Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, Tenerife, Spain, December 16-18, 2005 (pp81-86)

Study of a Discrete Iterative Map for Encryption Application in the Internet Part I

Aggarwal A.*, Bakopoulos Y. †, Soulioti V. †, Bardis N. ††, Kouremenos S. †, Nikolopoulos S. †

* Computer Science, University of Windsor, Windsor, Ontario, CANADA
†Division of Applied Technologies, NCSR "DEMOKRITOS", GREECE
†† Naval Academy of Greece, GREECE
akshaia@uwindsor.ca, yannisbakopoulos@yahoo.com, panagiotissouliotis@yahoo.gr, bardis@rgcds.org, stelios.kouremenos@gmail.com, nikiplos@central.ntua.gr

Abstract: A discrete iterative map is utilized for the creation of random number series. It contains discontinuities based on the modulo and signum functions. The binary number series created show almost total randomness, as indicated by block entropy tests. The concept of a virtual cryptographic device is mentioned and analyzed. A new method, based on the above is proposed, for secure and easy application in the Internet and all digital networks in general.

Key-Words: - symbolic dynamics, stream ciphers, pseudorandom, incompressible, encryption, entropy, signum, modulo, security, internet

1 Introduction

The Symbolic Dynamics of both continuous and discontinuous Discrete Dynamic Systems have been studied extensively [5], [6], [11]. Some applications in one and two dimensions have been examined [5-9], [13], [14]. One of the most important applications is the generation of pseudorandom number series for use in encryption of messages in large area networks such as the Internet [1-5], [10], [17-22]. The applications make use of the chaotic pseudorandom behavior such systems may exhibit in their phase space trajectories. [1], [3], [4], [19].

The most common method is to use the symbolic series of the systems' evolution in time. The symbolic dynamics must fulfill certain demands so as to be suitable for the specific application. The created series must appear to be random to a third party and to be almost totally incompressible. It must be reproducible, in the sense that the same initial conditions must always reproduce exactly the same series every time. It must also be easy and fast to create, starting from a relatively small set of real valued parameters. Finally, the set of all different series that can be created by this method should be as large as possible, so that frontal attacks by brute force would be useless [16].

The dynamic systems used are mostly chosen because they show chaotic behavior. The most well known are the standard map, the logistic map, the tent map and some others based on discontinuous functions like the step function or the modulo function [17]. Discontinuous dynamic systems of higher dimension exist in abundance, such as the Sigma – Delta Modulation systems mentioned by many authors [1], [3], [4], [7-9], [13-15], [19].

The authors of this work believe that such systems, suitably modified, can be applied with considerable success to random number generation and stream cipher creation. The system examined here belongs to this class. It is a two dimensional variant of the above mentioned systems. In its simplest form, with zero input and a signum discontinuity, it is described by Eqns. *(I)*

$$(\mathrm{I}): \qquad \chi_{n+1} = A\chi_n + B\cdot S(x_n) + U_n$$

or:

$$\begin{pmatrix} x_1(n+1) \\ \cdot \\ \cdot \\ x_k(n+1) \end{pmatrix} = \begin{pmatrix} a_{11} & \cdot & \cdot & a_{1k} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ a_{k1} & \cdot & \cdot & a_{kk} \end{pmatrix} \cdot \begin{pmatrix} x_1(n) \\ \cdot \\ \cdot \\ x_k(n) \end{pmatrix} + \begin{pmatrix} b_{11} & \cdot & \cdot & b_{1k} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ b_{k1} & \cdot & \cdot & b_{kk} \end{pmatrix} \cdot \begin{pmatrix} \mathrm{sgn}(x_1(n)) \\ \cdot \\ \cdot \\ \mathrm{sgn}(x_k(n)) \end{pmatrix} + \begin{pmatrix} w_1 \\ \cdot \\ \cdot \\ w_n \end{pmatrix}$$

όπου:

$$A = \begin{pmatrix} a_{11} & \cdot & \cdot & a_{1k} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ a_{k1} & \cdot & \cdot & a_{kk} \end{pmatrix}, B = \begin{pmatrix} b_{11} & \cdot & \cdot & b_{1k} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ b_{k1} & \cdot & \cdot & b_{kk} \end{pmatrix}, \chi_n = \begin{pmatrix} x_1(n) \\ \cdot \\ \cdot \\ x_k(n) \end{pmatrix}, \chi_{n+1} = \begin{pmatrix} x_1(n+1) \\ \cdot \\ \cdot \\ x_k(n+1) \end{pmatrix},$$

$$S(\chi_n) = \begin{pmatrix} \mathrm{sgn}(x_1(n)) \\ \cdot \\ \cdot \\ \mathrm{sgn}(x_k(n)) \end{pmatrix}, U_n = \begin{pmatrix} w_1 \\ \cdot \\ \cdot \\ w_k \end{pmatrix},$$

where A, is a rotation matrix in k dimensions, while B may be the identity matrix or any matrix with $|\det(B)| \leq 1$.

The signum function is defined in this work as sign(x) = -1 if x < 0 and sign(x) = 1 otherwise.
A more complicated system is created by the introduction of appropriate input functions. One form of input consists of a perturbation of the rotation matrix in Eqn (I). [3], [4], [19]. To each term a_{ij} of the matrix, a perturbation ε_{ij} is added. For example, if in two dimensions the rotation matrix has terms: $a_{11} = \cos(f) = a_{12}$, $a_{21} = \sin(f) = -a_{12}$, then a perturbation parameter can be added ε to a_{11} and a_{22}, so that $a_{11} = a_{22} = \cos(f) + \varepsilon$, leaving the other terms unchanged.
Eqns (II)

$$\text{(II):} \quad \begin{pmatrix} x_1(n+1) \\ x_2(n+1) \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} x_1(n) \\ x_2(n) \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \cdot \begin{pmatrix} \mathrm{sgn}(x_1(n)) \\ \mathrm{sgn}(x_2(n)) \end{pmatrix} + \begin{pmatrix} w_1(n) \\ w_2(n) \end{pmatrix}$$

A further step is to make use of the modulo function. As the authors of the present study have defined it, the function MOD [x;p] is equal to the value of the real variable x minus the product of p by the integral part of the quotient of the absolute value of x divided by p and by the signum of x:

$$\mathrm{MOD}(x;p) = x - \mathrm{sign}(x)\,(p)\,\mathrm{INT}(|x|/p).$$

Here p is defined to be positive.
Eqns (III)

$$\text{(III):} \quad \begin{pmatrix} x_1(n+1) \\ x_2(n+1) \end{pmatrix} = MOD\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} x_1(n) \\ x_2(n) \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \cdot \begin{pmatrix} \mathrm{sgn}(x_1(n)) \\ \mathrm{sgn}(x_2(n)) \end{pmatrix} + \begin{pmatrix} w_1(n) \\ w_2(n) \end{pmatrix}; p \}$$

or, by coordinates:

(IIIa):

$$x_i(n+1) = \mathrm{MOD}\{a_{i1}\chi_1(n) + a_{i2}\chi_2(n) + b_{i1}\mathrm{sgn}(\chi_1(n)) + b_{i2}\mathrm{sgn}(\chi_2(n)) + w_i(n);\ p\}$$

i = 1,2 (with obvious generalization in higher dimensions).

This is the form that we are studying further and it will be presented as Part II of the paper. It is one of the best fitted for random number generation with application to stream ciphers and Cryptographic Key Creation and Distribution.

2 Study of the Symbolic Dynamics

There are several interesting ways to define a symbolic dynamics based on the class of systems described by Equation (IIIa). The best one, according to the studies by the authors of this work is based on the properties of the signum function, as defined above.

Let the problem be restricted to its two – dimensional form. This may be done without any real loss of generality, since all the relevant concepts can be readily generalized to any dimensions.
The symbols used for the description of the system are four in number and are defined as follows: If $\mathrm{sign}(x_1(n)) = 1$ and $\mathrm{sgn}(x_2(n)) = 1$, then the value of the symbol is defined as s(n) = 0. If $\mathrm{sgn}(x_1(n)) = -1$ and $\mathrm{sgn}(x_2(n)) = 1$, then s(n) = 1. If $\mathrm{sgn}(x_1(n)) = -1$ and $\mathrm{sgn}(x_2(n)) = -1$, then s(n) = 2. Finally, if $\mathrm{sgn}(x_1(n)) = 1$ and $\mathrm{sgn}(x_2(n)) = -1$, then s(n) = 3.
So, for every vector x(n) in configuration space, with coordinates $x_1(n)$ and $x_2(n)$, will correspond a symbol s(n) taking values from the set: {0, 1, 2, 3}.

The symbolic series created depends on the following parameters: The initial values of the coordinates, $x_1(0)$ and $x_2(n)$. The rotation angle f. The perturbation parameter ε. The modulo parameter p. And finally the number of iterations n, defining the length of the symbol string.
In the next section, the symbolic series for systems described by the two – dimensional versions of Equations (I), (II) and (III) will be studied from the point of view of randomness. We are working on another paper, (Study of a Discrete Iterative Map for Encryption Applications in The Internet Part II,.) In that paper, the applications in cryptographic key creation and distribution in the Internet and in digital networks in general will be presented.

3 The map's profile in phase space

The simplest, two dimensional form of the map, is described by a simplified version of Eqn (I):

$$\text{(Ia)} \quad \begin{pmatrix} x_1(n+1) \\ x_2(n+1) \end{pmatrix} = \begin{pmatrix} \cos f & -\sin f \\ \sin f & \cos f \end{pmatrix} \begin{pmatrix} x_1(n) \\ x_2(n) \end{pmatrix} - \begin{pmatrix} \mathrm{sgn}(x_1(n)) \\ \mathrm{sgn}(x_2(n)) \end{pmatrix}$$

A study of the behavior of this map yields an unexpected wealth and variation of trajectories in phase space.
The computer study of the map indicates several interesting facts. In reference to the values of the rotation angle f of Eqn (Ia), it is obvious that there is a region of stability, where the trajectories are bounded within a certain area of the $x_1 - x_2$ plane.

This region is defined by the relation:
$f \in (-\pi/2,\ \pi/2)$.

For values of f within this region, the pictures in the $x_1 - x_2$ plane are either circles or regular convex polygons arranged in symmetric patterns around the origin. The polygons refer to the relation of f to π. If the ratio f/π is a rational number, the trajectories will consist of a cluster of regular polygons. If the ratio f/π is an irrational number, then the polygons will be replaced by circles.

One example of such a trajectory, for the value $f = \pi/6$, is presented in Fig. 1. The initial conditions $x_1(0) = 0.5$ and $x_2(0) = 0.2$ were chosen.

Fig 1.

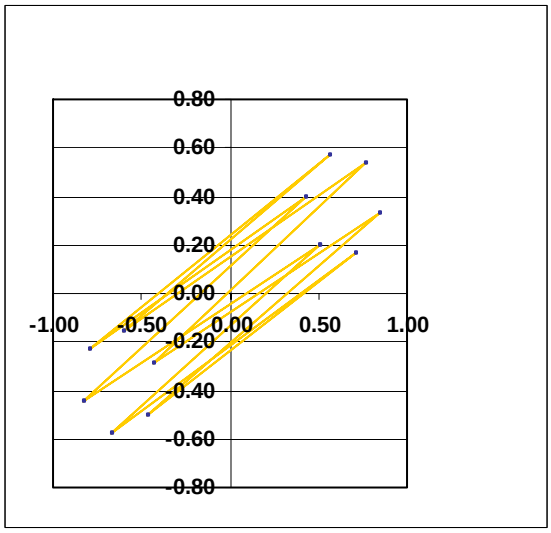


Table 1

Nr	x1	x2		symbol
1.00	0.50	0.20	0.54	0.00
2.00	-0.67	-0.58	0.88	2.00
3.00	0.71	0.17	0.73	0.00
4.00	-0.47	-0.50	0.68	2.00
5.00	0.84	0.33	0.91	0.00
6.00	-0.43	-0.29	0.52	2.00
7.00	0.77	0.53	0.93	0.00
8.00	-0.60	-0.16	0.62	2.00
9.00	0.56	0.57	0.79	0.00
10.00	-0.80	-0.23	0.83	2.00
11.00	0.42	0.40	0.58	0.00
12.00	-0.83	-0.44	0.94	2.00
13.00	0.50	0.20	0.54	0.00
14.00	-0.67	-0.58	0.88	2.00
15.00	0.71	0.17	0.73	0.00
16.00	-0.47	-0.50	0.68	2.00
17.00	0.84	0.33	0.91	0.00
18.00	-0.43	-0.29	0.52	2.00
19.00	0.77	0.53	0.93	0.00
20.00	-0.60	-0.16	0.62	2.00
21.00	0.56	0.57	0.79	0.00
22.00	-0.80	-0.23	0.83	2.00
23.00	0.42	0.40	0.58	0.00
24.00	-0.83	-0.44	0.94	2.00
25.00	0.50	0.20	0.54	0.00

In Table 1, the values of the coordinates of the successive points of the trajectory are given. It is obvious that the trajectory is bounded and periodic. The above given values are repeated every 12 steps, so this trajectory has a period of 12 steps. In Table 1, two cycles, of 24 iterations, are presented to make obvious the periodic repetition of points.
The last column in table 1 describes the symbolic dynamics of the trajectory. In agreement with the definition of symbolic dynamics given above, since the trajectory points lie in the first and the third quadrants, the symbols created by the trajectory are only 0 and 2. The symbolic series has a period of cycle 2.

The centers of the two trajectory polygons are approximately calculated. For the first quadrant, the polygon center coordinates are: $x_1(0) = 0.63,\ x_2(0) = 0.37$. If these values are inserted as initial conditions in the calculation of the trajectory points, the values of the next point coordinates will be: $x_1(1) = -0.63,\ x_2(1) = -0.37$.

The points of the trajectory, for any value of the discrete time n, will alternate regularly between these coordinate values, creating a trajectory of period 2. The symbolic series will be the same as in Table 1. It will also have period 2.

The trajectories defined when the centers of the trajectory polygons or circles are used as initial conditions, are called 'primary' trajectories. Characteristically, their period is the same with the period of the symbolic series.
The trajectory presented in Fig. 1 is not a primary trajectory. Its period is 12 and it includes, not 2, but 12 points. Such trajectories are called 'secondary'. In the example presented above, the trajectory has a period of 12, according to the period of the symbolic series and the angle of rotation $f = \pi/6$. If the ratio f/π is irrational, the trajectory points will lie on two circles, one on each quadrant, instead of polygons. The trajectory will not be periodic, but the symbolic series will be. Such trajectories will be called 'quasi periodic'. The points of the quasi periodic trajectory will be densely distributed on the

circle. This means that for every point of the circle and for every neighborhood of that point of the circle, given enough time, there will be a trajectory point belonging to the neighborhood. This means that, as time goes by, the trajectory points will be found between any two points of the circle, no matter how close they are. In this work, this property will be called 'eventual density'.
The trajectory presented in Fig. 2 is a primary trajectory. The table of coordinates of the points is given below:

Table 2

0,605172	0,788675
-1,60517	-0,21132
0,788675	-0,60517
-0,21132	1,605172
-0,60517	-0,78868
1,605172	0,211325
-0,78868	0,605172
0,211325	-1,60517
0,605172	0,788675

From the coordinate values, the symbolic series is indicated:
0,2,3,1,2,0,1,3. The series period is 8.

As mentioned above, to each quadrant of the phase space corresponds a number from the set: {0,1,2,3}. The first pair of coordinates in Table 2 indicates that the first point belongs to the first quadrant, since both $x_1(0)$ and $x_2(0)$ are positive. Therefore, to this point corresponds the symbol 0. The second pair of coordinates, ($x_1(1)$, $x_2(1)$), are both negative. Therefore, they belong to the third quadrant and the symbol is 2. The series is constructed this way and the trajectory period is equal to the symbolic series period.

Another primary trajectory is shown in Fig. 3

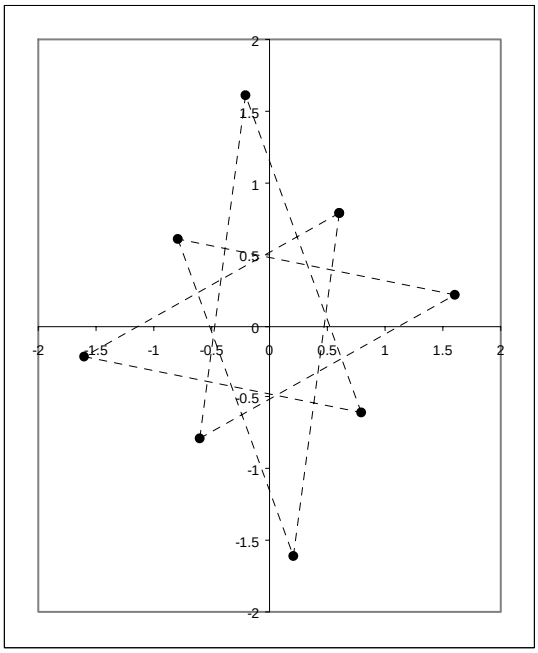
The rotation angle is $f = 9\pi/20$. The initial conditions are $x_1(0)$ = 3.72156122 and x2(0) = 0.292893. The trajectory period is 10, as can be seen from the coordinates table :

Table 3

3,721561	0,292893
-0,70711	2,721561
-1,79867	-1,27266
1,975613	-0,97561
0,272655	2,79867
-3,72156	-0,29289
0,707107	-2,72156
1,79867	1,272655
-1,97561	0,975613
-0,27266	-2,79867
3,721561	0,292893

The symbolic series is: 0,1,2,3,0,2,3,0,1,2, as can be seen from Table 3. The trajectory and symbolic series period is 10.

Fig 2.



f=5π/12
x=0,605172 , y=0,788675

0,605172	0,788675
-1,60517	-0,21132
0,788675	-0,60517
-0,21132	1,605172
-0,60517	-0,78868
1,605172	0,211325
-0,78868	0,605172
0,211325	-1,60517
0,605172	0,788675

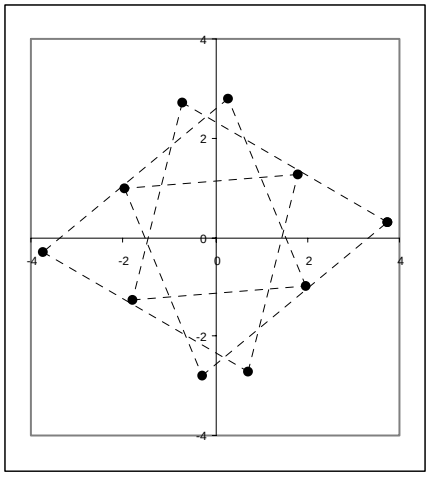


Fig. 3

f=9π/20
$x_1(0)$ =3,72156122 $x_2(0)$ =0,292893
Table 3

3,721561	0,292893
-0,70711	2,721561
-1,79867	-1,27266
1,975613	-0,97561
0,272655	2,79867
-3,72156	-0,29289
0,707107	-2,72156
1,79867	1,272655
-1,97561	0,975613
-0,27266	-2,79867
3,721561	0,292893

4 Conclusion

The virtual encryption machine [3], [4], [19], in the form of a discrete iterative map with discontinuity presented in this work has the properties required for application in random number generation and cryptographic key application in a digital network environment. It provides a high level of security, achieved through the incompressibility and apparent randomness of the created keys, the very large number of keys, which the virtual encryption machine has the ability to produce. The obvious repeatability of the process of key creation make the protocol proposed here especially attractive for Internet applications. The innovative methods of evaluation and verification of apparent randomness [12], increase the level of security and reliability of the protocol against eavesdroppers' attacks. Finally, the concept of adaptation of the protocol to defend in real time against specific forms of attacks [2], although still under study, seems very promising for security and protection against even some conceived forms of attack that are not realistic at the present level of technology but may very well present a real threat in the near future. So it seems that further study and development of the protocol presented here may lead to substantial advances in the technology and methods of communication security.

References:

[1] Yannis Bakopoulos, 'Application of Dynamic Systems for Cryptographic Key Distribution' *15th Congress on Nonlinear Dynamics, Chaos and Complexity* Patras Aug. 19 – 30, 2002 (A. Bountis)

[2] Yannis Bakopoulos, Yannis Vrettaros, Athanasios Drigas, 'An automatic process for the reliable and secure creation and distribution of quantum keys' *National Patent No* ***1003891***, *OBI*, 2002.

[3] Yannis Bakopoulos, Vassiliki Soulioti, 'A protocol for secure communication in digital networks' *National Patent No 1004308 OBI*, 2003;

[4] Yannis Bakopoulos, Vassiliki Soulioti, 'A protocol for secure communication in digital networks' *PCT/GR 03/ 00035* 2003

[5] L. O Chua. and T.Lin, (1988) *IEEE Trans. CAS* **35,** pp. 648 – 658.

[6] Robert L Devaney. *Physica* 10D (1984) pp.387 – 393.

[7] O. Feely and L. O. Chua 'Nonlinear Dynamics of a class of analog - to - digital converters' *Int. J. Bifurcation and Chaos*, Vol. 2**,** 1992, pp. 325 – 340.

[8] Orla Feely "Nonlinear Dynamics and Chaos in Sigma – Delta Modulation".*Journal of the Franklin Institute* Vol. 331B, No. 6, 1995 pp. 903 – 936.

[9] Orla Feely 'Nonlinear Dynamics of Chaotic Double-Loop Sigma Delta Modulation' *ISCAS* 1994: pp.101-104

[10] T Habutsu. et al. 'A secret key cryptosystem by

iterating a chaotic map' *International Conference on the Theory and Application of Cryptographic Techniques,* Springer Verlag, DE pp 127 – 140, XP000607774

[11] Leo P. Kadanov, and Chao Tang, *Proc. Natl. Acad. Sci. USA* Vol. 81, pp. 1276 – 1279, February 1984, Physics.

[12] K. Karamanos "Entropy analysis of substitutive sequences revisited" J. *Phys*. *A, Math. Gen*. **34,** (2001) 9231 – 9241.

[13] Stelios Kotsios and Orla Feely, *NDES Congress Spain* '96.

[14] Stelios Kotsios and Orla Feely 'The model – matching problemfor a special class of discrete systems with discontinuity'*IMA Journal of Mathematical Control & Information* (1998) Vol. 15**,** pp 93 – 104.

[15] Stelios Kotsios 2000 *Nonlinear Dynamics* 22 pp.175 – 191.

[16] George Marsaglia "A Current View of Random Generators" Keynote Address, *Computer Sciense and Statistics: 16th Symposium on the Interface*, Atlanta, 1984 (It appeared in *"The Proceedings"* of the Conference, published by Elsevier Press).

[17] S. Papadimitriou, A. Bezerianos, T. Bountis, G. Pavlides "Secure Communication protocols with discrete nonlinear chaotic maps".*Journal of Systems Architecture*, Vol. 47, No 1, 2001, pp. 61 – 72.

[18] James Rössler et al. *PHYSICAL REVIEW A*, volume 39, number 11, 1989, pp.5954 – 5960.

[19] V. Soulioti 'A study on Discrete Dynamic Systems with a linear part and discontnuity' *15th Congress on Nonlinear Dynamics, Chaos and Complexity* Patras Aug. 19 – 30, 2002 (A. Bountis)

[20]Richard J. Hughes et al 'Method and apparatus for free space quantum key distribution in daylight' *US 2001/055389*, December 27, 2001.

[21] Yuan et al 'Method and system for establishing a cryptographic key agreement using linear protocols', *US 5 966 444,* Oct. 12 1999

[22] Tohru Kohda et al 'Enciphering/Deciphering apparatus and method incorporating random variable and keystream generation' *USPatent 6 014 445* Jan 11, 2002.