Chapter 20
Mathematical Treatment for Constructing a Countermeasure Against the One-Time Pad Attack on the Baptista Type Cryptosystem

M.R.K. Ariffin
Universiti Putra Malaysia, Malaysia

M.S.M.Noorani
Universiti Kebangsaan Malaysia, Malaysia

ABSTRACT

In 1998, M.S. Baptista proposed a chaotic cryptosystem using the ergodicity property of the simple lowdimensional and chaotic logistic equation. Since then, many cryptosystems based on Baptista's work have been proposed. However, over the years research has shown that this cryptosystem is predictable and vulnerable to attacks and is widely discussed. Among the weaknesses are the non-uniform distribution of ciphertexts and succumbing to the one-time pad attack (a type of chosen plaintext attack). In this chapter the authors give a mathematical treatment to the phenomenon such that the cryptosystem would no longer succumb to the one-time pad attack and give an example that satisfies it.

1.0 INTRODUCTION

The relationship between chaos and cryptography makes it natural to employ chaotic systems to design new cryptosystems. It is based on the facts that chaotic signals are usually noise-like and chaotic systems are very sensitive to initial conditions. Their sensitivity to initial conditions and their spreading out of trajectories over the whole interval seems to be a model that satisfies the classic Shannon requirements of confusion and diffusion (Shannon, 1949). From 1989 onwards, many different chaotic encryption systems have been proposed. The most celebrated cryptosystems based on the ergodicity property of

DOI: 10.4018/978-1-61520-737-4.ch020

chaotic maps is presented by Baptista (1998) and has received more and more attentions in the past literature (Grassi & Mascolo, 1998; Alvarez, et.al., 1999; Chu & Chang 1999; Alvarez, et.al., 2000; Jakimoski, & Kocarev, 2001; Li, et.al., 2001; Wong, et.al., 2001; Garcia & Jimenez, 2002; Wong, 2002; Palacios & Juarez, 2002; Alvarez, et.al., 2003; Pareek, et.al., 2003; Li, et.al., 2003; Wong, 2003; Wong, et.al., 2003; Alvarez, et.al., 2004; Li, et.al., 2004; Alvarez & Li 2006). Researchers in this field have also constructed chaotic cryptosystems without using chaotic synchronization (most are designed for implementation on digital circuits or computers (Jakimoski, & Kocarev, 2001; Alvarez, et.al., 2003)) and secure communications based on chaotic synchronization of analog circuits (Baptista, 1998; Alvarez, et.al., 1999; Alvarez, et.al., 2000).

In 1998, M.S. Baptista proposed a chaotic cryptosystem using the ergodicity property of the simple low-dimensional and chaotic logistic equation $X_{n+1} = bX_n\left(1 - X_n\right)$ where X_0 and b are the secret keys. This cryptosystem has the ability to produce various ciphers responding to the same message input. In other words, this type of cryptosystem is a dynamic cryptosystem due to mathematical considerations and not due to computer programming methods. Since the ciphertexts are small integers, they are suitable to be transmitted through today's public digital networks. In Baptista's original work, in order to avoid statistical and differential cryptanalysis, a random number is generated each time the chaotic trajectory has reached the desired region. If it is greater than a threshold η, the current number of iterations will be transmitted as the ciphertext. Otherwise, the iteration will continue.

Motivated by the interest in chaotic cryptosystem, and by Baptista's ergodic cipher, numerous algorithms based on variations of Baptista's have been proposed. However, over the years research has shown that this cryptosystem is predictable and vulnerable to attacks and is widely discussed. Among the weaknesses are the non-uniform distribution of ciphertexts and succumbing to the one-time pad attack (a type of chosen plaintext attack).

Wong, et.al., (2001), examined the system and came out with two major drawbacks with Baptista's approach. First, the resultant ciphertext is usually concentrated at the smaller number of iterations (i.e. the distribution of the ciphertext is non-uniform). Second, a sequence of random numbers may have to be generated for a single block of message text. After examining the problems, Wong proposed a remedy that gave a flatter distribution of ciphertext, with single random number generation for each block of message text. Wong states that, the tradeoff between the spread of the distribution of ciphertext and the encryption time can be controlled by a single parameter. Wong also used the logistic map in illustrating the remedy.

Wong (2002) proposed a fast chaotic cryptographic scheme based on iterating the logistic map whereby no random numbers are needed to be generated. Wong proposed the use of a dynamical look-up table instead of a static one. This means that the table for looking up the ciphertext and plaintext is no longer fixed during the whole encryption and decryption processes. Instead, it depends on the plaintext and will continuously be updated in encryption and decryption. The dynamical table updating process is performed until the end of the input source. By doing so, Wong claims that the relationship between consecutive ciphertext becomes dynamic and it is much more difficult for cryptanalysis. Wong performed decryption using values of X_0 and b which differ from the correct value by 10^{-9} and found that even the first decrypted block is incorrect.

Alvarez, et.al., (2003), examined Baptista's system. He presented three types of cryptanalytic attacks: one-time pad attacks, entropy attacks and key recovery attacks. The one-time pad attack is based on the chosen plain text attack scenario. However, it is noted here in Alvarez's attack, it is assumed that the S