laws and initial states, will rapidly diverge as they evolve in time and soon become completely uncorrelated. Useful surveys of this concept of synchronized chaos are presented in [7, 15, 20, 29].

The result of Pecora and Carroll appeared to open a door to the use of a chaotic signal as a carrier for the communication of secret information. The chaotic signal would *mask* the information from detection by an eavesdropper on the communication channel. A synchronized chaotic system at the receiving end would be used to decode the message.

Soon after results were published on the use of synchronized chaos to mask and transmit secure communications, other researchers sought to find weaknesses in the method. Before long, it was shown that such transmissions are vulnerable to unmasking by a sophisticated eavesdropper using state