TRANSACTIONS ON SCIENCE AND TECHNOLOGY

Modified Baptista Type Chaotic Cryptosystem via the Mutation Technique Idea

Muhamad Azlan Daud[1#], Mohd Mughti Hasni[2],
Wardatul Akmam Din[1], Zahari Mahad[3]

1 Preparatory Center for Science and Technology, Universiti Malaysia Sabah, Jalan UMS, 88400 Kota Kinabalu, Sabah, MALAYSIA.
2 Department of Fundamental and Applied Sciences, Faculty of Science and Information Technology, Universiti Teknologi PETRONAS, 36210 Bandar Seri Iskandar, Perak, MALAYSIA.
3 Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, MALAYSIA
# Corresponding author. E-Mail: azlan.daud@ums.edu.my; Tel: +6088-320000 Ext: 5621; Fax: +6088-435324.

ABSTRACT In 1998, M.S. Baptista proposes a chaos-based cryptography system using the ergodicity property of the simple low-dimensional and chaotic logistic equation. Each "letter" will have a particular site in the interval $[0,1]$. 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 paper, our objective is to modify the Baptista's chaotic scheme proposed previously. We employ the mutation technique idea from GIC cryptosystem such that the cryptosystem would no longer succumb to the one-time pad attack.

KEYWORDS: chaotic logistic equation, chaotic cryptosystems; mutation technique; ergodicity, one-time pad

I **Received** 19 December 2018 II **Revised** 9 July 2018 II **Accepted** 12 July 2018 II **In press** 6 August 2018 II **Online** 28 August 2018 I

INTRODUCTION

In 1998, M. S. Baptista proposed a chaos-based cryptography system using the ergodicity property of the simple low-dimensional and chaotic logistic equation. Each "letter" will have a particular site in the interval $[0,1]$. Cryptographic system is implemented by iterating the logistic map, $x_{i+1} = bx_i(1 - x_i)$, where for a control parameter $b \in \mathbb{Z}^+$ set to make logistic map have a chaotic behavior. When the iteration is an element of a site specific alphabet, the number of iterations passed, n, where $n \geq 1$ will be taken. Then a random number will be generated, k and compared with n. If $k > n$ then n will be different ciphertext of identical letters. Then, someone who wants to overcome these cryptographic systems will have to deal with text ciphers that can represent different characters. Therefore, the attacker is then confronted with a high probability of text ciphers because each text ciphers has the same probability to represent any letter (Baptista, 1998).

In 2003, Alvarez reviews the cryptographic system in his paper entitled "Cryptanalysis of a Discrete Chaotic Cryptosystem Using External Key" and produces a one-time pad attack, a type of attack that can occur once the original text is known. This attack can successfully overcome chaos-based cryptography of dynamic system proposed by Baptista. This attack has been exploited successfully for text ciphers with ergodic nature that resembles a one-time pad attack by assuming the key. Method of attack is based on the symbolic dynamics of one-dimensional quadratic mapping, (Alvarez *et al.*, 2003).

After the Baptista's original proposal, many variant cryptosystems based on chaotic maps have been proposed for cryptographic implementation. In 2008, (Ariffin & Noorani, 2008) attempts to modify the cryptosystem to enhance the performance of the original Baptista's cryptosystem via an example. Rhouma (2009) identifies a flaw in Ariffin's, specifically in step 4 of the encryption procedure, where it does not implement one-to-one operation, resulting in failure to decrypt the ciphertext.

Genetic algorithms Inspired Cryptography (GIC) cryptosystem has been developed by (Tragha *et al.*, 2005) who make use of two important techniques: crossover and mutation in data encryption (Kochladze & Beselia, 2016). By using these techniques, the ciphertext and secret key can be generated. GIC cryptosystem is one example of symmetry cryptosystem where one secret key has been involved in the process of encryption and decryption. GIC has been considered as a secure cryptosystem where it reinforces resistance to cryptanalysis (Hassan *et al.*, 2014).

The GIC cryptosystem encrypts a plaintext by changing part of the original properties in plaintext to produce a ciphertext that has different properties to the block in plaintext. The encryption process in GIC cryptosystem is initiated by breaking the plaintext into blocks of the same size. After that, the technique of genetic algorithm mutation or crossover techniques will run to encrypt the plain text by changing some of the bits in the blocks of plain text. Crossovers are the process of converting part of the bit between two or more different blocks to form something new. Mutation techniques involve some changes in the value of the bit in one block with random. In this paper, the mutation technique idea from GIC cryptosystem is discretized in order for it to be suitable for cryptographic applications (Daud *et al.*, 2016). The mutation technique idea will be utilized to enhance a cryptosystem utilizing the Baptista's mechanism. The result will be resistant toward Alvarez's one time pad attack (Ariffin *et al.*, 2012). Modified Baptista Type Chaotic Cryptosystem via the Mutation Technique Idea will implement one-to-one operation, resulting in no failure to decrypt the ciphertext (Daud & Ariffin, 2013).

THE MODIFIED ENCRYPTION ALGORITHM

The Baptista cryptosystem is not protected against attacks similar to the one-time pad attack that occurred in 2003 (Alvarez *et al.*, 2003). The strong characteristics from the original Baptista cryptosystem have to be sustained. In this subsection, we will go through the GIC Mutation technique. GIC Mutation technique consisting of the maps,

$$m_i^{'} = 1 - m_i, \qquad i = x, x+1, x+2, \dots, y$$

where $x < y$, i and $i+1$ are bit numbers in a certain block. One block plaintext is consist of 16 – bits,

$$M = [0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0]$$

Let $x = 3$ and $y \ = 11$, then we perform GIC Mutation technique maps $m_{i+1} = 1 - m_i$ to get

$$M' = [0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0]$$

Encryption Algorithm

Algorithm 1: Preparing a chaotic map

```
1: Assume that we construct a look-up table consisting of $j$ $\varepsilon$-intervals.
2: Represent each site with $S_1, S_2, S_3, \dots, S_j$.
3: The minimum value of the first interval is 0, and the upper bound of the interval is 1.
4: Choose a one-dimensional chaotic map; $x_{i+1} = bx_i(1 - x_i)$, where for a control parameter $b \in \mathbb{Z}^+$
   set to make logistic map have a chaotic behavior.
5: Then, we have $n$-sets of ciphertext, $C_1 = [c_1, c_2, c_3, \dots, c_{n-1}, c_n]$
6: Determine the largest value of ciphertext, $c_l$ from original ciphertext, $C_1$.
```

Algorithm 2: Preparing the new secret keys $\boldsymbol{x}$, $\boldsymbol{y}$ and $\boldsymbol{c_l}$

```
1: The new map, $c_i' = c_l - c_i$ for $i = x, x+1, x+2, \dots, y$, where $x, y \in \mathbb{Z}^+$ and $x < y$.
2: Choose the secret keys, $x$ and $y$ randomly.
3: Then, the new ciphertext, $C'$; $C_2 = [c_1', c_2', c_3', \dots, c_{n-1}', c_n']$
```

UNIQUENESS OF THE MODIFIED DECRYPTION PROCESS AND BAPTISTA DECRYPTION ALGORITHM

Uniqueness of the Modified Decryption Process

Proposition 1 (Modified Decryption Algorithm)

The following decryption process of encryption information by Algorithm 2 is unique.

i. Compute, $c_x = c_l - c_x'$.

ii. Compute, $c_{x+1} = c_l - c_{x+1}'$.

iii. Continue until $c_y = c_l - c_y'$. The original data is C.

Proof

Let c_x' be parameter that is used to input into the modified decryption procedure prior to the procedure giving output c_x (i.e $c_x = c_l - c_x'$). The encryption algorithm consists of a sequence of subtractions. Assume that the encryption process is not unique, then, we have the following relations;

$$c_{x+j}' = c_l - c_{x+j}$$

and

$$c_{x+j}' = c_l - [c_{x+j}]$$

where $c_{x+j} \neq \lfloor c_{x+j} \rfloor$. Following through we will have:

$$c_l - c_{x+j} = c_l - \lfloor c_{x+j} \rfloor$$

This would imply that $\boldsymbol{c_{x+j} - [c_{x+j}] = 0}$. Thus, $\boldsymbol{c_{x+j} = [c_{x+j}]}$. This is a contradiction. Hence assumption is false and the modified decryption process provides a unique output.■

Baptista Decryption Process

The original data C is a set of integer. Each integer is used to iterate the logistic map until it falls into the corresponding phase space of the first character and continues iterating until the final character to get the original plaintext.

RESULT AND DISCUSSION

Example

Let us use a 4-symbol source, $S_4 = \{s_1, s_2, s_3, s_4\}$. For illustrative purposes, we assume the key $X_0 = 0.232323$ and parameter $b = 4$. The text message is given by $P = s_4, s_3, s_1, s_1, s_2, s_4, s_3, s_1$.

Table 1. Phase Space for $S_4 = \{s_1, s_2, s_3, s_4\}$

Site	Associated interval (phase space)
s_1	[0, 0.25)
s_2	[0.25, 0.5)
s_3	[0.5, 0.75)
s_4	[0.75, 1)

Encryption procedures step-by-step:.

i. Choose $x = 2$ and $y = 6$.

ii. Each character P is then encrypted via Baptista cryptography method.

iii. Let the following ciphertext, C_1: 2, 1, 2, 3, 7, 1, 16, 2.

iv. The largest value of ciphertext, $c_l = 16$.

v. From the following ciphertext, C_1, compute $c_i' = c_l - c_i$, for $i = x, x + 1, x + 2, \ldots, y$

$$
\begin{aligned}
c_2' &= 16 - 1 \\
c_3' &= 16 - 2 \\
c_4' &= 16 - 3 \\
c_5' &= 16 - 7 \\
c_6' &= 16 - 1 \\
c_7' &= 16 - 16
\end{aligned}
$$

vi. Return a new ciphertexts, C_2:2, 15,14, 13, 9, 15, 0, 2

vii. Next transmit $C_2$to recipient.

Decryption procedures step-by-step:.

i. The following ciphertex C_2 : 2, 15,14, 13, 9, 15, 0, 2.

ii. To decrypt, compute $c_x = c_l - c_x'$ where $x = 2$ and $y = 6$.

iii. Do subtraction procedure

$$
\begin{aligned}
c_2' &= 16 - 15 \\
c_3' &= 16 - 14 \\
c_4' &= 16 - 13 \\
c_5' &= 16 - 9 \\
c_6' &= 16 - 15 \\
c_7' &= 16 - 0
\end{aligned}
$$

iv. From the subtraction, we will get the actual ciphertext, $C_1 = 2, 1, 2, 3, 7, 1, 16, 2$.

v. Iterate the chaotic map first 2-times, second 1-time and so on.

vi. Return the plaintext, $P = s_4, s_3, s_1, s_1, s_2, s_4, s_3, s_1$.

Cryptanalysis Using Alvarez's One Time Pad Attack (Chosen Plaintext Attack)

In this section, we analyzed the modified Baptista Cryptosystem algorithm with the one-time pad attack designed by Alvarez (2003). Let number of ciphertext is 12. The secret key we will use is given by $x = 1$, $y = 5$ and c_i depending on the C_1.

i. Start by requesting the ciphertext forS_1. After the procedure gets, $S_1^* = (6, 8, 10, 10, 10, 3, 11, 1, 1, 1, 1, 5)$.

ii. For S_2, $S_2^* = (3, 0, 7, 7, 7, 2, 7, 7, 2, 7, 9, 2)$.

iii. For S_3, $S_3^* = (19, 18, 11, 0, 10, 2, 4, 5, 6, 2, 10, 2)$.

iv. For S_4, $S_4^* = (5, 5, 4, 1, 4, 2, 2, 2, 2, 7, 2, 5)$.

v. With the above information a one-time pad constructed as:

$$O = xx\boxed{s_2 s_2}x s_4 s_1 xxx\boxed{s_4 s_2}xxx\boxed{s_4 s_1}s_4 x s_2 x\boxed{s_4 s_3}x s_4 x s_4\boxed{s_2 s_1}s_4 s_2 s_4$$
$$xxxxx s_2\boxed{s_4 s_1}x s_4 s_3 xx s_2 s_4 s_2 x s_1 xx s_1\boxed{s_3 s_3}s_2 xxxxxxxx\boxed{s_3 s_2 s_1}$$
$$s_1 s_3 s_2 s_1 s_1 s_1 x s_3 xx s_1 x s_3 xxxxx s_3 x s_3 xxxxxxxxx s_3 x s_3.$$

vi. Constructed one-time pad has 2 possibilities at 7 places and 3 possibilities at 2 places.

With the above information a cryptanalyst will have to construct a one time-pad with $(4 \times 4)^7 \times (4 \times 4 \times 4)^2 = 1099511627776$ possibilities of combination. Assuming that, for a large symbol source, the number of possible combinations will be larger than 2^{128}. Hence, the one-time pad attack against the Baptista's cryptosystem is enhanced by the mutation technique idea will be infeasible. However, the cryptanalyst will obtain a one-time pad with more than one possible combination, assume if he employs the one-time pad attack against our modified Baptista type chaotic cryptosystem. In our 4-character "alphabet" example, there are at least 1099511627776 combinations to try. The number of possibilities to construct the correct one-time pad sequence increases exponentially as the increase number of characters in an "alphabet". This fact ensures the security of our modified Baptista type chaotic cryptosystem against the one-time pad attack**.**

CONCLUSION

From the results, this strengthened Baptista type cryptosystem is now resistant towards the one-time pad attack. It is obvious that the advantages of this method by the number of possibilities to construct the correct one-time pad sequence increases exponentially as the number of characters in an "alphabet" increases. It also has certain cryptographic properties that are favorable. Since it utilizes integers as its ciphertext, it is suitable to transmit digital information. Research on further enhancement of the cryptosystem via the mutation technique idea should be conducted in order to gauge the effectiveness of the mutation technique idea within the Baptista type cryptosystem. Empirical results should be compared with other symmetric cryptosystems in order to further understand this unique cryptosystem. Furthermore, research should also be conducted with other chaotic maps and results focusing on security as well efficiency of these maps will give a better conviction on which chaotic map is most suitable to be utilized via the Baptista concept with the mutation technique idea

ACKNOWLEDGEMENTS

We would like to thank University Malaysia Sabah for supporting our participation and scholarship.

REFERENCES

[1] Alvarez G., Montoya F., Romera M. & Pastor G. (2003). Cryptanalysis of an ergodic chaotic cipher. *Physics Letters A*, **311**, 172–179.

[2] Ariffin M. R. K. & Noorani M. S. M. (2008). Modified Baptista type chaotic cryptosystem via matrix secret key. *Physics Letters A*, 327, 427 - 430.

[3] Ariffin M. R. K., Al-Saidi N. M. G., Said M. R. M., Mahad Z. & Daud M. A. (2012). A New Direction in Utilization of Chaotic Fractal Functions for Cryptosystems. *In:* Banerjee, S., Rondoni, L. & Mitra, M. (Eds). *Applications of Chaos and Nonlinear Dynamics in Science and Engineering* (Vol. 2). Springer Verlag Berlin Heidelberg, 233-248.

[4] Baptista M. S. (1998). Cryptography with chaos. *Physics Letters A*, **240**, 50–54.

[5] Daud M. A. & Ariffin M. R. K. (2013). A new Efficient Analytically Proven Lossless Data Compression for Data Transmission Technique. *Malaysian Journal of Mathematical Sciences*, **7**(S), 117-129.

[6] Daud M. A., Ariffin M. R. K., Kularajasingam S., Hussin C. H. C., Juhan N. & Hasni M. M. (2016). Use of new efficient lossless data compression method in transmitting encrypted baptista symmetric chaotic cryptosystem data. *Jurnal Teknologi*, **78**, 6-4.

[7] Hassan S. O., Shalash A. F. & Saudy N. F. (2014). Modifications on RSA cryptosystem using genetic optimization. *International Journal of Research and Reviews in Applied Sciences*, **19**, 150-155.

[8] Kochladze Z. & Beselia L. (2016). Cracking of the Merkle-Hellman Cryptosystem Using Genetic Algorithm. *Transactions on Science and Technology*, **3**(1-2), 291 - 296.

[9] Rhouma R. (2009). Comment on modified Baptista type chaotic cryptosystem via matrix secret key. *Physics Letters A*, 373, 3398–3400.

[10] Tragha A., Omary F., Kriouile A. (2005). *Genetic Algorithms Inspired Cryptography*. AMSE Association for the Advancement of Modeling & Simulation Techniques in Enterprises, Series D: Computer Science and Statistics.