ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Chaotic Based Public Key Encryption Using Augmented Lorenz Equation

Winnie Sara Simon, Josy Elsa Varghese

Pursuing M.Tech, Dept. of CSE, Caarmel Engineering College, MG University, Kerala, India

Assistant Professor, Dept of CSE, Caarmel Engineering College, MG University, Kerala, India

ABSTRACT: An asymmetric secret key cryptographic system using an application of augmented Lorenz equation to chaotic cryptography is proposed. The cipher text is generated by superimposing the chaotic signal generated from augmented Lorenz equation onto a plain text. The plain text can be extracted from the received cipher text by unmasking the chaotic signal, which can be reproduced using a secret key. The secret key consists of real numbers that are obtained from augmented Lorenz equation. Two channels are used for communication- a quantum communication channel through which the secret key is transmitted and a classical data communication channel through which the cipher text is transmitted. The performance of symmetric key cryptography and asymmetric key cryptography on augmented Lorenz equations are compared and analyzed.

KEYWORDS: Augmented Lorenz equations, chaotic cryptography, quantum key distribution

I. INTRODUCTION

Chaotic Cryptography is one of the interesting applications of chaos to engineering. It makes use of chaos theory, which studies the behaviour of dynamical systems to perform different cryptographic tasks in a cryptographic system. In chaotic cryptography, encryption is done by superimposing a chaotic signal generated through different techniques on to a plain text. During decryption, the chaotic signal is unmasked from the cipher text to obtain plain text. The complex behaviour of chaotic dynamical systems is used to hide or mask information in chaotic cryptosystems. The signals generated from chaotic dynamics are broadband, noise-like and difficult to predict. Chaotic synchronization, chaotic shift keying, chaos control, distributed dynamics encryption, public-key encryption, chaotic block ciphers, and cryptanalysis of chaos-based cryptosystems are the different methods invented for chaos-based cryptography.

In chaos based message encryption, the bifurcation parameters (the chaotic system parameters) or the initial conditions of chaotic dynamics are used as secret keys that are shared between sender and receiver. The Prandtl number σ, reduced Rayleigh number R_0 and geometrical parameter b are known as the bifurcation parameters. The number of possible combinations of bifurcation parameters and initial conditions of the chaotic system determines the size of the key space. However, the size of the key space is not significantly large and a slight difference in secret key would not have much impact on the dynamic behaviour of the signal. This makes it easy for an adversary to guess the secret key from the reduced key space using Brute Force attack and then eventually break the secret key. Alvarez and Li [1] discussed such a security issue in terms of the notions of diffusion and confusion.

The rotational motion of the chaotic waterwheel, which was discovered by Malkus and Howard exactly matches to the Lorenz equations with b=1 [2] [3]. A chaotic gas turbine motivated by chaotic waterwheel was developed whose non dimensionalized expression of equations of motion of the turbine represents a network of infinitely many Lorenz subsystems. The Augmented Lorenz equations are obtained when the non-dimensionalized equations with a number of Lorenz subsystems are truncated at a finite number N. The augmented Lorenz model is a (2N+1) -dimensional system of non-linear ordinary differential equations for 2N+1 generalized coordinates. The dynamical nature of the augmented Lorenz model depends on a dimensionless N×N diagonal integer matrix in addition to σ and R_0 with b=1. The main advantage of Augmented Lorenz model is that the system is not bound to the physics of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

the gas turbine. Also augmented Lorenz model yields sufficient high-dimensional chaos necessary to perform cryptographic tasks.

In the proposed system, the augmented Lorenz equations are applied to a chaotic cryptosystem, as a symmetric and asymmetric key system, designed in a different manner from the CO method [4]. The communication in the cryptographic system is assumed to take place through digital systems that are connected via both a classical channel and a quantum communication channel. The main advantage of the proposed system is the large key space. The size of the key space is 2^{N-1}. The secret key obtained from the large key space is distributed from sender to receiver using a quantum key distribution protocol (QKD). To obtain the binary secret key, N×N-dimensional diagonal integer matrix specifying the dynamic behaviour of the augmented Lorenz equations can be extended to a diagonal real matrix. The remaining parameters and the initial conditions of the augmented Lorenz equations are assumed to be known to every participant including the adversary. After sharing the secret key through a quantum key distribution channel with the help of quantum key distribution protocol, the sender sends a plaintext encrypted using chaotic masking and the receiver decrypts the cipher text by eliminating the masking signal exactly reproduced using the secret key. The number of combinations of the secret key is prohibitively large (e.g. 2^{100}) to discourage the adversary from breaking the key.

The rest of the paper is organized as follows. Section 2 formulates the motivation and overview. Section 3 shows the system architecture. Section4 describes the methodology. Section 5 concludes the work.

II. MOTIVATION & OVERVIEW

Chaotic cryptography deals with hiding secret messages and then recovering it using algorithm which consists of encryption rule that uses chaotic functions (analog or digital). Chaos is not a sufficient property for encryption. The notion of cryptographic security has no counterpart in chaos theory at present, and crypto-tools are necessary to check the cryptographic security of a chaos-derived encryption algorithm. The entities use chaos theory as a new way to encrypt messages but because of lack of thorough, provable security properties and low acceptable performance, chaotic cryptography has encountered setbacks.

A system of three ordinary differential equations studied by Lorenz [5] which are now known as Lorenz equations, is one of the simplest systems to exhibit chaotic behaviour. The three time-dependent state variables x(t), y(t) and z(t) in Lorenz equations determine the evolution of a system. Lorenz wrote the equations in the form

$$dx/dt = \sigma(y-x) \quad (1)$$

$$dy/dt = rx-y-xz \quad (2)$$

$$dz/dt = xy-bz \quad (3)$$

where σ, r and b are real, positive parameters. The variables in the problem can be interpreted as follows:

- x is proportional to the intensity of the convective motion.
- y is proportional to the temperature difference between the ascending and descending currents.
- z is proportional to the distortion of the vertical temperature profile from linearity.
- t is the dimensionless time.
- σ is called the Prandtl number (it involves the viscosity and thermal conductivity of the fluid),
- r is a control parameter, representing the temperature difference between the top and bottom of the tank
- b measures the width-to-height ratio of the convection layer.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

A chaotic cryptosystem using the Lorenz equations [5] was introduced by Cuomo and Oppenheim and Cuomo *et al* [1]. In the Cuomo-Oppenheim (CO) method [4], the sender Alice transmits a message *m* (a plaintext) masked by a chaotic signal, usually the variable *X* of a first Lorenz oscillator in Alice's system, to receiver Bob via a classical communication channel. In Bob's system, the received signal *m+X* (a cipher text) is directly input to the variable of a second Lorenz oscillator, and the signal *Y* from the second oscillator is directly input to the variable *Y* of a third Lorenz oscillator. As long as the plaintext *m* and noise contamination on the communication channel are sufficiently smaller than the masking signal *X*, a replica of the masking signal is approximately reproduced by the third oscillator owing to chaotic synchronization between the Lorenz oscillators that are set identical using the secret key consisting of σ, R_0 and *b* distributed from Alice to Bob with an appropriate key distribution protocol. Eventually, the cipher text is decrypted by subtracting the replica of *X* from *m+X*.

However, the CO method [1] is known to be weak against Eve's attacks to break the secret key, even though the key distribution is achieved with a high degree of security. In fact, the dynamical properties of the Lorenz model, such as the bifurcation structure as a function of σ, R_0 and *b*; the geometrical structure of the basin of attraction as a function of the initial conditions for the variables *X*, *Y* and *Z*; and the dynamical stability of the synchronization manifold for coupled Lorenz oscillators, have been extensively investigated. These established results make it feasible to identify the secret key from the eavesdropped signal.

Chaotic cryptography takes advantage of the complex behaviour of chaotic dynamical systems to hide or mask information. Cuomo-Oppenheim method [1] method uses the dynamic behaviour of Lorenz system to perform cryptographic operations. The distribution of key is achieved with great security in CO method. But an eavesdropper can easily guess the secret key used in CO method as the size of the key space is not sufficiently large through a brute force attack. The adversary can then break the secret key and obtain the plain text that is transmitted from sender to receiver. To tackle this problem and to enhance the security, the system to generate chaotic signal from augmented Lorenz equation is proposed.

III. SYSTEM ARCHITECTURE

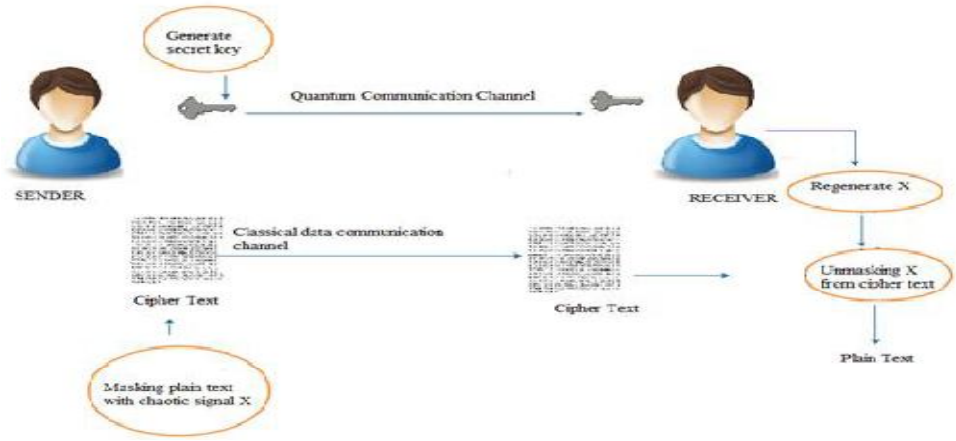

Fig1.System Architecture

The figure 1 depicts the system architecture of the proposed system. Here, the sender first generate secret key from augmented Lorenz equations and send it to the receiver via a quantum communication channel with the help of quantum key distribution (QKD) protocol. The sender generates the chaotic signal X from the secret key. He then masks the plain text with the chaotic signal (m+X) and sends it to the receiver via a classical data communication channel. At the receiver side, the chaotic signal X is regenerated from the secret key and the receiver then unmasks the plain text from cipher text by subtracting the chaotic signal X from m+X (cipher text).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

IV. METHODOLOGY

A. Generalization of Augmented Lorenz Equations

The augmented Lorenz equations in their original form are given below.

$$\dot{X} = \sigma\, tr[(n^{-1})^2 Y] - X \quad (4)$$
$$\dot{Y} = RX - nZX - Y \quad (5)$$
$$\dot{Z} = nYX - Z \quad (6)$$
$$R = R_0 n_2 \varphi W \quad (7)$$

Here, X is a dimensionless scalar variable; Y and Z are dimensionless $N \times N$ diagonal matrices whose diagonal components are labelled as Y_n and Z_n, respectively, with n running from 1 to N. $\dot{X}$, $\dot{Y}$ and $\dot{Z}$ represent the first-order derivatives of X,Y and Z with respect to dimensionless time τ ,respectively and tr(.) expresses the diagonal sum of a matrix. (6)

The augmented Lorenz equations can be generalized by extending the diagonal integer matrix n in n = diag(1,....,*n*,..., *N*) to a diagonal real matrix M consisting of positive real numbers. That is,

$$M=diag(M_1,....,M_n,...M_N), \quad (8)$$

where M_1=1 and M_2 to M_n are set to positive real numbers under the constraints of n-1< $M_n \leq n$+1 for n= 2,....,N. The secret key is obtained from the key matrix M.

B. Message Encryption

The key matrix M = diag (M_1, M_2,.....,M_N) is used as the secret key in the proposed system.M_1 is always set to M_1 =1. The remaining components M_2,.....,M_N constitute the secret key. The binary secret-key system in which M_n takes either n or n= 0.5 for n= 2,.....,N is adopted for secret key distribution . The real matrix M is mapped into an integer diagonal matrix Q= diag(Q_1,Q_2,....Q_N), where Q_1 is always set to Q_1=0 and Q_n with n running from 2 to N is 0 or 1 corresponding to M_n= n or M_n= n+0.5 , respectively. Thus, by sharing Q_2,...,Q_N Alice and Bob establish the secret key.

For determining the key matrix, the procedure can be reversed. First, Alice and Bob randomly assign 0 or 1 to Q_n (n= 2,....,N). Then, they establish the key matrix by setting M_n to n or n+0.5 in accordance with the value of Q_n. When using a QKD protocol to share the key matrix between Alice and Bob, the reverse procedure is convenient.

The augmented Lorenz model is not applicable to the CO method for message encryption. An alternative method for applying the augmented Lorenz model to cryptography is proposed. The system utilizes both a conventional digital communication channel on which the cipher text is sent from Alice to Bob and a quantum communication channel on which the secret key is shared between Alice and Bob. Message encryption is performed using chaotic masking on a classical digital system by Alice. The plain text is masked by chaotic signal X as digital pseudorandom numbers numerically generated from the augmented Lorenz equations. The bifurcation parameters R_0, σ and φ; the initial conditions of X, Y and Z ; the time width ∂_T ; and the truncation time T_0 to eliminate the initial transient part of the numerical solutions of X, which are all indispensable for the numerical integration of the equations, are available to any party (including Eve) as public keys. Thus, Alice sends the cipher text $m+X$ to Bob via a classical communication channel. Bob retrieves from the cipher text by exactly reproducing the masking signal through numerical integration of the augmented Lorenz equations identified by the secret key and subsequently subtracting from on his digital system

C. Secret-Key Distribution

The remaining problem is to safely distribute the key matrix from Alice to Bob. The Diffie-Hellman (DH) and the Rivest-Shamir-Adleman (RSA) methods are the well-known key-distribution methods that are applicable to distributing

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

the key matrix. The key matrix M is represented as a binary-key system, i.e. Q = diag(Q_1,Q_2,....Q_N), and the string "$Q_2Q_3Q_4$.....Q_N " is treated as a plaintext of a string of letters consisting of the letters "0" and "1".

One of the most promising quantum information processing is the Bennett-Brassard 1984 (BB84) Quantum key distribution (QKD) protocol. It is a task of generating a private key shared between two parties using a quantum channel and an authenticated classical channel (Eg. Telephone lines). The private key can then be used to encrypt messages that are sent over an insecure classical channel. The QKD protocol guarantees unconditional security within the limit of quantum mechanics, in the sense that the adversary cannot make any clone of the secret key and his eavesdropping is inevitably detected by the sender and the receiver.

The BB84 protocol is a practical choice of QKD protocols. While applying BB84 protocol to proposed cryptosystem, the key matrix M is represented as the binary secret-key system Q_2...Q_N, each of which can be coded by the direction of polarization of a single photon. The sender transmits a train of more than of 2*N* single photons (2*N* qubits) through randomly chosen polarization basis, a rectilinear basis or a diagonal basis to the receiver over a quantum communication channel. The receiver receives the train of photons and observes their polarizations with his chosen polarization basis. After reporting their choices of the basis between the sender and the receiver on a classical communication channel, they share the *sifted* keys from which the secret key is set, estimate the communication error rate of the quantum channel, and know which photon has been observed by the adversary and the amount of information that the adversary has elicited by eavesdropping. If the error rate is significantly large, the sender and the receiver discard their results and restart the QKD process from the beginning. The binary secret key is safely shared between sender and receiver after the error correction and privacy amplification.

V. CONCLUSION

A symmetric and asymmetric secret key cryptographic system over augmented Lorenz equations is proposed. The cipher text is obtained by superimposing the chaotic signal generated from augmented Lorenz equation onto a plain text. The plain text can be extracted from the received cipher text by unmasking the chaotic signal using a private key. Also an asymmetric secret key cryptographic system over augmented Lorenz equations is proposed where a public key and a private key are used. Both the public key and private key are obtained from augmented Lorenz equations. A quantum communication channel and a classical data communication channel are used for communication. The secret key is transmitted through quantum communication channel and cipher text is transmitted through classical data communication channel. The performance of both symmetric key cryptographic method and asymmetric key cryptographic method over augmented Lorenz equations are compared and analysed. Since complete security cannot be achieved, there is always scope for improvement.

ACKNOWLEDGEMENT

We would like to thank reviewers for their helpful and constructive comments. We would also like to thank the faculties, the resource providers and the system administrator for the useful feedback and constant support.

REFERENCES

1. G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," Int. J. Bifurcation Chaos, vol. 16, pp. 2129–2151, 2006.
2. .S.H.Strogatz,NonlinearDynamicsandChaos. Reading,MA,USA: Addison-Wesley, 1994, p. 9..
3. M.KolárandG.Gumbs,"Theoryfortheexperimentalobservationof chaos in a rotating waterwheel," Phys. Rev. A, vol. 45, pp. 626–637, 1992. B. Chen and V. Chandran, "Biometric based cryptographic key generation from faces," in Proc. Digital Image Comput. Tech. Applicat., 2007,pp. 394–401.
4. K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronizedchaoswithapplicationstocommunications,"Phys.Rev. Lett., vol. 71, no. 1, pp. 65–68, 1993
5. E.N.Lorenz,"Deterministicnonperiodicflow,"J.Atmos.Sci.,vol.20, pp. 130–141, 1963