Random Number and Encryption Key Generation by the use of Discontinuous Discrete Maps and their Symbolic Dynamics

BAKOPOULOS Y. [1], SOULIOTI V. [1,4], KOUREMENOS [1], NIKOLOPOULOS S. [5], ECONOMOU C.[3] and AGGARWAL A.[2]

[1] Division of Applied Technologies, NCSR "DEMOKRITOS"
[2] High performance and Grid Computing Research Group School of Computer Science, University of Windsor.
[3] Department of Computer Science, IST Studies
[4] C.R.A.N.S., Mathematics Dept., Univ. of Patras
[5] Hellenic Ministry of Public Order

Abstract: - A new method of creating random number series to be used as encryption keys is presented. It is based on the symbolic dynamics of a class of discontinuous discrete maps. The ensuing keys have been successfully tested by the application of the basic established commercial tests and are deemed suitable for use in encryption in large scale networks such as the Internet, in a 'one time pad' type of communication protocol.

Key words:- Random numbers, encryption keys, discontinuous maps, symbolic dynamics, Vernam Ciphers, one time pad, virtual encryption devices.

1 INTRODUCTION

Security on the Internet is a big issue of today [1–30], in the days of prospective wireless communications, business transactions, e-learning, e-government, e-health. The problem of encryption has always been a major issue in large area communication networks, as protection against illegitimate intruders, eavesdroppers and hackers. In today's Internet environment, with its wireless services, large scale economic transactions and all kinds of sensitive information transfer, it has become the heart of information security. As such, it has attracted the attention of many researchers from various branches of mathematics and physics [1-4], [5], [10], [16], [17], [19-22], [30].

The method with the widest use is that of private and public keys, following standards like DES, AES, RC4, RSA as much as some modifications of symmetric cryptography [31]. These systems are based on the difficulty and complexity of calculations involved in breaking the code and so provide conditional security. They are breakable, given enough time and computing power to the adversary cryptanalysts. The same holds for all kinds of block cipher type keys. Generally there is no mathematical proof of absolute security for any encryption protocol besides the well known Vernam, or 'one time pad', protocol or others modern encryption protocols for remote user authentication in Integrated Systems [33].

The application of Quantum Key Distribution methods and protocols is a new arrival to the networks of today [2], [20], [30] (and references therein). It is based on the random processes of quantum phenomena and is the most advanced version of Vernam keys today.

Even in this modern form, QKD protocols, the 'one time pad' method is hardly suitable for a large area digital network environment, such as the Internet. The extremely large numbers of users, the complexity of connection topologies and the variety of services, platforms and applications requires a flexible and adaptable method of routine communications in order to be reliable and easy for the majority of clients. All QKD protocols require high technology, both expensive and unwieldy for the average user.

In this work, the authors propose a method of secure and easy communication similar in appearance and advantages to the old Vernam 'one time key' protocol but without the inherent problems of the old method. It is based on the generation of apparently 'random' binary keys, in the form of symbolic series of a discontinuous discrete recursive map [1], [3], [4], [19], [21].

The structure of this manuscript is as follows: In Section 2, the theoretical study of our map is presented. Then, in Section 3, the practical application of the method is given and finally Section 4 culminates with discussion and pointers for further work.

2 DESCRIPTION OF THE MAP

The authors have studied a family of discontinuous maps, initially defined in two dimensions by the equations presented below (see [1], [3], [4], [14], [15], [19]):

$$\vec{x}(n+1) = A\vec{x}(n) + B\vec{S}(n) + \vec{U}(n) \qquad (1)$$

defined in a phase space of arbitrary dimension *k*. Especially in two dimensions the equations are:

$$\begin{pmatrix} x_1(n+1) \\ x_2(n+1) \end{pmatrix} = \\ = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{21} \end{pmatrix} \cdot \begin{pmatrix} x_1(n) \\ x_2(n) \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \cdot \begin{pmatrix} \mathrm{sgn}(x_1(n)) \\ \mathrm{sgn}(x_2(n)) \end{pmatrix} + \begin{pmatrix} w_1(n) \\ w_2(n) \end{pmatrix} \qquad (2)$$

where:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \qquad (3)$$

$$B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \qquad (4)$$

$$\vec{x}(n) = \begin{pmatrix} x_1(n) \\ x_2(n) \end{pmatrix} \text{ and } \vec{x}(n+1) = \begin{pmatrix} x_1(n+1) \\ x_2(n+1) \end{pmatrix} \qquad (5)$$

$$\vec{S}(\vec{x}(n)) = \begin{pmatrix} \mathrm{sgn}(x_1(n)) \\ \mathrm{sgn}(x_2(n)) \end{pmatrix} \qquad (6)$$

where the function $sgn(x)$ is defined as follows:

$$\mathrm{sgn}(x) = \begin{cases} -1, & x < 0 \\ 1, & 0 \le x \end{cases} \qquad (7)$$

The matrices A and B have the properties: $\det(A), \det(B) > 1$ and they have no real eigenvalues.

As a particular case, the matrices $A = \begin{pmatrix} \cos(\phi) & -\sin(\phi) \\ \sin(\phi) & \cos(\phi) \end{pmatrix}$, $B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ have been studied among others. In that case, the map's trajectories in phase space are mostly periodic, although very complex non-periodic trajectories have been predicted theoretically and in some cases demonstrated by computer experiments [1], [3-4], [19].

In this work, in order to make det(A) significantly larger than one and therefore increase the map complexity, a modulo function has been added to the initial equations. The equations (1) and (2) then take the form:

$$\vec{x}(n+1) = MOD\{A\vec{x}(n) + B\vec{S}(n) + \vec{U}(n); p\} \qquad (8)$$

$$\begin{pmatrix} x_1(n+1) \\ x_2(n+1) \end{pmatrix} = \\ = \mathrm{MOD}\left\{ \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{21} \end{pmatrix} \begin{pmatrix} x_1(n) \\ x_2(n) \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \begin{pmatrix} \mathrm{sgn}(x_1(n)) \\ \mathrm{sgn}(x_2(n)) \end{pmatrix} + \begin{pmatrix} w_1(n) \\ w_2(n) \end{pmatrix}; p \right\} \qquad (9)$$

where MOD is the Modulo function and the real number p is usually taken equal to one.

In this later case, all trajectories are non-periodic, in fact they indicate very little structure. This is a starting point for the use of this map as a pseudo-random number generator.

The general idea is to create an appropriate symbolic dynamics from the map of equation (9), transform it into a binary series and examine whether it appears 'random' to a third party. If there is a significant lack of apparent structure, such a series may be used for a number of applications, most important among them the creation and distribution of encryption keys.

The creation of encryption keys and the subsequent creation of encryption protocols must, in this method, follow the outlines of the Vernam 'one time key' method. The idea is to exchange information between two users so that subsequent communications are carried out without further exchange of information about the keys.

In the original application of the Vernam protocol, the users obtain copies of a 'one time pad' of keys, of specific number and key length. The keys are marked for use at a specific date and time and are used only once. If the keys are random and the rule of one time use is strictly obeyed, this is the only theoretically secure method of communication.

Today's technology offers a modern variation of Vernam's old method, in the form of quantum key distribution (QKD). Already some methods based on such protocols have become available commercially. Although secure and reliable, the method seems expensive, time consuming and cumbersome, due to its making use of complex and sophisticated optical equipment. Its application to a world wide communication network such as the internet appears impractical.

Still, it is exactly in such networks, especially the Internet, where a secure and fast method of communication is absolutely necessary.

In a method making use of apparently random keys, these problems are mostly solved. Not only the creation and distribution of keys becomes easier and simpler, since the only information needing to be transmitted is the description of the exact initial map and the initial conditions by which the keys are created, but the users are given a variety of choices of map forms and initial conditions distribution methods, since, due to the simplicity of the initial map and the small size of the set of initial conditions, a large number of them may be stored, each one creating a key of arbitrary length [1], [3-4], [19].

In the following paragraph, a new method of symbolic dynamics and subsequent encryption keys' creation is presented, along with the theoretical and statistical evaluation to which it has been submitted.

3 DESCRIPTION OF THE SYMBOLIC SERIES, ITS PROPERTIES AND ITS APPLICATIONS

The creation of apparently random number series must obey certain long established rules, in order to be suitable for specific applications. In the most interesting case, that of encryption keys, the rules are especially well defined and stringent. First of all, the series must be almost totally without apparent structure. There are a lot of statistical criteria and corresponding tests available [web sites], [16], as well as some theoretical studies [12], also leading to a form of tests. Next, the series must be repeatable, in the sense of obtaining the same series by starting with the same initial conditions. Finally, the created keys must form a large enough key space so that a brute force attack will make no sense and the keys must be uncorrelated in the sense that knowledge of one of them should not yield any information about any of the others. This is expressed as sensitivity to initial conditions: a small change in the initial conditions should produce a key totally different from the initial one.

The method chosen for the creation of the keys was the following:

Each point $\vec{x}(n)$ of the map's trajectory in phase space is characterized by the appropriate coordinates $\left(x_1(n) \quad x_2(n) \quad . \quad x_k(n)\right)$. If one of them is chosen and, as an example, its 10^{th} decimal digit is isolated, then the series to be used as encryption key is created by the following rule: if the digit is even, the corresponding series element is 0. If the digit is odd, the corresponding series element is 1.

The symbol $\sigma(n)$, to be used as a key element, is defined by the following equation: $\sigma(n) = Mod\{INT\{10^{10} x_1(n)\}; 2\}$

This way, a binary symbolic series of arbitrary length is constructed. For every finite time value n, corresponds a binary digit of the key, according to the equation given above.

Our method generates 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

The keys created by this new method have been submitted to the NIST tests, as well as the "Diehard" tests constructed by Prof. G. Marsaglia [16]. These tests are available in the Internet. For the tests, two hundred series, of one million bits each, were prepared with the help of Java and Assembly software written in house. Furthermore, the keys were tested by the innovative method presented to us by Dr. K. Karamanos [12] and with his kind permission.

Also the keys were tested for sensitivity to initial conditions by various transformation and cross correlation software packages and also tested on the modern method of nonlinear complexity by Assist. Prof. N.Bardis [32]. The test execute at the Department of Automation Laboratories, Technological Education Institute of Halkis.

The tests results so far were 100% successful and are being continued. The final results will be presented in a future, extended manuscript.

4 CONCLUSION

Our work may be best summarized as follows:

- We have a method to generate 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 are created by the use of a family of discontinuous discrete dynamic systems and their symbolic dynamics. Yet they appear as 'random' series of binary digits to a third party. The apparent 'randomness', or, in other words, the lack of any structure in the series has been theoretically proven by topological arguments and ascertained by appropriate statistical tests
- Due to the above described property, the usual problems of key distribution do not exist here. The parameters required for the generation of a key for each message can be included as part of the previous message. No need for 'pads' or repeated contacts of trusted persons.
- In the above mentioned tests, more than two hundred keys of a length of a million bits have been tested by the most well known commercial tests available. The NIST tests and those published by prof. George Marsaglia are included. Our keys have been 100% successful. Therefore they are in principle suitable for 'one time key' applications.
- Our method generates 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 is 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.

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, IEEE Trans. CAS 35, 1988, 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, XP000607774, pp 127 – 140.

[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, 1988, pp. 648-658.
[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, 1990, pp. 241-255.
[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, 1992, pp. 401-409.
[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, 1990, pp.1068-1070.
[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, 1993, pp. 299-307.
[30] Nikolaos Papadakos, Quantum Information Theory and Applications to Quantum Cryptography, arXive: quant – ph/ 0201057 v1, 2002.
[31] Bardis N.G, Mitrouli M, Maris Th.I., Orlova M.N., "Some properties of Boolean functions and design of cryptographically strong balanced Boolean functions", World Scientific and Engineering Society TRANSACTIONS on INFORMATION SCIENCE and APPLICATIONS, Issue 2, Volume 1, ISSN 1790-0832, pp: 717 – 723, August 2004
[32]N.G.Bardis, A.Polymenopoulos, E.G.Bardis, A.P.Markovskyy, D.V.Andrikou, "An approach to determine the complexity of random and pseudo random binary sequences", World Scientific and Engineering Society TRANSACTIONS on COMMUNICATIONS, Issue 1, Volume 1, ISSN 1109-2742, 2002, pp: 37 – 42.
[33] Bardis N.G, Polymenopoulos A., Bardis E.G, Markovskyy A.P, "Methods for Increasing the Efficiency of the Remote User Authentication in Integrated Systems", INTERNATIONAL JOURNAL COMPUTER SCIENCE, Volume 12 No.1, 2003. ISSN 1535-6698, Nova Science Publishers, Inc, pp.55-63, 2003.