Cryptographic in Chaotic System

Pawan1, Shruti Sharma2, Salam Glain Thomson Singh3
1,2,3Dept. of Electronics and Comm. Engg, International Institute of Tech. & Management, Murthal, Sonepat, India

Abstract
It is widely recognized that data security will play a central role in the design of future communication systems. Many of those cryptography applications will be realized as chaotic systems, which rely heavily on security mechanisms. Note that a large share of those chaotic applications will be wireless, which makes the communication channel especially vulnerable. All modern security protocols use symmetric-key and public key algorithms. This contribution surveys several important cryptographic concepts and their relevance to chaotic system applications. The security requirements, such as authentication, confidentiality and integrity, always make computationally intensive processes and can easily become the bottleneck of the related applications. This paper presents chaotic secure communication scheme using synchronization. It shows how cryptography can be implemented for data transfer between source and destination.

Keywords
Cryptography; Chaotic synchronization; Chaotic modulation; Chaos Shift Keying.

I. Introduction
Chaotic Cryptography is an application of chaos theory which is aimed to provide security in the transmission of signal performed through telecommunications technologies. By secure communications, one has to understand that the contents of the information transmitted are inaccessible to possible eavesdroppers. In chaotic cryptography based on the complex dynamic behaviors provided by chaotic systems. After the seminal works of Pecora and Carroll [1,2], the basic idea of synchronization and control chaotic systems has received a great deal of interest among researchers from various fields. Most of the synchronization techniques consist of two parts: One of them is used as the transmitter, and the other as the receiver. They are connected in a configuration where the transmitter drives the receiver in such a way that identical synchronization of chaos between the two oscillators is achieved. For the purpose of transmission of information, at the transmitter, a information is added as a small perturbation to the chaotic signal that drives the receiver. In this way, the information transmitted is encrypted by the chaotic signal. When the receiver synchronizes to the transmitter, the information is decoded by a subtraction between the message sent by transmitter and its copy generated at the receiver by means of the synchronization of chaos mechanism. This works because, whilst the transmitter output contains the chaotic carrier plus the signal, the receiver output is made only by a copy of the chaotic carrier without the information. Chaotic cryptography method is preferred as over to traditional cryptography method because a digital signal can be transmitted to receiver at gigabit per second speed over 115 km with Bit Error Rate of one that at such a maximum speed, it is easier to generate strong, high-power chaotic signals than periodic signals. Chaotic signals are sensitive to initial conditions and have a noise like time series. As a result, chaotic transmissions have less risk of interception and are difficult to detect by eavesdroppers. It has also been observed that optimal asynchronous CDMA codes using chaotic spread-spectrum sequences can support 15% more users than the standard GOLD codes for the same Bit Error Rate (BER) performance [5]. In chaotic cryptography, the nonlinear characteristic of communication devices are utilized instead of being avoided, this minimizes the complicated measures to maintain linearity. As a result, chaotic cryptography systems can function over a larger dynamical range, with less complex components and operate at maximum power levels than conventional cryptography systems. The Block diagram of chaotic cryptography system.

![Chaotic secure communication](image)

For perfect chaotic cryptography error should be minimum. Chaotic carrier have the unpredictable behavior for long time but it is predictable for short time duration, Which is shown in fig. 2
that the dynamical state of one of the oscillators is completely obtained by the state of the other. When the chaotic systems are mutually coupled this functional has to be invertible, if there is a master-slave configuration the master determines the evolution of the slave, and \( \eta \) does not need to be invertible. Identical synchronization is the particular case of generalized synchronization when \( \Phi \) is the identity.

**C. Phase synchronization**

Phase synchronization found when the coupled chaotic oscillators maintain their phase difference bounded while their amplitudes remain uncorrelated. This phenomenon occurs even if the oscillators are not identical. In any case, if \( \eta_1(t) \) and \( \eta_2(t) \) denote the phases of the two coupled oscillators, synchronization of the phase is given by the relation \( \eta_1(t) = b \eta_2(t) \) with \( a \) and \( b \) whole numbers. A suitable example is the phase rotation about the unstable equilibrium points in a two dimensional projection of spiral Chua attractor [6].

**III. Chaotic Modulation**

Chaotic modulation is a process in which chaotic carrier is superimpose with message signal and chaotic carrier varies the characteristic according to message signal. The most important techniques are given below.

- Chaos Shift Keying (CSK);
- Differential Chaos Shift Keying (DCSK);
- Additive Chaos Modulation (ACM);
- Multiplicative Chaos Modulation (MCM).

Chaos shift keying also called chaotic switching was used to transmit digital signal. In this technique, digital signal is used to switch the transmitted message signal between two very similar chaotic oscillators, which are used to encode binary message signal. These two chaotic oscillators produced chaotic signal with same structure and different parameters. At the receiver end, recovered message signal is used to drive a chaotic system, which is similar to any of two chaotic systems in the transmitter. Then original signal is passed by butterfly filter. Chaos Shift Keying is very robust to noise, but when chaotic oscillators are very far away in bifurcation space, then it show very less degree of security [7]. Since, this scheme still has many possibilities of improvements.

**IV. Conclusion**

In this paper a detailed overview on cryptography has been described and explained different scheme of chaotic synchronization. Tell the advantages of chaotic cryptography over conventional cryptography. A few of most important chaotic modulation technique has been described. The lots of the research carried out so far that clearly show that chaotic cryptography has quite a numbers of advantages over conventional communication system.

**V. Acknowledgement**

The author is grateful to Mrs. Sajun Saini, Assistant Professor, Department of Electrical Engineering, DCRUST, MURTHAL, SONEPAT for his support and guidance.

**References**


Biography

Er. Pawan, Received B.teh Degree in ECE Deptt. From MDU Rohtak & M.Tech Degree From DCRUST,Murthal. Presently he is a Working Assistant Professor in ECE Deptt. at Internatioanl Institute of Technology & Managemant,Murthal , Sonepat. His Interet area is Control system, Digital Signal Process, Fuzzy Control Theory.

She is currently pushhing B.tech degree in ECE Deptt.,in IITM, Murthal. Her research interests include Signal Processing, computer networking Image Processing, communication systems, digital signal processing and network controlled systems.

He is currently pushhing B.tech degree in ECE Deptt.,in IITM, Murthal. His research interests include Signal Processing, Image Processing, communication systems, digital signal processing and Control system