Chaos Synchronization based Data Transmission with Asymmetric Encryption

Santo Banerjee
Laboratory of Cryptography, Analysis and Structure,
Institute for Mathematical Research,
Universiti Putra Malaysia

M.R.K Ariffin
Laboratory of Cryptography, Analysis and Structure,
Institute for Mathematical Research,
Universiti Putra Malaysia

ABSTRACT

In this article we consider the phenomena of chaos synchronization with bidirectional linear feedback coupling. The synchronized system can be used as a cryptosystem, where both the model can be considered as a transceiver. We have proposed an asymmetric cryptographic scheme for ensuring security of data being transmitted in the above manner. We utilize the recent disclosed AA_{β} public key cryptosystem which has implementation speed of $O(n^2)$. It is an asymmetric cryptographic scheme that utilizes the factorization problem of two large primes and is implemented only by using the multiplication operation for both encryption and decryption. With this simple mathematical structure, it would have low computational requirements and would have minimal impact on the continuity of data being transferred through chaos synchronization.

General Terms

Chaos synchronization, bidirectional linear feedback coupling, AA_{β} public key cryptosystem

Keywords

Chaotic encoding system, asymmetric cryptosystem

1. INTRODUCTION

Since the discovery of chaos synchronization [1], different approaches have been proposed, such as drive response synchronization [2], linear and nonlinear feedback synchronization [3], adaptive synchronization [4], coupled synchronization [5], active control method [6], impulsive synchronization [7], etc. The seminal work of Pecora and Caroll [1], attracted many researchers to the study of complex nonlinear systems [2-6]. Chaos and synchronization of two coupled chaotic systems have become an integral part of fast mode communication, since they work in the physical layer of the transmission system. The need for secure data communication is ever more necessary, given the tremendous growth in telecommunications and internet. Given the efficient mechanism that chaos synchronization offers to transmit data, it is important that a security mechanism be integrated to the system to ensure security. A suitable cryptographic technique will be chosen. Having in mind objectives of implementers of chaos synchronization techniques for communication to achieve fast and ``continuous" data transmission, the cryptographic scheme to be implemented must not drastically sacrifice this objective. The paper is as follows. In Section 2, we will describe synchronization between two chaotic systems with bidirectional coupling. We will focus on the Lorenz Stenflo system. Results show that synchronization occurs after $t>20$ hence ensuring fast and ``continuous" data transmission. The encoding scheme based on syncronization of chaotic systems is introduced in Section 3. In Section 4, we list criteria's that are deemed critical to be satisfied by any proposed security measure that is to be integrated with the chaos synchronization data transmission system. In Section 5, we propose a suitable asymmetric encryption scheme to provide security for data being transmitted which was recently introduced by Ariffin et.al [14]. An example is provided in Section 6 and we conclude in Section 7.

2. SYNCHRONIZATION BETWEEN TWO CHAOTIC SYSTEMS WITH BIDIRECTIONAL COUPLING

2.1 The system and its chaotic properties

We consider the Lorenz Stenflo system [9,10],

$$\begin{aligned} \dot{x}_1 &= a(x_2 - x_1) + cx_4 \\ \dot{x}_2 &= x_1(r - x_3) - x_2 \\ \dot{x}_3 &= x_1x_2 - bx_3 \\ \dot{x}_4 &= -x_1 - ax_4 \end{aligned} \tag{1}$$

Where x_1, x_2, x_3, x_4 are the state variables and a, b, c, r are parameters of the above system. The system (1) describing the acoustic gravity waves and forms an interesting extension of the Lorenz equation for its analysis with respect to its periodic and chaotic spectrum. The deterministic model (1) exhibits chaos for $a = 2.0, b = 0.7, c = 1.5$ and $r = 26.0$.

Figure (1) represents the color map of the bifurcation diagram of the system (1) with respect to the parameter r.

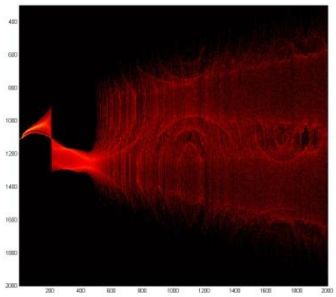

Fig 1: Optical bifurcation of the system (1)

2.2 Chaos Synchronization

We now consider the synchronization between system (1) and another identical system with bidirectional linear feedback coupling. The coupled system can be written as

$$\dot{X} = f(X) + K_1(X - Y) \quad (2)$$

$$\dot{Y} = f(Y) + K_2(Y - X) \quad (3)$$

where we have the following parameter representation $K_1 = (K_{11}, K_{12}, K_{13}, K_{14})$ and $K_2 = (K_{21}, K_{22}, K_{23}, K_{24})$. Let the error vectors be defined as

$$e_1 = y_1 - x_1, e_2 = y_2 - x_2, e_3 = y_3 - x_3, e_4 = y_4 - x_4 \quad (4)$$

Figure (3) represents the time variation of the error vectors e_i for $K_1 = 5, K_2 = 4.5$.

It can be observed that all the error vector components tends to zero after $t > 20$. We will apply the two synchronized chaotic systems for digital data transmission [11,12]. At the synchronized state, the sender uses the system (2) and the receiver use the system (3) to construct their encoding keys (see Section 3). It has to noted that, due to the short length of the key (either the the time for synchronization or the sequence of encoding keys), security has to be provided by other means (namely the suggested asymmetric cryptosystem in this paper in Section 5). The utilization of the encoding key is to transform data into a digitalized state suitable to be transmitted. It will be discussed in the next section.

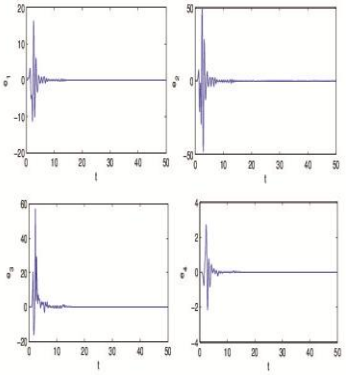

Fig. 2: Time variation of the synchronization errors with bidirectional coupling

3. PROPOSED CHAOS SYNCHRONIZATION ENCODING SCHEME

Transmission of data based on chaos exploits the phenomenon of chaos synchronization wherein the role of the transmitter and receiver is explicitly delegated. However, with bidirectional coupling it is possible to induce a flexibility to the role of the communicating parties and as a consequence of which full duplex mode of communication can be achieved. Recently, this mode of communication is creating a lot of buzz.

To choose the values of the encoding keys as integer, the sender and receiver choose [1000x] and [1000y], respectively from their own data set [8]. The data from $\boldsymbol{x(t)}$ picked up by the sender and the corresponding secret keys are shown in Table 1.

The encoding and decoding formula for phase-1 can be written as $\boldsymbol{c_i = p_i + k_i} \pmod{\mathbf{256}}, \boldsymbol{p_i = c_i - k_i} \pmod{\mathbf{256}}$ where $\boldsymbol{k_i}$ are the encoding keys to mask the message. In correspondence to every message unit we use one and only one key, which is randomly generated. For a complete message the encoding keys are a series of numbers $\{\boldsymbol{k_i}\}_{\boldsymbol{i=1}}^{\boldsymbol{n}}$. Actually, the key $\boldsymbol{k_j}$ encodes the message unit $\boldsymbol{p_j}$.

4. INDUCING SECURITY

A point to be observed is the practical value of synchronization time which is short in length. As a result to efficiently implement data transmission via chaotic synchronization in a secure manner, an encryption method has to be induced to the transmission either symmetric or asymmetric or a combination of both. Important issues surrounding the above proposed security mechanisms include (but not limited to) are:

1) Effective key distribution- to choose from symmetric or asymmetric.
2) Encryption/decryption speed.
3) Time Delay

4.1 Effective key distribution - to choose from symmetric or asymmetric

Key distribution is an integral element to ensure security deployment would not be disrupted. Unless an organization has unlimited resources to deploy keys to every authorized personnel communicating on a network, symmetric encryption would be unrealistic for the organization. As a result, asymmetric encryption would be the preferred choice. An asymmetric encryption scheme would allow for the public key of an intended recipient of data to be published without fear. After encryption is executed using the recipients' public key and the ciphertext relayed back to the recipient, data would then be decrypted via the recipients' private key.

4.2 Encryption/decryption speed

It is clear that in order to avoid key distribution issues, asymmetric encryption would be the viable security mechanism for data. However, prior to implementing such a security mechanism, the particular characteristics of possible algorithms should be scrutinized to ensure efficient implementation. The following table describes two popular and well known asymmetric schemes and the proposed AA_β cryptosystem in this paper.

Table 1. Encryption and decryption speed for message block of length $\boldsymbol{n}$

Algorithm	Speed	Remarks
RSA	$O(n^3)$	Exponential and modulo operations
ECC	$O(n^3)$	Scalar multiplication and modulo operations
AA_β	$O(n^2)$	Utilizes basic arithmetic operation of multiplication

In the case for asymmetric encryption implementation with either RSA or ECC a total (average) of n^3-steps are executed to encrypt a data block of length n -bits. Whereas, the AA_β cryptosystem would require n^2-steps.

4.3 Time Delay

With reference to section 4.2, time delay would be an overwhelming issue, since data transmitted via chaotic synchronization method in the previous section is "continuous" in nature. Organizations intending to deploy such solutions (i.e. the utilization of chaotic synchronization) would naturally appreciate the continuous streaming of data. Thus a delay is inevitable if asymmetric encryption is to be deployed. By referring to Table 1.0, a total of n^3-steps are expected to be executed to encrypt a data block of length n-bits if either the RSA or ECC algorithms are implemented. Hence, a delay of n^3-steps is expected. The actual time delay would depend on the equipment used.

5. THE AA_{β} CRYPTOSYSTEM

The communication model is between two parties A (Along) and B (Busu).

Definition 5.1 (Key Generation)
Let p and q be two secret prime numbers of n-bit length. Along's public keys are given by e_{A1} and e_{A2} such that

$$e_{A1} = pq \quad (5)$$
$$e_{A2} \equiv v \pmod{p} \quad (6)$$

where v is 0.8125n-bits long. Along's private keys are given by

$$d_{A1} = p \quad (7)$$
$$d_{A2} = v \quad (8)$$

Definition 5.2 (Encryption)
Busu will generate two ephemeral session keys: k_1 and k_2 each $(\frac{n}{6})$-bits long. The message that Busu will relay to Along is a $(\frac{4n}{5})$-bit integer m. Busu will produce the following ciphertext:

$$C = k_1 e_{A1} + k_2 e_{A2} + m \quad (9)$$

Proposition 1 (Decryption) [2]
Upon receiving the ciphertext C, Along will compute:

$$m = \big(C \pmod{d_{A1}}\big) \pmod{d_{A2}} \quad (10)$$

5.1 The AA_{β} - public key cryptography scheme

We will now discuss the $\boldsymbol{AA_{\beta}}$-cryptosystem. It is as follows: the scenario is that Busu will send an encrypted message to Along. Along will provide Busu with his public key pair $\boldsymbol{e_{A1}}$ and $\boldsymbol{e_{A2}}$. Busu intends to send the integer plaintext $\boldsymbol{P = m}$ as in Definition 5.2. Busu will then proceed to generate the ciphertext $\boldsymbol{C}$. Then Busu transmits the ciphertext $\boldsymbol{C}$ to Along.

Upon receiving the ciphertext from Busu, Along by Proposition 1, can retrieve the integer plaintext $\boldsymbol{P = m}$.

6. EXAMPLE

For illustrative purposes we will use encrypt "hello". Let both the sender and receiver are pre assigned to choose the variable x_1, y_1 respectively from their corresponding data sets at time $t = 100,101,102,\ldots$ to construct the secret keys. To encode the message "hello", they need five keys $k_1, \ldots, k_5$. The corresponding $1000k_i \pmod{256}$ generates the integers $\{136, 164, 249, 101, 10\}$. For implementation purposes we will use a particular control character to be inserted in between the integers to identify the particular characters. For this example we will use the symbol "#" which corresponds to the ASCII value 35. The list will now become $\{136, 35, 164, 35, 249, 35, 101, 35, 10\}$. Next we will concatenate (each block will of 8-bits, if less system will pad 0's from the most significant bit) the above values and as a result the message to be encrypted is given by (we produce here its hexadecimal value) $M = 8823A423F9236523$. Since the length of the message is 64-bits, for illustrative purposes we will set $n = 80$. The primes that we use in this example are given by $p = FE55B650E3BA876B76C7$ and $q = F3CADD74B48A7C1D79A9$. The other private value is $v = 1ED93B98E3BE30CDD$. The corresponding public keys are
$e_{A1} = F234E7B494960AAD0894E93FE960D82009A0785F$ and $e_{A2} = AB3F4ACE764297ADD75E37AC0C9023D061F68045$.
The sender will generate the ephemeral session keys $k_1 = 1C91$ and $k_2 = 1D0F$.
Finally, the ciphertext is given by $C = 2E772D7DC3070B3C8D8770AEDB3B602243A5A42B4BF$.
Decryption is trivial.

7. CONCLUSION

In this work, we have proposed a a merger of chaotic synchronization by two way synchronized acoustic wave systems techniques for fast data transmission together with an asymmetric cryptosystem that has minimum effect on the ``continuous" transmission of data for high speed communication purposes. The asymmetric scheme which has been proposed to encrypt data is much more faster than traditional asymmetric encryptions. The system possesses a vast key space and is immune to major statistical attacks. The system can be effectively used in real time

8. ACKNOWLEDGMENTS

This work was partially funded by PRGS-5528100, Ministry of Higher Education, MALAYSIA.

9. REFERENCES

[1] Fujisaka H. and Yamada T. 1983. Stability theory of synchronized motion in coupled-oscillator systems; Pecora L. M. and Carroll T. L. 1990. Synchronization in chaotic systems.

[2] Carroll T. L. and Pecora L. M. 1991. Synchronizing chaotic Circuits.

[3] Agiza H. N. and Yassen M. T. 2001. Synchronization of Rossler and Chen Chaotic Dynamical Systems Using Active Control.; Chen H.-H. 2007. Adaptive synchronization of chaotic systems via linear balanced feedback control.

[4] Wang Y. W., Guan Z. H. and Wang H. 2003. Feedback and adaptive control for the synchronization of Chen system via a single variable.; Bowong S. 2007. Adaptive synchronization between two different chaotic dynamical systems.

[5] Alexeyev A. A. and Shalfeev V. D. 1995. Chaotic synchronization of mutually coupled generators with frequency-controlled feedback loop.

[6] Wu X., Guan Z. H., Wu Z. and Li T. 2007. Chaos synchronization between Chen system and Genesio system.

[7] Yang T. and Chua L. O. 1997. Impulsive control and synchronization of nonlinear dynamical systems and application to secure communication.

[8] S.Banerjee, J. A.Yorke and C.Grebogi. 1998. Robust Chaos.

[9] L.Stenflo. 1996. A Nonlinear equations for acoustic gravity waves.

[10] S. Banerjee, P.Saha and A. RoyChowdhury. 2001. Chaotic scenario in the Stenflo equations.

[11] S.Banerjee, L.Rondoni, S.Mukhopadhyay. 2011b. Synchronization of time delayed semiconductor lasers and its applications in digital cryptography.

[12] S.Banerjee , D.Ghosh, A.Ray and A.R. Chowdhury. 2008. Synchronization between two different time-delayed systems and image encryption.

[13] M.R.K.Ariffin , M.A.Asbullah and N.A.Abu. 2011. Security Features of an Asymmetric Cryptosystem based on the Diophantine Equation Hard Problem. arXiv:1103.4433v23