Journal of Engineering and Applied Sciences 12 (16): 4118-4122, 2017
ISSN: 1816-949X

CRADG: A Chaotic RADG Security System

[1]Salah Albermany, [1]Maryam Nathim1 and [2]Zahir M. Hussain
[1]Faculty of Mathematics and Computer Science, University of Kufa, Kufa, Iraq
[2]School of Engineering, Edith Cowan University (ECU), Joondalup, Australia

Abstract: A high-performance ciphering algorithm is presented. The proposed method combines old school ciphering (Reaction Automata Direct Graph (RADG)) with chaotic systems to obtain higher level of security. Chaotic sequences are highly sensitive to any changes in their parameters, adding a higher level of security to the proposed approach, called CRADG.

Key words: Chaos, RADG, security, parameters, ciphering, system

INTRODUCTION

Cryptography is an important method to keep personal data secret in order to avoid prohibited access. Lately the internet becomes popular and cipher technology becomes essential to everyone (Marton *et al*., 2012). In recent years there has been significant research efforts to understand chaotic systems and apply their properties towards improving important systems, especially security systems. Chaos properties such as sensitivity to nitial conditions and other chaos generation parameters, similarity of chaotic sequences to random sequences, broadband spectrum, quasirandomness and ergodicity. Chaos has started many research directions in various computer-relatedand information the oretic fields where cryptography became one of the most significant applications. While the classical cryptography isbased on number theory and discrete mathematics the emerging chaos-based cryptography is based on complex dynamics of deterministic nonlinear systems (Kwok and Tang, 2007).

This study presents a novel keyless security scheme which is based on Reaction Automata Direct Graph (RADG) a new trend in security that has recently merged and proved to be efficient. However, one of the weaknesses of this technique is the fixed graph design. The problem discussed in this study is changing the graph from fixed to dynamic using chaotic system, decreasing the decryption time yet adding more security level. It is shown that by using both chaos and RADG technologies better results are obtained with more effective ciphering.

RADG: RADG (Reaction Automata Direct Graph) is a combination of automata direct graph and reaction states, RADG doesn't need key exchange or agreement between users. RADG can be represented by a sextuple as

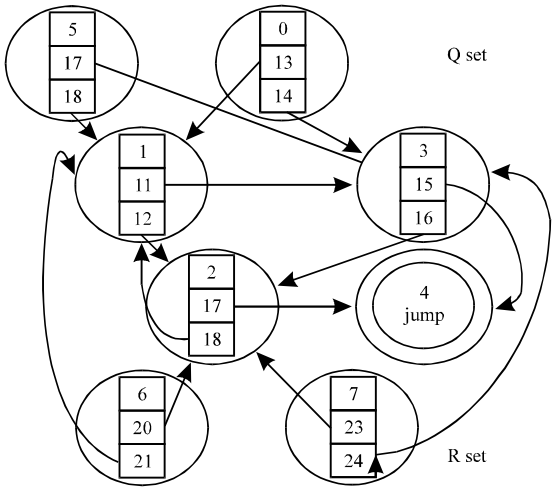

Fig. 1: Transition design

(Q; R; Σ; Ψ; J; T) such that Q stands for a set of standard states, R stands for a set of reaction states, Σ stands for a set of input data, Ψ stands for a set of output transitions, J stands for a set (which is subset of Q called jump states) and T represent transition function. Each state has λ values. RADG ciphering depends on relation between states. On the other hand, the design of RADG depends on m; n; k and λ where n = |Q|; m = |R| and λ representing the number of values in each state. Encryption begins in Q set of states taking each value of the state depending on the transitions and the message whenit gets to a jump state it moves randomly taking values from the R state and going back to the Q set usingthe corresponding transition. The example below helps understanding RADG design (Albermany and Safda, 2014).

Example: If n = 4; k = 1; m = 1 and λ = 2 number of value in each state then the transition design is in Fig. 1.

Corresponding Author: Salah Albermany, Faculty of Mathematics and Computer Science, University of Kufa, Kufa, Iraq

Chaos: Chaos theory is a branch of mathematics that studies and analyzes the behavior of continuous or discrete dynamical systems that are characterized as being highly sensitive to any changes in the systeminitial conditions often referred to as the butterfly effect.

It is worth noting that a very small change in initial conditions (including rounding errorsin digital implementation of chaos systems) can give a highly different output, making these systems very suitable for security applications where the long-termprediction of their behavior would be intimidating for the attacker (Lau and Hussain, 2005).

This complex behavior would be obtained even if these systems are deterministic where their future output values are dependent of the initial conditions (Kellert, 1993). In other words, the deterministic nature of these systems are not predictable (Kellert, 1993; Werndl, 2009).

This kind of behavior is known as deterministic chaos or simply chaos. Edward Lorenz summarized the theory of chaos as follows (Danforth, 2013): "Chaos when the present determines the future but the approximate present does not approximately determinethe future".

Behavior of logistic equation: This map has been presented in 1976 study by the biologist May (1976) as a discrete-time demographic model which is similar in behaviorto the logistic equation proposed by Pierre FranoisVerhulst. The logistic map is given by the following non-linear first-order difference equation:

$$x_{n+1} = rx_n(1-x_n)$$

where the system output represented by the sequence $\{x_n\}$ belongs to the interval (0, 1). Biologically, that represents the ratio of existing population to the maximum possible population. The values of interest for the parameter r are those enclosed inside the interval (0, 4).

Behavior is dependent on r

For the range 0≤r≤1: In this range, we have, f(x) = rx (1-x) = x giving a single fixed point x = 0. Now f(0) = r⇒x = 0 is attracting. It can also be shown that it is globally attracting in the sense that $f(x_0)\Rightarrow 0$ as $n\Rightarrow 1$ for any x_0 is in (0, 1).

Proof:

$|f(x)| < r(|x|) \Rightarrow |f^2(x)| = |f(x)| \times |f(x)|$

Now substituting $|f(x)|$ with $|f(x)| < r(|x|)$:

$\Rightarrow < r(|x|) \times |f(x)| \Rightarrow r^2(|x|)$

$f(x) < r(x) \Rightarrow f^2(x) < r|f(x)| < r^2(|x|)$, ...

$\Rightarrow f^n(x) < r^n(x) \Rightarrow f^n(x) \Rightarrow 0$ as $n \Rightarrow \infty$

When 1<r≤3: In this range, solving f (x) = x will give rise to 2 fixed points as follows:

x = 0 (unstable, repellor) and x = 1-(1/r) (attractor)

$f(x) = rx(1-x) = rx-rx^2$

$f'(x) = r-2rx$

$f'(0) = r>1 \Rightarrow x = 0$ is repelling:

$$\left|f' = \left(1-\frac{1}{r}\right)\right| = \left|r-2r\left(1-\left(\frac{1}{r}\right)\right)\right|$$
$$= |r-2r+2|$$
$$= |-r+2|$$
$$= |2-r| < 1$$

⇒ x = 1-1/r is attracting. In this case, we don't have any periodic points. It can be shown that:

$f(x_0)$ 1-1/r as $n\infty$ for any $x_0 \in (0,1)$

For any $f(x_0) \in (0,1)$

Proof:

$$|f'(x)| = |r-2r| < 1$$
$$= 2r\left|\frac{1}{2}-x\right| < 1 \text{ (common factor)}$$
$$= \left|\frac{1}{2}-x\right| < 1 = 2r$$

dividing both sides (2r):

$$= \left|x-\frac{1}{2}\right| < 1 = 2r$$

reversing because of the absloute sign:

$$= -\frac{1}{2r} < x-1/2 < 1/2r$$

removing the absloute:

$$= \frac{1}{2}-1 = 2r < x < \frac{1}{2r}+\frac{1}{2}$$
$$x \in \left(\frac{1}{2}-\frac{1}{2r},\ 1/2+1/2r\right)$$

And:

$$\therefore 1-1/r\ 2\left(\frac{1}{2}-1-2r,\ 1/2+1/2r\right)$$
$$f(x) = <1 \Rightarrow \left|x-\frac{1}{2}\right| < 1/2r$$
$$\text{For any } x_0 \in \left(\frac{1}{2}-\frac{1}{2r},\ \frac{1}{2}+\frac{1}{2r}\right)$$
$$f^n(x_0) \Rightarrow 1-1/r \text{ as } n \Rightarrow \infty$$

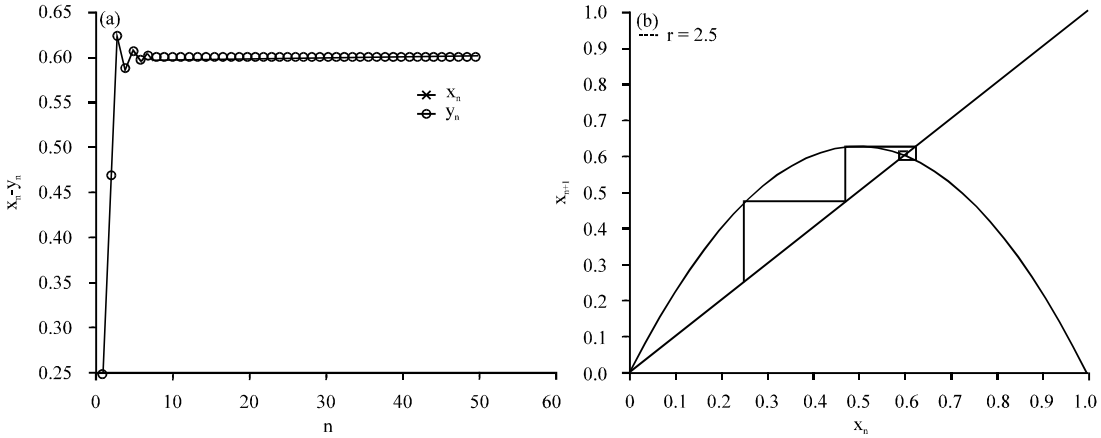

Fig. 2: Preimage of interval; a) logistic map, p = 2.5 and b) Spiderweb for logistic map

It can be shown on MATLAB that all the preimages of this interval are (0.1) (Fig. 2). Such situations can be reached by choosing the parameter r to be in the range (Kwok and Tang, 2007). The attractor is defined as the destination set towards which some initial values converge. Based on this definition, the fixed point is the attractor in the above case.

r>3: When r approaches 3, the convergence of the chaotic sequence to the fixed point:

$$x = (r-1)/r$$

becomes very slow while aperiodic point of period 2 will take place when $3<r<1+\sqrt{6}$ (approximately 3.45). Here both of the fixed points are repelling. However, periodic points will appear. This fact is proved below by solving the equation $f_2(x) = x$ which gives 4 roots:

$$x = 0, 1-\frac{1}{r}, \frac{r+1\pm\sqrt{(r-3)(r+1)}}{2r}$$

The first 2 of these roots represent the repelling fixed points while the other two roots represent two-periodic points. System stability:

$$f_2(x_0) = f(x_1) f(x_0) \text{ where } x_1 = f(x_0)$$

When:

$$x_0 = \frac{r+1\pm\sqrt{(r-3)(r+1)}}{2r}$$

$$g^2(x_0) = 4+2r-r^2$$

Therefore, the 2-cycle is attracting for:

$$|4+2r-r^2|<1; \text{ i.e.,} 3<r<1+\sqrt{6} \approx 3.449\ldots$$

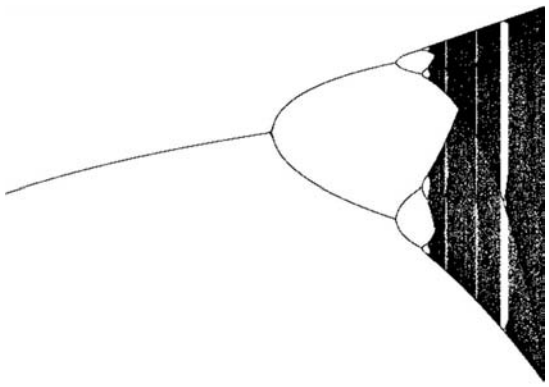

Fig. 3: MATLAB simulation

when it is repelling. It is clear that the sequence will converge to a periodic orbit whose period is 2. According to the above definition, the periodic orbit with period 2 becomes an attractor. Increasing the value of the system parameter r will double the period of the periodic orbit to become 4, 8, 16, ... This change of the orbit structure as a result of the change of the system parameter is called bifurcation, shown below using MATLAB simulation (Fig. 3).

MATERIALS AND METHODS

The proposed CRADG: The proposed method describes the use of RADG and combines it with the logistic function, i.e., instead of using static transitions between states we get the states from the logistic map equation. Although, we can use any one dimensional chaotic equation such as: tentmap, sinusoidal map, elliptical map. Since, each time the equation is executed it gives the value of next stateexcept for the initial seed in the equation which is agreed on by the 2 users (Fig. 4) (Table 1-3).

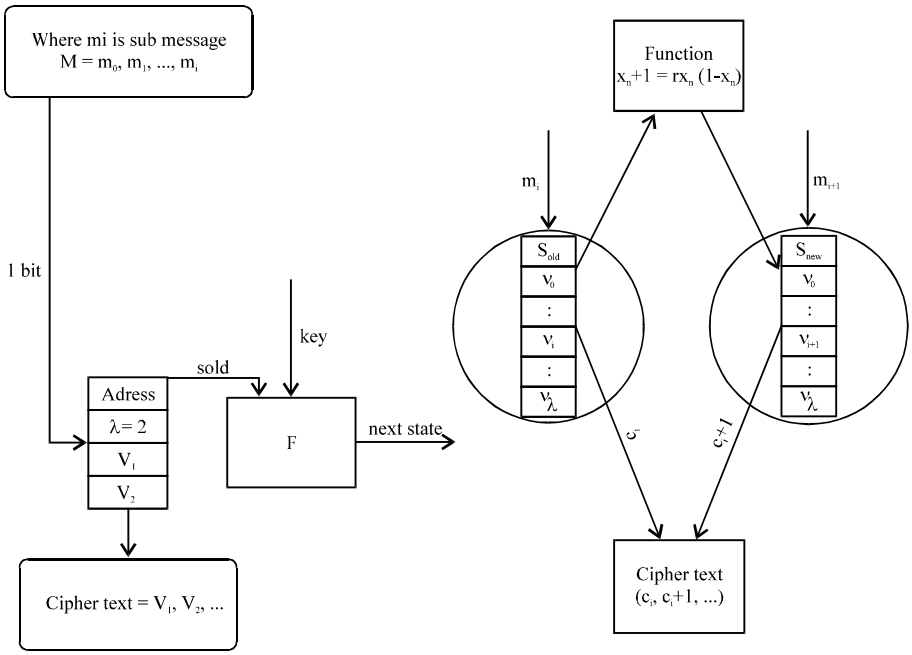

Fig. 4: Flow chart

Table 1: Key for transition

Notation	Notation detail
Key	Key of logistic map
Seed	First number of the sequence
$State_{no}$	Current state number
INQ	State in Q set
INR	State in R set
Index	Index of the while loop
$Message_{length}$	The length of message

Table 2: The cipher

State	Cipher if 0	Cipher if 1
0	2	30
1	25	7
2	16	14
3	22	15
4	10	4
5	Jump	Jump
6	0	3
7	9	1
8	6	24
9	Jump	Jump
10	13	17
11	5	11
12	28	12
13	26	23
14	31	19
15	21	29
16	27	18
17	20	8

Table 3: The incoming bit from the message

Index	Message	$State_{no}$	Status	Values
0	0	1	InQ	25
1	1	3	InQ	15
2	0	8	InQ	6
3	1	4	InQ	4
4	0	11	InR	5
5	0	1	InQ	25

Flowchart

Algorithm

Key for transition:

Step 1. $3.8 \leq key \leq 4$

Step 2. $0 < seed < 1$ and $x(0) = seed$

Encryption:

Step 3. $State_{no} \leftarrow x_{n+1} = rx_n (1-x_n)$

Step 4. Status←INq

Step 5. While (index<$message_{length}$)

Step 6. If $state_{no}$ = jump

Step 7. $State_{no}$random (0, R_{length})

Step 8.

Cipher [index] = R [$state_{no}$] get value [message]

Step 9. Else $state_{no} = x_n$

Step 10.

Cipher [index] = Q [$state_{no}$] get value [message]

Step 11. End if

Step 12. End while

Decryption:

Step 13. $State_{no} \leftarrow x_{message\ length}$

Step 14. While (index_0)

Step 15. If status INQ

Step 16.

decipher [index] = Q [$state_{no}$]: get value [message]

Step 17. else

decipher [index] = R [$state_{no}$]: get value [message]

Step 18. End if

Step 19. End while

RESULTS AND DISCUSSION

Example: Assuming the 2 users agreed on the key = 3.8 and seed = 0.01 (i.e., = x_0) and the message is (010100) given the Cipher table.

Encryption: First we compute the state number using the first number of the chaotic sequence which is 0.01, since the state number is an integer and enclosed between 0and the maximum number (n) in the Q set we multiply the output by n and take the floor of the new value which gives 0 (this ensure that we don't have any number going out of range). We cross reference the state with the incoming bit from the message in the cipher table bit by bit until the message ends, except for the jump state which takes us to another set using random algorithm for choosing the state number).

Decryption: Starting from the last cipher which is 25. Taking the value of then converting into an integer value (same process with encryption) we get the $state_{no} = 1$ then cross reference it with the cipher table we get that 25 came from 0. Repeating all the way until the cipher is finished except for the jump states we have to search in the R_{set}.

CONCLUSION

A new security approach has been proposed based on the classical RADG and chaos theory. The proposed method, called CRADG, out performs the original RADG as follows; the system design is more dynamic including more parameters. The time of decryption is less than the original because we had to search the cipher value in all states every time. Now we don't the state values are generated by the chaotic function. The security is upgraded using the chaotic equation, since any tiny changes in the initial condition will cause dramatic changes in the future.

REFERENCES

Albermany, S.A. and G.A. Safda, 2014. Keyless security in wireless networks. Wirel. Pers. Commun., 79: 1713-1731.

Danforth, C.M., 2013. Chaos in an atmosphere hanging on a wall. MPE, London, England.

Kellert, S.H., 1993. In the Wake of Chaos: Unpredictable Order in Dynamical Systems. University of Chicago Press, Chicago, IL., USA., ISBN-13: 9780226429748, pp: 32.

Kwok, H.S. and W.K.S. Tang, 2007. A fast image encryption system based on chaotic maps with finite precision representation. Chaos Solitons Fract., 32: 1518-1529.

Lau, Y.S. and Z.M. Hussain, 2005. A new approach in choas shift keying for secure communication. Proceedings of the 3rd IEEE International Conference on Information Technology and Applications Vol. 2, July 4-7, 2005, IEEE, Sydney, New South Wales, ISBN:0-7695-2316-1, pp: 630-633.

Marton, K., A. Suciui, C. Sacarea and O. Cret, 2012. Generation and testing of random numbers for cryptographic applications. Proc. Rom. Acad., 13: 368-377.

May, R.M., 1976. Simple mathematical models with very complicated dynamics. Nature, 261: 459-467.

Werndl, C., 2009. What are the new implications of chaos for unpredictability?. Br. J. Philosophy Sci., 60: 195-220.