Communication networks security: A new method for creating encryption keys

ATHANASIOS S. DRIGAS, YANNIS BAKOPOULOS, YANNIS VRETTAROS
Applied Technologies Department
NCSR "DEMOKRITOS"
Ag. Paraskevi
GREECE
dr@imm.demokritos.gr, john@imm.demokritos.gr, jvr@imm.demokritos.gr
http://imm.demokritos.gr

Abstract: - We have created an innovative method for the production of binary series of arbitrary length, which appear to be random to an uninformed third party. Our method is based on the symbolic dynamics of a special family of recursive maps exhibiting extremely complex trajectories in their phase space. Among other applications, our binary series can be used as encryption keys in protocols based on the Vernam 'one time only' secure communication protocol. Based on fast software implementation, due to the simple form of the defining formulas, such protocols would combine the absolute security of the Vernam protocol with an ease and speed of use that would permit their application in every form of digital communications in the Internet or any other communication network, including wireless and mobile telephony.

Key-Words: - Encryption, recursive maps, sign function, modulo function, perturbation parameter, binary series, "one time only", security, communication protocols.

1 Introduction

The issue of encryption is today the most important problem for communication security [1-4],[10],[17],[19-22],[31-32]. The reasons are simple. Today's trend is to expand, globalize and unify digital network communication and sharing of resources and services. This expansion and future globalization is expected to be achieved on a substantially advanced technology anticipated in the near future, including, among others, 128-bit processors, terabit storage capacities, all optical circuits and, above all, quantum computers. Furthermore, there is the expressed desire and strategic target of the Information Society decision makers all over the world to convert cable and fiber communication networks into wireless ones. Without proper security measures the Internet and all wide area communication networks would be turned into a hackers' paradise.

The encryption protocols and techniques commercially available today can barely hold the burden of secure communications as it stands on the present state of the art. The main problem is that, given enough computing power, all encryption methods available today are vulnerable to eavesdropper attacks, at least in theory. The only exception is the well known Vernam 'one time key' protocol. But even in its modern form, Quantum Key Distribution, this method, though theoretically safe, is so cumbersome and expensive, both in money and in time and network resources, as to be almost impossible to apply in a large area digital communications and information exchange networks, such as the Internet [1-4],[19],[31-32].

We have a method to generate 'apparently random' binary number series of arbitrary length, to be used as encryption keys in a Vernam type, "one time only use", encryption protocol. The implementation of the key is the same as in all 'one time key' applications. The key is added bit by bit, by a XOR operation, to the unencrypted binary file containing the message. The receiver of the message applies the same XOR operation to decrypt it.

Our keys will be created by the use of a family of discontinuous discrete dynamic systems and their symbolic dynamics. They should best be described by the following Equations [1-4],[19],[32], also see [5-9],[11],[13-15],[18],[23-30]:

(I): $\vec{x}(n+1) = A\vec{x}(n) + B\left(S(\vec{x}(n))\right) + \vec{U}(n)$

where $\vec{x}(n)$, $\vec{x}(n+1)$ are successive position vectors in the system's phase space, A, B suitable matrices with the absolute value of their determinant larger than or equal to 1, $\vec{U}(n)$ an arbitrary input vector and $\left(S(\vec{x}(n))\right)$ the sign vector to be explained below. In this presentation, the work will be restricted to two dimensions:

(II): $$\begin{pmatrix} x_1(n+1) \\ x_2(n+1) \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_1(n) \\ x_2(n) \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \begin{pmatrix} \mathrm{sgn}(x_1(n)) \\ sign(x_2(n)) \end{pmatrix} + \begin{pmatrix} U_1(n) \\ U_2(n) \end{pmatrix}$$

The function sgn(x) has value -1 if x < 0 and 1 otherwise. Therefore, $\left(S(\vec{x}(n))\right)$ is a vector with the sign functions of the position vector's coordinates as its coordinates.

There have been considered many methods to create binary symbolic series from the above Equations, to be used as encryption keys. These series obviously are not really random, since they are created by a well understood and repeatable mathematical recursive method. Yet they should appear as 'random' series of binary digits to a third party. The apparent 'randomness', or, in other words, the lack of any apparent structure in the series should be theoretically proven by topological arguments and ascertained by appropriate statistical tests available in the Internet there are many suits of tests, some of them considered the most well known and commercially acceptable. The NIST tests and those published by prof. George Marsaglia [16] are included. The best methods examined so far yield test results which are 80-90% successful. The method is still at the calibration stage and hopefully better results will appear soon.

Due to the above described property, the usual problems of key distribution would not exist here. No need for repeated meetings of trusted parties for distribution of new key pads. The small number of parameters necessary for the generation of each key may be included in the previous message. This way the integrity of communication would be preserved. Only one initial contact will be required, in order to distribute the exact form of the dynamic system and a first set of parameters.

Our method will generate a theoretically arbitrary length of key series, starting from a small number of initial parameters each time. The defining equations, due to the discontinuous 'step' and 'modulo' functions they include, are especially sensitive to initial conditions. As a result, the space of different keys is extremely large. If the dynamic system is defined by a ten dimensional vector equation, then the number of different keys may be of the order of 10^2000. As appropriate tests have proven, there is no cross correlation between the keys.

Due to the above properties, the method would be suitable for many Internet applications, including e-mail encryption and possibly wireless and mobile phone applications. If the above arguments hold, the method will be secure even against attacks applying massive parallel processing, by the use of quantum algorithms. This is because of the randomness and the extremely large key space.

An added advantage is that our method of secure communication may combine, for distributing the protocol and procedure information and thus initiating the communication process, an established QKD setup [1-4],[19],[31],[32] chosen from those available commercially today. So a practical and feasible application for such protocols will be offered since the QKD protocol should be used just once, at the beginning of communications, to safely initiate first contact. From then on, our method will be applied as described without help from QKD. Any other safe method for the initiation of communications, such as personal contact or trusted messengers, is equally acceptable.

In the following, a specific example of our method will be presented. It will be based on a simple map containing a linear part and a sign vector singularity, modulated by a MOD function, so as to remain bounded and not escape to infinity. In Section 2, the properties of the initial system, containing a rotation matrix and the sgn(x) singular function, will be given. In Section 3, the system will be studied after an essential modification. A perturbation coefficient will be added to the rotation matrix and a MOD function. In Section 4, the theoretical and experimental arguments for the usefulness of the map as a random number generator and an encryption system will be presented. In Section 5, the results will be discussed and some final conclusions will be drawn.

2 Study of the Initial Map

In its simplest form, the recursive map has the form given below.

(III): $$\begin{pmatrix} x_1(n+1) \\ x_2(n+1) \end{pmatrix} = \begin{pmatrix} \cos(\phi) & -\sin(\phi) \\ \sin(\phi) & \cos(\phi) \end{pmatrix} \begin{pmatrix} x_1(n) \\ x_2(n) \end{pmatrix} - \begin{pmatrix} \mathrm{sgn}(x_1(n)) \\ sign(x_2(n)) \end{pmatrix}$$

Here the linear part of the map is a rotation by a constant angle ϕ, while the vector $\begin{pmatrix} \mathrm{sgn}(x_1(n)) \\ sign(x_2(n)) \end{pmatrix}$ is the sign vector $\left(S(\overset{\mathrm{r}}{x}(n))\right)$ described above. By computer study it becomes obvious that the behavior of the map depends mainly on the angle of rotation ϕ. For values of ϕ from the interval: $(-\pi,\pi)$, the map exhibits a stable behavior for $\phi \in (-\pi/2, \pi/2)$. For values of ϕ outside this interval, the map goes on to infinity. The fastest rate of divergence is for $\phi = \pi$.

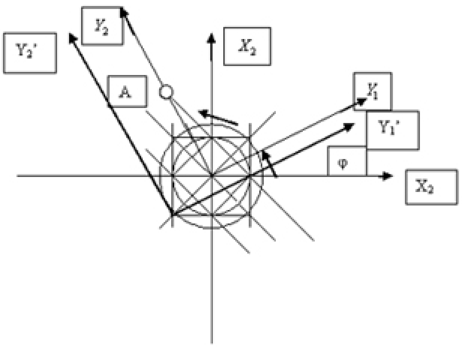

Figure 1. Image of the coordinate system under the Eq.I map

In Fig. 1 a rotation of the coordinate system by the angle ϕ is shown. The axes rotate from position X_1-X_2 to position Y1-Y2. If the angle of rotation ϕ is less than $(-\pi/4, \pi/4)$, then the trajectories of the map are all bounded. In Fig. 1, the distance of the point A from the origin indicates the maximum distance of a trajectory point in this case. If $|\phi| \in (\pi/4, \pi/2)$, the map's trajectories may go on to arbitrarily large but always finite size, depending on the initial conditions $\begin{pmatrix} x_1(0) \\ x_2(0) \end{pmatrix}$.

There are some very characteristic features in Fig. 1 First of all, there is a fundamental square with apices $\begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} -1 \\ 1 \end{pmatrix} \begin{pmatrix} -1 \\ -1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$. There are four diagonal lines, with a 450 degree inclination, creating a small diamond-oriented square of side $\sqrt{2}$, intersecting the largest square with a side of size 2 at points: $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} -1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ -1 \end{pmatrix}$. The rotation by the angle ϕ is indicated by two arrows pointing anticlockwise from axes X1, X2, to Y1, Y2. Then the application of the sign vector will image the 0 quadrant of a circle having the origin as center onto a quadrant of an equal circle, with its center at point $\begin{pmatrix} -1 \\ -1 \end{pmatrix}$ and radius 2 (not shown). The image will be rotated anticlockwise by the angle ϕ. If the radius of the circle is equal to the distance of the origin to the point A, then the image of A would be equidistant to A from the origin. So, the circle mentioned above is an attractor of all trajectories for the specific angle ϕ. A formal proof of this fact is given in detail elsewhere [32]. In contrast, if a smaller circle, with the origin as center and a radius equal to $\sqrt{2}\big/_2$ is considered (not shown), it is obvious that its image, with $\begin{pmatrix} -1 \\ -1 \end{pmatrix}$ as center, or, for that matter, with any of the apices of the larger square as center, will not intersect with it except at one point of contact. This means that the image of any point within this smaller circle is further from the origin than the initial point. So the smaller circle is in fact a repeller for any angle ϕ.

The conclusion is that any trajectory, no matter what the initial conditions are, is contained within a specific annular region, with outer boundary the circle of radius from the origin to A and inner boundary the circle of radius $\sqrt{2}\big/_2$. This observation is the starting point to an argument, presented elsewhere [Bakopoulos, Soulioti to be published], by which for every angle ϕ in the interval $\left(-\pi/4, \pi/4\right)$ there are trajectories of completely non-periodic behavior, which are uncountably infinite in quantity. The fact that this map and its modifications are suitable for pseudorandom number generation has the above argument as its starting point, as will be discussed in Section 5.

The trajectories usually consist of a number of circles, distributed in various ways among the four quadrants. In exception, if the initial point is on the center of one of the circles, the corresponding trajectory consists only of the centers of all the circles. On the other hand, if there is a distance between the initial point and the center of the corresponding circle at the same quadrant, the trajectory consists of points belonging to the corresponding circles, of equal radii with the distance of the initial point from its center.

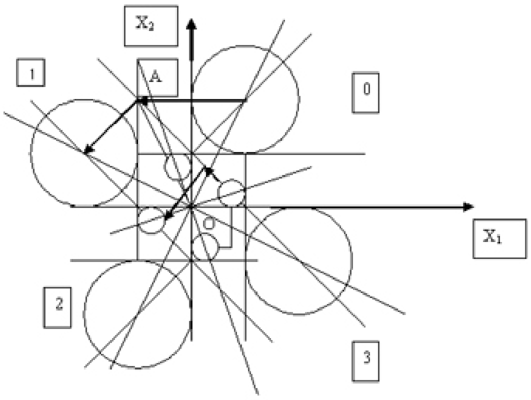

Figure 2. Fundamental trajectories of the basic system

In general, each trajectory is characterized by its passing through a series of quadrants. The numbers 0, 1, 2, 3, characterize the quadrants of the plane. As the quadrants are visited in succession by the map points, their designated numbers comprise the symbolic series of the map (Fig. 2).

If the points of the map are identical to the centers of the corresponding trajectory circle, then the trajectory is periodic with its period equal to that of the corresponding symbolic series. Such a trajectory is called 'primary'. If the symbolic series is periodic but the points of the map do not coincide with the centers of the trajectory circles, then the trajectory is called 'secondary'. In that case, if the ratio π/ϕ is rational, the secondary trajectory consists of the apices of suitable regular polygons inscribed to the circles of the trajectory. Then the secondary trajectory is periodic and its period is equal to the period of the symbolic series, multiplied by the ratio $2\lambda\pi/\phi$, λ being a suitable positive integer. If the ratio is irrational, the points of the map continue to cover the circles' perimeters 'almost everywhere', except for a countable set of points. This is called a quasi- periodic trajectory [1],[3-4],[19],[32].

In Fig. 2, some fundamental trajectories are indicated. If the four quadrants of the Euclidean plane are indicated as in Fig. 2, by the numbers 0, 1, 2, 3, then a trajectory is described by the four largest outer circles. Such a trajectory is indicated as 0-1-2-3….At each step of the recursive map, the vector indicating the state of the system follows the above given order as it changes from one quadrant to another. The relative position of the map point to the center of its circle remains constant. If the initial point is one of the centers of the four circles, then the trajectory consists of the four centers only. In that case it is called a primary trajectory and it is periodic for every value of ϕ from the interval $(-\pi/2, \pi/2)$. If the initial point is at a distance from the corresponding center in the same quadrant, then the distance remains constant for the whole trajectory. The relative orientation of the straight line joining the center of a circle with the corresponding trajectory point changes anticlockwise by ϕ at every step. This way, when a point arrives at quadrant 0,its new position on the trajectory circle of this quadrant is moved by 4ϕ anticlockwise.

In Fig. 2, two more trajectories are indicated. One of them is characterized by the numbers 0-2 and is indicated by the two smaller circles in the corresponding quadrants. The other is characterized as 1-3 and is indicated by the two other small circles.

In Fig. 3 the circles indicating the three various trajectories, 0-1-2-3, 0-2, 1-3, can be seen. These are the maximum size circles that may support these trajectories. Their centers define the primary trajectories with period the same as the period of their symbolic series. The secondary trajectories lie on circles of equal radii, with size varying from zero to the maximum size shown in Figs 2 and 3.

If the above mentioned ratio π/ϕ is an irrational number, the trajectory has at most the size of the maximum circle, as in Fig. 3. Then this circle is called 'the area of influence' of the trajectory for the specific symbol in the symbolic series. If the ratio π/ϕ is rational, then the area of influence is an appropriate regular convex polygon. The polygon's order depends on the angle of rotation and the form of the symbolic series. Typically, for the 0-1-2-3 trajectory and for a rotation angle $\phi = \pi/6$ the corresponding shape is a hexagon, while for the same trajectory and $\phi = \pi/4$ the respective polygon is an octagon. On the other hand for a period 2 trajectory like the 0-2 or the 1-3, the maximum polygon for $\phi = \pi/6$ is a dodecagon, a polygon of 12 sides.
Another definition for the area of influence is that it is the maximum object that may follow a trajectory with a given symbolic series.

A description of the properties of the basic map is given elsewhere [1],[3-4],[19],[32]. The properties of recursive maps including similar discontinuities has been studied extensively in the relative literature.

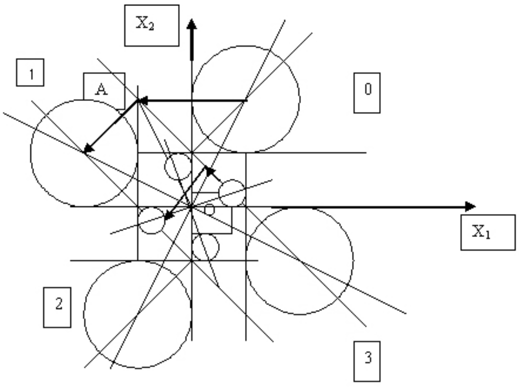

Figure 3. The mechanism of application of the basic map

The 0-1-2-3, 0-2 and 1-3 trajectories presented above exist for every value of $\phi \in (-\pi/2, \pi/2)$. The 0-1-2-3 trajectory is symmetric to 90^0 degree rotations and inversions with the axes of symmetry inclined by $\phi/2$ clockwise, relative to the coordinate system of the plane. The 0-2 and 1-3 are symmetric as a family, in the sense that a 90^0 degree rotation of one trajectory will bring it onto the other. The axes of symmetry are inclined by $\phi/2$ anticlockwise relative to the coordinate axes. This is not true for other trajectories, which may, or may not, exist for all values of ϕ. There are certain empirical rules which seem to be obeyed by most trajectories: (a) There are no repetitions of a symbol of a quadrant within a symbolic series period. This rules seems to be broken only in special cases of trajectories with an area of influence restricted to a point or a line segment on an axis. Such degenerate trajectories exist for example for $\phi = \pi/4$ and are of the form: 2-0-0-2-3-1-3-1 or: 0-2-0-2-3-1-1-3. These are restricted on an area of influence in the form of a straight line segment. (b) There may not be reversals of direction. For ϕ positive, such reversals as 1-0 or 3-2 have not been observed. A 0 must be followed by 1 or a 2. The reverse is true for negative angle of rotation. No exceptions to this rule have been observed within a periodic symbolic series.

For best understanding of the issue of periodic and non periodic symbolic series and trajectories, the concept of pre orbit points must be examined. By pre orbit points we define those points that appear during the initial steps of a recursive map before its symbolic series enters its proper period. The pre orbit points are by definition of finite number, and are characterized by the fact that they are isolated. There is always a circle around each of them within which no other point of the same trajectory exists. These properties distinguish a set of pre orbit points, no matter how large in size, from a non periodic trajectory. In the latter case, the number of points is infinite and they are not separable. Any number of other points may be found within a circle around a specific point of a non periodic trajectory, however small.

Examples of such non periodic trajectories are the trajectories found for specific initial conditions for values of ϕ equal to $\pi/6$ and $4\pi/9$ (see Figs in [32]).

3. The Extended Map

From the study of the initial map some conclusions may be drawn. First of all, although there is a very large complexity in the form and variety of the map's trajectories, there is also a large amount of order, contrary to the requirement of 'apparent randomness'. Even in the non periodic trajectories, whenever they occur, there are certain restrictive rules and symmetries. The three rules of the periodic symbolic series are not so rigid for the non periodic ones but still repetitions of the symbols are rare and reversals such as mentioned in the previous sector even rarer. This would prevent the use of the system as it is for 'apparently random' number generation.

A slight modification created the potential for further study of the structure and better understanding of the system. The introduction of a perturbation parameter ε in the rotation matrix, as described by Eq.IV, changed the behavior of the map to the point of making 'almost all' trajectories non periodic and most of them unstable [1-4],[19],[32], [Bakopoulos, Soulioti to be published].

For small values of the perturbation parameter, of the order of $\varepsilon = 10^{-3}$ or less, the trajectories appear to 'jump', from one stable trajectory of the previous system (Eq. III), to the other, in an apparently random manner, ultimately depending on the moment in discrete time when the trajectory will pass from one area of influence to another by crossing into a quadrant not corresponding to the previous trajectory. This will inevitably happen since the determinant of the matrix in Eq. IV is now larger than one, so that the distance of the trajectory point from the center of each area of influence cannot remain constant. Periodic trajectories are of measure zero due to the high instability of the system. In fact, although predictable by the Equation defining the system [32], they are not apparent by computer experimentation. Instead in Figures of [32], all trajectories and symbolic series appear non periodic, a fact that presents hope for random number generation.

(IV): $$\begin{pmatrix} x_1(n+1) \\ x_2(n+1) \end{pmatrix} = \begin{pmatrix} \cos(\phi)(1+\varepsilon) & -\sin(\phi) \\ \sin(\phi) & \cos(\phi)(1+\varepsilon) \end{pmatrix} \begin{pmatrix} x_1(n) \\ x_2(n) \end{pmatrix} - \begin{pmatrix} \operatorname{sgn}(x_1(n)) \\ sign(x_2(n)) \end{pmatrix}$$

Still, for such small values of the perturbation parameter, the symbolic series maintain enough structure and similarity to the initial system to remain unsuitable for the required applications. If larger values of ε. Such as $\varepsilon = 0.1$, or larger, were used, the system became unstable and went to infinity. To remedy this situation, a MOD function was introduced (Eq.V).

(V):
$$\begin{pmatrix} x_1(n+1) \\ x_2(n+1) \end{pmatrix} = MOD\{\begin{pmatrix} \cos(\phi)(1+\varepsilon) & -\sin(\phi) \\ \sin(\phi) & \cos(\phi)(1+\varepsilon) \end{pmatrix} \begin{pmatrix} x_1(n) \\ x_2(n) \end{pmatrix} - \begin{pmatrix} \operatorname{sgn}(x_1(n)) \\ sign(x_2(n)) \end{pmatrix}; p\}$$

In (V), p is a positive real number and ε takes large values, typically much larger than 1. The MOD function essentially ‘folds’ the plane inside a square of side $2p$ with the origin as its center.

4. Applications of the Map In Encryption

The map of Eq.V has the potential for the production of random numbers of such ‘apparent randomness’ that they may be applied to encryption schemes as explained in the Introduction. This is due to theoretical reasoning as well as computer study and appropriate statistical tests.

There are many ways to create a series of numbers from (V). The simplest way is to use the symbolic series of non periodic trajectories. It must be converted into binary form and, depending on the manner of the conversion, it will pass the commercial statistical tests available in the Internet to a rate of about 60%. Improved methods include special functions and modifications such as taking the nth decimal point of a coordinate value and put it in MOD(2) form. Since the modulo class of 2 has only two members. 0 and 1, the result is a binary series. These series have been tested by the available tests, with success approaching 100%.

The theory predicts such behavior, since the maps defined by Eq.III,IV,V contain the sign function, the perturbation parameter and the appropriate MOD functions. The sign function introduces a large complexity due to its unpredictable ‘jumping’ from one quadrant to another. This is supported by the theoretical proof of the existence of an uncountably infinite number of non periodic series [Bakopoulos, Soulioti to be published]. The perturbation parameter reveals this complexity and finally the MOD function keeps it in a manageable form.

Besides the theoretical arguments, our method was tested by the tests of the NIST Institute, the tests provided on line by Prof. G. Marsaglia [16] and by some innovative method created by Dr K. Karamanos [12], at the Free University of Brussels. In a test where the key was created by taking the MOD(2) of the tenth decimal point of the first coordinate of the map points, the success reached practically 100%, on a sample of some 200 keys of 1000000 bits length. Transinformation and intercorrelation test also indicate a very large sensitivity to initial conditions, up to the 20th decimal point.

The other requirements for a binary encryption key are that the series are repeatable, fast and easy to construct and the key space must be large, so as to preclude brute force attacks. This is achieved because of the extreme sensitivity of the system even to the smallest variations of the parameter values. There are many ways to create a key from a map of the general form given by Eq.I. One way to increase the complexity is to increase the dimensions of the map from 2 to something larger. It is the authors’ opinion that the use of even a 10 dimensional state space would not make the application to heavy for on line use. In this extreme case, assuming a normal 32 bit processor, a network of Java enabled computer systems would be able to handle calculations with 10 - 20 decimals and communicate without delay problem. In that case, a system like the one described by Eq.I, with two 10x10 matrices and a ten dimensional initial conditions vector would depend on more than two hundred parameters. If each parameter has a sensitivity of 10^{-10} to 10^{-20} decimals and for 100 parameters the variations are $(10^{-10})^{-200}$ in multitude, the key space would contain 10^{2000} keys, enough to withstand a brute force attack even from a quantum computer. For less sensitive content, the dimension of the application may be less, depending on the security demands. These are the arguments on which the use of the method for encryption applications is based.

Although the authors are convinced of the suitability of their method for applications, there are still open questions and details to be clarified. Even if the increasing of dimensions seems to be the best method for strengthening security, other possibilities, such as the increase of the decimals or the introduction of more discontinuous functions are possible and will be the subject of further research.

5. Conclusions

In the previous sectors, a recursive map has been presented and studied in various forms, described by Eq.I-V with increasing complexity. The existence of non periodic trajectories in the map's state space, the unpredictability introduced by the discontinuous functions sign and modulo, as well as the perturbation induced by the parameter ε, make possible the creation of series of 'apparently random' binary digits, suitable for use in demanding applications such as encryption. The properties of the ensuing encryption methods and protocols have the required properties in terms of security, repeatability, ease and speed of use and a large enough key space to face and withstand brute force attacks even by a quantum computer. Although it may be concluded that there exist strong arguments for the suitability of the system for the highest level security communications, there is ground for further study and development to improve the method, This may be the direction of future research.

6. 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) (In Greek).

[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 problem for 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 (and refs therein)

[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, JUNE 1 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). (In Greek).

[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' *US Patent 6 014 445* Jan 11, 2002.

[23] L. O. Chua and T. Lin, 'Chaos in digital filters', IEEE Trans. Circuits and Systems, Vol 35, pp. 648-658 (1988).

[24] L.O. Chua and T. Lin, 'Fractal pattern of second order non-linear digital filters: A new symbolic analysis', International Journal of Circuit theory and Applications, Vol. 18, pp. 541-550, (1990).

[25] L.O. Chua and T. Lin, 'Chaos and fractals from 3rd order digital filters', International Journal of Circuit theory and Applications, Vol. 18, pp. 241-255, (1990).

[26] Zbigniew Galias and Maciej J. Orgozalec, 'On symbolic dynamics of a chaotic second-order digital filter', International Journal of Circuit theory and Applications, Vol. 31, pp. 401-409, (1992).

[27] Zbigniew Galias and Maciej J. Orgozalec, 'Bifurcation phenomena in second-order digital filter with saturation-type adder overflow characteristics', IEEE Transactions on Circuits and Systems, Vol. 37, No 8, pp.1068-1070, (1990)

[28] Chai Wah Wu and Leon o. Chua, 'Symbolic dynamics of piecewise-linear maps' IEEE Transactions on Circuits and Systems-II: Analog and Digital Signal Processing,, Vol. 41, No 6, (1994).

[29] Chai Wah Wu and Leon o. Chua. 'Properties of admissible symbolic sequences in a second order digital filter with overflow non-linearity', International Journal of Circuit theory and Applications, Vol. 21, pp. 299-307, (1993).

[30] Nikolaos Papadakos, *Quantum Information Theory and Applications to Quantum Cryptography*, arXive: quant – ph/ 0201057 v1 (2002)\

[31] V. Soulioti, Y. Bakopoulos, S Kouremenos, Y. Vrettaros, S. Nikolopoulos, A.S.Drigas. Stream Ciphers created by a Discrete Dynamic System for application in the Internet. *Proceedings of 8th* WSEAS Int. Conf. on COMMUNICATIONS, July 12-15, 2004, Vouliagmeni, *Athens, Greece.*