QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

A Proposed Public Key Encryption Based on Hybrid Chaotic Maps

Prof. Dr. Ahmed T. Sadeeq
Department of Computer Science, University of Technology - Iraq
drahmaed_tark@yahoo.com
Assist Prof. Dr. Alaa K. Farhan
Department of Computer Science, University of Technology – Iraq
Dralaa_cs@yahoo.com
Shaimaa A. Hassan
Institute of Medical Technology, Middle Technical University- Iraq
aminamoj@yahoo.com

ARTICLE INFO

Article History:

Received: 19 March 2017

Accepted: 1 April 2017

Published: 10 April 2017

DOI:

10.25212/lfu.qzj.2.2.08

Keywords: *Public Key Encryption, Hybrid Chaotic Map, 3D Logistic Map, 3D Arnold Cat Map, Rotation Equation.*

ABSTRACT

Cryptography has long history by providing a way to store sensitive information or transmit it across insecure networks (i.e. the Internet) so that it cannot be read by anyone except the intended recipient. Because data transmitted over the network is vulnerable to attack, it must be considering the security aspect of it. In this paper, a public key encryption algorithm based on hybrid chaotic maps is proposed. The proposed algorithm uses a mixing of three dimensional Logistic map, three dimensional Arnold Cat map, two dimensional Rotation Equation and Chebyshev map to set random values to this algorithm and to generate privet and public keys that are used to encrypt and decrypt data. The experimental results show that the generated keys have the characteristics of truly random numbers and pass most of statistical and NIST tests.

1. INTRODUCTION

Forthousands of years cryptography and encryption have been used for secure communication. Cryptography is the science and the study of secret writing techniques [1].

Asymmetric encryption also known as **public-key encryption** is one form of cryptosystem in which different keys are used to perform encryption and decryption one is a public key and the other is a private key. Public Key encryption can be used for authentication, confidentiality, or both [2].

The major advantage of using the public key encryption is that they avoid the need of sharing any shared key between the transmitter and the receiver via a secure channel. In a shared key encryption scheme the transmission of a private key via a secure channel can cause a completely danger to the encryption scheme [3].

Chaos theory is a field of mathematics. It is the study of complex, nonlinear and dynamic systems. This field was pioneered by Lorenz in1963**.** [4]. Nonlinear equation is deterministic that can generates random or chaotic behavior over time [5]. Dynamic system is very

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

sensitive to initial condition and its response known as a Butterfly Effect, in which small change in initial state has led to unpredictable change in the final state [6]. The chaotic behavior has been widely studied and many generators have already been used to generate sequences of pseudo random numbers [7].

2. RELATED WORK

Many researchers uses chaotic map in public key encryption. In [8] a public-key encryption algorithm based on iteration of one-dimensional Chebyshev chaotic maps and two-dimensional of torus automorphisms chaotic map was proposed. This encryption schemes are both secure and practical, and can be used also for digital signature.

In [9] a new cryptosystem by using iterations of an expansion chaotic map was proposed. The expansion map is modified logistic map. The proposed cryptosystem is a symmetric-key cryptography has characteristic of public-key cryptography, that uses three kinds of keys, a public key, a private key and a common private key.

In [10] an expansion of the public key encryption based on chebyshev polynomials with a modest hash function was proposed. This model can be applied on multilevel inputs types such as images and videos.

3. PUBLIC KEY ENCRYPTION BASED ON CHEBYSHEV MAP

A public-key encryption algorithm based on chaotic maps is first proposed by Alfred in 1996. Chaotic map used in this algorithm is Chebyshev map which shown in Equation (1). The algorithms described here use a remarkable property called semi group property as shown in Equation (2).

$$Tn(x) = 2xT_{n-1}(x) - T_{n-2}(x) \quad (1)$$

Where $n \geq 2$, $x \in [-1, 1]$, $T_0(x) = 1$ and $T_1(x) = x$.

$$T_r(T_s(x)) = T_{r \cdot s}(x) \quad (2)$$

Public key encryption based on Chebyshev map consists of three algorithms. The first one is the Key generation algorithm (shown in Algorithm (1)) that generates public and private keys. The second one is the encryption algorithm (shown in Algorithm (2)), while the third algorithm is the decryption algorithm (shown in Algorithm (3)) [10].

Algorithm (1): Key Generation.

Output: Pubic key (x,Ts(x)), Private key s.

Begin

Generates a large integer s;

Selects a random number x in the interval [-1, 1] and computes Ts(x);

Sets the public key to (x, Ts(x)) and the private key to s;

End.

Algorithm (2): Message Encryption.

Input: public key (x, Ts(x)).

Output: Cipher message C.

Begin

Obtains authentic public key (x, Ts(x));

Represents the message as a number M in the interval [-1,1];

Generates a large integer r;

Computes Tr(x), Tr·s(x) = Tr(Ts(x)) and X =M· Tr·s(x);

The cipher text C = (Tr(x), X);

End.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

Algorithm (3): Message Decryption.
Input: Private Key s.
Output: Message M.
Begin
Uses the private key s to compute Ts·r(x) = Ts(Tr(x));
Recovers M by computing M = X/Ts·r(x);
End.

4. THE PROPOSED ALGORITHMS OF PUBLIC KEY ENCRYPTION BASED ON HYBRID CHAOTIC MAPS

This method is depends on chaotic maps to generate private and public keys to encrypt and decrypt data using public key encryption. So, the main purpose of this improvement is to strength the randomization by using hybrid chaotic maps.

The proposed algorithm uses hybrid chaotic maps in setting the main parameters, generating public and private keys and also in encrypting and decrypting messages. To provide a good environment for this map to work, numbers between 0 and 255 are divided to interval between 0 and 1. The Fraction_code algorithm shown in Algorithm (4) takes integer values between 0 and 255 and converts them to 256 real ranges between 0 and 1 to support the values resulted from the chaotic maps.

The main parameters (s,r,x) are set by using a combination of hybrid multidimensional chaotic maps. The chaotic maps that are used as key generator consist of a combination of three dimensional Logistic map shown in Equation (3) [11], Rotation Equation map shown in Equation (4)[12,13] and three dimensional Arnold Cat map shown in Equation (5) [14,15]. The block diagram of this combination is shown in Figure (1).

$$\begin{aligned} x_{i+1} &= \lambda x_i(1-x_i) + \beta y_i^2 + \alpha z_i^3 \\ y_{i+1} &= \lambda y_i(1-y_i) + \beta z_i^2 y_i + \alpha x_i^3 \\ z_{i+1} &= \lambda z_i(1-z_i) + \beta x_i^2 z_i + \alpha y_i^2 \end{aligned} \quad (3)$$

Here Equation (3) exhibits the chaotic behavior for $3.53<\lambda<3.81$, $0<\beta<0.022$, $0<\alpha<0.015$, and can take the value between [0,1].

$$\begin{aligned} x_{t+1} &= -a-(x_t+a)\cos\theta + y_t \sin\theta / r_t \\ y_{t+1} &= -x_t r_t \sin\theta + y_t \cos\theta \\ r_t &= \sqrt{0.5\left(x_t^2 + \sqrt{x_t^4 + 4y_t^2}\right)} \end{aligned} \quad (4)$$

Where the parameters are θ = 2 and a = 2.8, with initial conditions x0 = 0.5, y0 = 1.0.

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = \begin{bmatrix} 1 & a & 0 \\ b & ab+1 & 0 \\ c & d & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \bmod 1 \quad (5)$$

After the initial values are set, each one of those maps generates real values that are converted to binary by using a threshold value as shown in Algorithm (5). The threshold value that is used in the present study is equal to 0.5. So, the resulted binary digits from those maps are eight digits (three digits from Logistic and Cat maps and two digits for Rotation map). Those digits are merged together and the result is converted to decimal. This decimal value is used to loop Chebyshev map shown in Equation (6) [16].

$$x_{(n+1)} = Tk(x_n) = \cos(k \times \arccos(xn)) \quad (6)$$

Where $x_n \in [-1, 1]$ and $k \in [2,\infty)$.Restricted in the interval [−1, 1] [10].

The final result is converted to binary number. Then, a normalization process is made to that binary number. This process is described in Algorithm (6). The first loop is used to set the parameter s which is a large integer that represents the private key. The second loop is used to set the parameter r, while the third loop is used to set random x which it is between

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

0 and 1. In key generation step shown in Algorithm (7), the s and x parameters are used with a Rotation equation to compute the public key. The r, x and s parameters are used with a first order Chebyshev map and another with a Rotation equation to encrypt and decrypt message. The encryption algorithm is shown in Algorithm (8).

In decryption steps shown in Algorithm (9) the same chaotic maps with the same initial values are used to generate the random values. Those values are converted to binary using Algorithm (5) and an inverse Fraction_code is used in decryption process to convert the result to ASSCII form as shown in Algorithm (10).

Algorithm (4): Fraction_code

Input: integer values between 1 and 256;
Output: Fraction _code as array of ranges between 0 and 1;
Begin
  For i=0 to 255
      Represent the value of i as a real value in range [i, i+1) with three fraction digits;
      Put the result of above step in Fract_array[i];
  End For
  Fraction_code = Fract_array;
End.

Algorithm (5): Convert The Result of 3-D Chaotic Map to Binary Using Threshold Value.

Input: Result of 3-D chaotic R.
Output: Binary-digits.
Begin
  For j=1 to number of R
      If R_j >= 0.5 **Then**
        Binary-digits= Binary-digits & 1
      Else
        Binary-digits= Binary-digits & 0
      End If
  End For
End.

Algorithm (6): Normalization of Binary Values.

Input: Real Value R.
Output: Normalized Binary Value BN.
Begin
  B= Convert R to binary;
  If B contains exponent part and fraction part **Then**
    BN=merge the fraction with the exponent after eliminate '.'
  Else If B in exponential (Floating point) format **Then**
    BN= B* 10^number of digit after exponential part
  Else
    BN=B
  End If
End.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

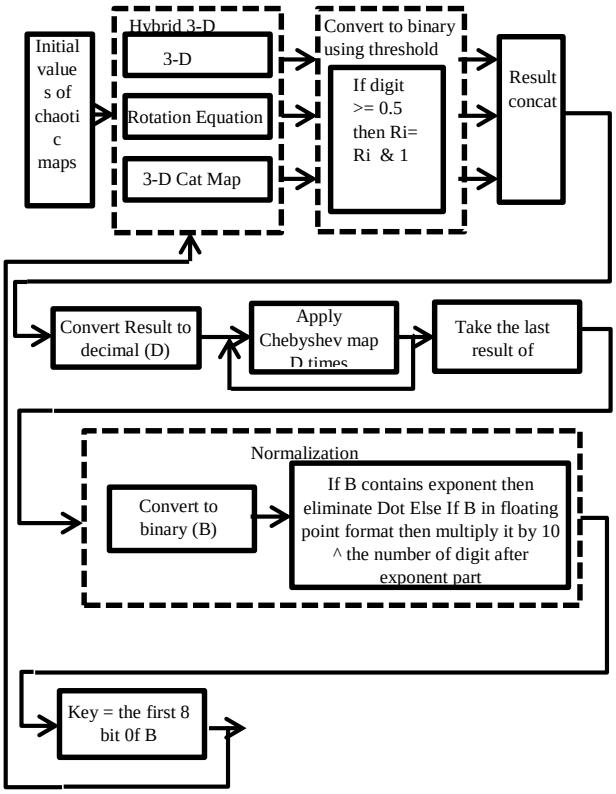

FIGURE 1: The Combination of the 3-D chaotic maps.

Algorithm (7): Public and private Key Generation

Input: vector of initial chaotic map values.
Output: Public key, Private key;
Begin
For i=1 to 3
Apply 3-D Logistic map shown in Equation (3);
Apply Rotation Equation shown in Equation (4);
Apply 3-D Arnold Cat map shown in Equation (5);
Convert the result of the three maps to binary using threshold = 0.5;
Bit= concat the result of the three maps;
D= convert Bit to decimal;
For j= 1 to D
Apply first order Chebyshev map shown in Equation (1);
End For
B=take the last result of Chebyshev map and convert it to binary;
Normalize B using Algorithm (6);
If i=1 **Then**
S=take only first 8 bit of B and convert it to decimal;
Else
If i=2 **Then**
R= Take only first 8 bit of B and convert it to decimal;
Else
T= Take 30 bit from B and convert it to decimal;
X= convert T to real value between [0,1] using Fraction_code;
End If

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

End For
Compute Rotation Equation (RRs(x));
Public key=(x,RRs);
Privet key=s;
End.

Algorithm (8): Public Key Encryption
Input: Message M, Initial values of Rotation and Chebyshev.
Output: Cipher.
Begin
M= select a message and convert it to ranges between [0,1] using Fraction-code Algorithm;
Compute Lr(x) by using Chebcheve map shown in Equetion (1);
Compute RRrs(x) using Rotation Equation shown in Equation (4);
X=M.RRrs(x);
Cipher= (Lr(x),X);
End For
End.

Algorithm (9): Public Key Decryption.
Input: Cipher.
Output: Palin.
Begin
Compute Rotation Equation RR(sr);
M= X/ RR(sr);
Plain= Inverse Fraction_Code;
End.

Algorithm (10): Inverse Fraction_code
Input: Fraction _code as array of ranges between 0 and 1;
Output: integer values between 1 and 256;
Begin
For i=0 to 255
Take the real value and find the equivalent integer value in Fraction_code array;
Put the rult of above step in Inverse Fract_array[i];
End For
Inverse Fraction_code =Inverse Fract_array;
End.

5. EXPERIMENTAL RESULTS

In this section the proposed algorithm is tested. Those tests includes testing the key generated from the proposed algorithm. The five basic statistical tests and NIST tests are used to examine the randomness of the generated key

The basic tests are used to determine whether the sequence possess specific characteristics of truly random numbers. However, if the sequence passes all tests there is no guarantee that it was produced by a random bit generator [16].The generated keys from the proposed algorithm are examined using those tests. The results show that the generated bit streams have the characteristics of truly random numbers as shown in Table (1). In this table, the different length of keys are statistically tested and pass most of tests.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

TABLE 1: The results of Statistical tests.

Key Size	Test Name	Value (X)	X2 Chi Square			
			α	Degree	Value (X)	Result
32	Frequency	0.5	0.05	1	3.8415	Pass
	Serial	0.88817	0.05	2	5.9915	Pass
	Poker	0.5	0.05	1	5.9915	Pass
	Run	0	0.05	-2	3.8415	Pass
64	Frequency	0.25	0.05	1	3.8415	Pass
	Serial	1.0675	0.05	2	5.9915	Pass
	Poker	11.25	0.05	3	9.4877	Not Pass
	Run	2.125	0.05	0	5.9915	Pass
128	Frequency	2	0.05	1	3.8415	Pass
	Serial	2.4331	0.05	2	5.9915	Pass
	Poker	7.5238	0.05	7	15.5073	Pass
	Run	2.8101	0.05	2	9.4877	Pass
256	Frequency	8.2656	0.05	1	3.8415	Not Pass
	Serial	7.7148	0.05	2	5.9915	Not Pass
	Poker	13.5411	0.05	7	15.5073	Pass
	Run	7.4057	0.05	2	15.5073	Pass

NIST tests consist of sixteen tests that are used to test the randomness of sequences. The SUCCESS means that the sequence is acceptable and it has enough randomness, while the FAILURE means that the sequence is not acceptable because of non-randomness.There are two tests which are Random Excursion, and Random Excursion Variant that do not give results each running because they only give results when the number of cycles greater than 500 as shown in Equation (7) [17].

$$j < \max(0.005\sqrt{n}, 500) \quad (7)$$

Where J indicates the total number of the cycles in the sequence. Another test which is Linear Complexity test is also not indicates P-value because some bits are discarded. Table (2) shows the result of the NIST tests. The generated sequence from the proposed algorithm passes most of those tests.

TABLE 2: The results of NIST tests.

Test Name	Number of tests	Number of Success	Number of Fail	Percentage of Success tests
Approximate Entropy	181	181	0	100%
Block Frequency	181	181	0	100%
Cumulative Sum (Forward)	362	362	0	100%
Fast Fourier Transform	181	181	0	100%
Frequency	181	180	1	99%
Lempel Ziv Compression	181	181	0	100%
Longest Run of Ones	181	181	0	100%
Non Periodic Template	26788	21429	5359	79%
Overlapping Template of all Ones	181	181	0	100%
Rank	181	181	0	100%
Run	181	178	3	98%
Serial	362	357	5	98%
Universal	0	0	0	Not number

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

6. CONCLUSIONS

From the presented study it has been concluded that, using hybrid chaotic maps in public key encryption instead of one map strengths the system and makes it more robust against the attackers. Also, the results of hybrid maps have the characteristics of truly random numbers because they pass most of statistical and NIST test which makes it difficult for the intruder to crack the original data.

References

[1] Nicholas G. McDonald, "Past, Present, and Future Methods of Cryptography and Data Encryption", A Research Review, 2010.
[2] William Stallings, "Cryptography and Network Security Principles and Practice", Fifth Edition, Prentice Hall, 2011.
[3] Adel A., Amr H. , Hany H., "Survey Report on Chaos Based Public-key Cryptosystem" , International Journal of Emerging Technology and Advanced (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 12, December 2013).
[4] David Levy, "Chaos Theory and Strategy: Theory, Application. And Managerial Implications", Massachusetts Strategic Management Journal, Vol. 15, 167-178, U.S.A (1994).
[5] L. Douglas Kiel, Euel W. Elliott, "Chaos Theory in the Social Sciences: Foundations and Applications", The University of Michigan Press, 1996.
[6] Étienne Ghys, "The Butterfly Effect", 12th International Congress on Mathematical Education, 2012.
[7] Kharel, Rupak, "Design and Implementation of Secure Chaotic Communication Systems", Doctoral thesis, Northumbria University, 2011.
[8] Ljupco Kocarev, Marjan Sterjev, Attila Fekete, Gabor Vattay, "Public-key encryption with chaos", American Institute of Physics, Vol. 14, No. 4, 1078-1082, 2004.
[9] Shuichi Aono, Yoshifumi Nishio, "A Cryptosystem Based on Iterations of Chaotic Map", IEICE Technical Report, Vol.107, No.87, 2007.
[10] K. Prasadh, K. Ramar, R. Gnana jeyaraman, "Public key cryptosystems based on chaotic Chebyshev polynomials", Journal of Engineering and Technology Research, Vol.1 (7), 122-128, 2009.
[11] Pawan N. Khade, and Manish Narnaware, "3D Chaotic Functions for Image Encryption", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, 2012 ISSN 1694-0814.
[12] Skiadas, "Mathematical models of Chaos. In Chaos Applications in Telecommunications", Stavroulakis, P., Ed.; CRC Press: Boca Raton, FL, USA, 2006; pp. 383–413.
[13] Skiadas, " In Chaotic Modelling and Simulation: Analysis of Chaotic Models, Attractors and Forms", CRC Press: Boca Raton, FL, USA, 2008.
[14] Daniel-Ioan Curiac and Constantin Volosencu, "Path Planning Algorithm based on Arnold Cat Map for Surveillance UAVs", Defence Science Journal, Vol. 65, No. 6, November 2015, pp. 483-488, DOI : 10.14429/dsj.65.8483 ,2015, DESIDOC
[15] Tang, W.K. & Liu, Y., "Formation of High-Dimensional Chaotic Maps and Their Uses in Cryptography. Chaos Based Cryptography", Springer Berlin Heidelberg, 2011, pp. 99-136.
[16] Mohammed Saleh, "Proposed Block Cipher Algorithm with Cloud Computing Based on Key Generation", M.Sc. Thesis, University of Technology, 2013.
[17] Maytham M. Hammood, Kenji Yoshigoe and Ali M. Sagheer, "Enhancing Security and Speed of RC4". International Journal of Computing and Network Technology ISSN 2210-1519 Int. J. Com. Net. Teach. 3, No. 2 (May 2015).