Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Modified Baptista type chaotic cryptosystem via matrix secret key

M.R.K. Ariffin [a,*], M.S.M. Noorani [b]

[a] *Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia*
[b] *School of Mathematical Sciences, Faculty of Science and Technology, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia*

ARTICLE INFO

Article history:
Received 19 November 2007
Received in revised form 17 June 2008
Accepted 20 June 2008
Available online 3 July 2008
Communicated by A.P. Fordy

PACS:
05.45.Vx

Keywords:
Chaotic cryptosystems
Ergodicity
Cryptanalysis
Logistic map
Secret key

ABSTRACT

In 1998, M.S. Baptista proposed a chaotic cryptosystem using the ergodicity property of the simple low-dimensional 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 Letter, our objective is to modify the chaotic cryptographic scheme proposed previously. We use a matrix secret key such that the cryptosystem would no longer succumb to the one-time pad attack.

1. 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 [1]. From 1989 onwards, many different chaotic encryption systems have been proposed. The most celebrated cryptosystems based on the ergodicity property of chaotic maps is presented in [2] and received more and more attentions in the past literature [3–17]. Researchers in this field have also constructed chaotic cryptosystems without using chaotic synchronization (most are designed for implementation on digital circuits or computers [5,6]) and secure communications based on chaotic synchronization of analog circuits [2–4].

Since Baptista proposed in 1998 a new cryptosystem based on the ergodic property of chaotic systems [5], a number of new algorithms based on variations of Baptista's have been published. It encrypts the message text into the number of iterations needed for a chaotic map to reach a region on a phase space (i.e. a particular section on the range of the map) that corresponds to that text. He demonstrated his approach using a simple one-dimensional logistic map given by the following equation:

$$X_{n+1} = bX_n(1 - X_n)$$

where b is the gain and $X_n \in [0, 1]$.

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.

Wong [13], 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

[*] Corresponding author. Tel.: +603 8946 6838; fax: +603 8942 3789.
E-mail address: rezal@putra.upm.edu.my (M.R.K. Ariffin).

0375-9601/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.physleta.2008.06.077

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 [14], 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 [6], 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 association between the $S\varepsilon$-intervals and the units of some alphabet is part of the algorithm. Hence, the association is known to the cryptanalyst. In Baptista's work, this element is part of the secret key. If kept secret would result in the cryptanalyst opting for the brute force attack. Through the entropy attack a table consisting of the frequency of each symbol source $S_n = \{s_i\}_{i=1}^{n}$ is established. Due to weaknesses of the original Baptista cryptosystem, the information in the table allows one to perform a ciphertext only attack. The key recovery attack (more of an academic attack, since the assumption is $N_0 = 0, \eta = 0$) is to obtain X_0 when b is known and vice versa.

Alvarez [11], also observed the dynamical look-up table (Wong [14]) method and stated that the look-up table updating method is most unfortunate, since it allows the attacker to easily predict the new positions of the symbols even without the exact knowledge of X_0 and b. He states that, it is not necessary to know the exact value of X_0 and b to predict the next update, it suffices to know the subinterval where X_0 lands.

In this Letter, we will concentrate on Baptista's original cryptographic method and will overcome Alvarez's attack [6,11].

2. Problem statement—One-time pad attacks (i.e. chosen plaintext attack)

We will begin this second section with an overview of Alvarez's one-time pad attack He proved that the ergodic cipher put forward by Baptista behaves as a one-time pad which reuses its key, and as a result, is easy to break. The method of attack is based on the symbolic dynamics of one-dimensional quadratic map.

The illustration of this class of known plaintext attack is as follows. Assume that unknown to the cryptanalyst, the keys are $X_0 = 0.232323$ and $b = 3.78$, using the interval $[0.2, 0.8]$. Let us use a 4-symbol source $S_4 = \{s_1, s_2, s_3, s_4\}$. Under these assumptions, in a *known plaintext attack* scenario, we request the ciphertext of messages consisting of all their symbols set to s_1, s_2, s_3 and s_4, respectively.

We begin by requesting the ciphertext for a plaintext consisting of only s_1: $P = (s_1, s_1, s_1, s_1, s_1, s_1, \ldots)$. The corresponding ciphertext is $E_1 = (5, 9, 5, 3, 4, 5, \ldots)$. We are now going to construct the one-time pad which indicates the position of X_n. Examining the ciphertext, we know for sure that the 6th symbol in the one-time pad is s_1 (or equivalently, we can say that X_6 belongs to the cell that encodes s_1), that the 14th symbol is another s_1, and the 20th, and the 23rd and so on. After considering the whole message, we get the following partial sequence for the one-time pad $O = xxxxxs_1xxxxxxxxs_1xxxxs_1xxs_1xxxs_1xxxxs_1 \ldots.$ Since we chose the interval $[0.2, 0.8]$ instead of the whole attractor, the letters marked x could correspond to either an iteration below the lower bound 0.2 or beyond the upper bound 0.8 or it could also correspond to the other symbols from the 4-symbol source.

For s_2, the corresponding ciphertext is $E_2 = (8, 2, 2, 5, 7, 5, \ldots)$. We can complete more gaps in the sequence $O = xxxxxs_1xxs_2xs_2xs_2xs_1 xxs_2xs_1xxs_1xs_2xs_1xxs_2xs_1x \ldots.$ For s_3, $E_3 = (3, 3, 14, 7, \ldots)$ and $O = xxxs_3xs_1s_3xs_2xs_2xs_2xs_1xxs_2xs_1s_3xs_1xs_2xs_1s_3xs_2xs_1x \ldots.$ Lastly for s_4, the ciphertext is given by $E_4 = (1, 14, 17, 1, \ldots)$, and we are able to construct $O = xs_4xs_3xs_1s_3xs_2xs_2xs_2xs_1s_4xs_2xs_1s_3xs_1xs_2xs_1s_3xs_2xs_1s_4 \ldots.$

Hence, the one-time pad is constructed. The symbol x correspond to points outside the boundaries and cannot be used for encryption. It is important to note that knowing the one-time pad generated by a certain key (X_0 and b) is entirely equivalent to knowing the key.

As an example, let us first construct the ε-intervals with its corresponding source. Since $n = 4$, we have $\varepsilon = 0.15$, and s_1 is associated with the interval $[0.2, 0.35)$, s_2 with the interval $[0.35, 0.5)$, s_3 with the interval $[0.5, 0.65)$ and finally s_4 with the interval $[0.65, 0.8)$. Given the following ciphertext $C^* = (1, 4, 3, 2, 2, 3, 5)$, it is easily derived from the one-time pad that the corresponding plaintext is $P = s_4, s_1, s_2, s_2, s_2, s_4, s_3$.

The focus of our research is to overcome the one-time pad attack. As pointed out by Alvarez, obtaining the one-time pad is as good as knowing the key (i.e. X_0 and b), making the system 100% vulnerable. Hence, our objective is to modify the original Baptista chaotic cryptosystem, through introducing a matrix secret key and eventually making the one-time pad attack untenable.

3. Result—The modified Baptista type chaotic cryptosystem via matrix secret key

We will modify Baptista's cryptographic method to overcome the above attack. It will be presented in stages.

3.1. Encryption

3.1.1. Preparing the associated sites choosing a chaotic map and secret keys.

i. Assume that we construct a look-up table consisting of n ε-intervals. The sites are numbered $0, 1, 2, \ldots, n-1$.
ii. Represent each site with its decimal representation.
iii. The minimum value of the first interval is 0, and the upper bound of the final interval is 1.
iv. Choose a one-dimensional chaotic map with the onto property [18].
Example 1:
The logistic map, $x(n+1) = bx(n)(1 - x(n))$ for $b = 4$.