Chapter 17
A Modular Dynamical Cryptosystem Based on Continuous-Interval Cellular Automata

Jesus D. Terrazas Gonzalez
University of Manitoba, Canada

Witold Kinsner
University of Manitoba, Canada

ABSTRACT

This paper presents a new cryptosystem based on chaotic continuous-interval cellular automata (CCA) to increase data protection as demonstrated by their flexibility to encrypt and decrypt information from distinct sources. Enhancements to cryptosystems are also presented including (i) a model based on a new chaotic CCA attractor, (ii) the dynamical integration of modules containing dynamical systems to generate complex sequences, and (iii) an enhancement for symmetric cryptosystems by allowing them to generate an unlimited number of keys. This paper also presents a process of mixing chaotic sequences obtained from cellular automata, instead of using differential equations, as a basis to achieve higher security and higher speed for the encryption and decryption processes, as compared to other recent approaches. The complexity of the mixed sequences is measured using the variance fractal dimension trajectory to compare them to the unmixed chaotic sequences to verify that the former are more complex. This type of polyscale measure and evaluation has never been done in the past outside this research group.

DOI: 10.4018/978-1-4666-2476-4.ch017

1. INTRODUCTION

Cryptosystems have been developed to handle the challenging task of data protection in the modern information era. The purpose of cryptography is to hide the contents of messages to make them unrecognizable except by someone who has the decryption method available (Anghelescu, Ionita, & Sofron, 2008). Different cryptosystems have been proposed and implemented in either hardware (Anghelescu *et al*., 2007, 2008), or software (Anghelescu, Sofron, Rîncu, & Iana, 2008), or mixtures of both. Cryptosystems based on *cellular automata* (CA) (Anghelescu *et al*., 2008) are preferred over continuous chaotic systems (Moulin & Sbodio, 2010; Yifang, Rong, & Yi, 2009). Because of the simplicity and speed of CA-based computations, in contrast to the more costly equivalent models based on differential equations. Systems similar to CA were studied in the late 1950s to generate random sequences in cryptography (Wolfram, 2002).

The cryptosystem proposed in this paper is based on *continuous-interval cellular automata* (CCA) that are generalized CA. The specific interval considered is. It is shown that this cryptosystem is very fast, highly secure, and applicable to many classes of data, including text, sound, and images.

The degree of complexity of a dynamical-system or a cryptosystem based on CA has not been measured in the past. This paper presents such a complexity measure based on the *variance fractal dimension trajectory* (VFDT) (Kinsner, 2007b, 2011b; Kinsner & Grieder, 2008) to compare an unmixed CCA chaotic sequence and a mixed CCA chaotic sequence.

Cryptography is successful if the encoded information cannot be broken, and if it is computationally efficient (Stinson, 2006). Security is an important, challenging, and multi-dimensional research field in networked computing and communication systems (Alpcan & Başar, 2011). Cryptography is one of the many aspects of network security, including: access control, security protocols, information and hardware security, privacy, risk management, resource allocation among the most important ones (Alpcan & Başar, 2011). It is a good practice to identify potential non secure points, new tools, and the correct time to implement changes (Panayiotou & Bennett, 2009).

Web services bring about many new security problems. Some approaches to manage the access control rely on poor ways to enforce authentication-like feedback (Jin & Peng, 2010) from honest and dishonest accesses. This implies that the system is not able to block undesired accesses making it weak. The need of web-based systems that reduce the dishonest accesses is of vital importance for their users.

Given the dynamic nature of network security (Alpcan & Başar, 2011) one should not rely on static measures, or computationally costly algorithms. Dynamical problems require dynamical solutions (Kinsner, 2007a). A design approach for dynamical cryptosystems is provided considering the important contributions of Shannon: *"*Good mixing transformations are often formed by repeated products of two simple non-commuting operations. Hopf has shown, for example, that pastry dough can be mixed by such a sequence of operations. The dough is first rolled out into a thin slab, then folded over, then rolled, and then folded again, etc.*"* (Shannon, 1949). This idea is the core in the interaction among modules containing a CA to obtain a mixture of different complex behaviours where simple operations are of paramount importance. Implementations based either on high speed hardware, or software, or hybrid are easier to deploy.

Past computing and communication systems have not been designed with security as a priority (Sung, Hsu, & Chen, 2010; Zhao, 2010). Since it is practically impossible for a security expert to oversee all systems all the time (Alpcan & Başar, 2011), the development of more robust protection tools is required. Data from sensors or commands sent through insecure channels to actuators require protection and authenticity verification of the source requesting the execution of a task in high importance applications.