2015 International Symposium on Nonlinear Theory and its Applications
NOLTA2015, Kowloon, Hong Kong, China, December 1-4, 2015

Chaos-Based Cryptography Using Augmented Lorenz Equations

Kenichiro Cho and Takaya Miyano

Graduate School of Science and Engineering, Ritsumeikan University
1-1-1 Noji-Higashi, Kusatsu, Shiga, 525-8577 Japan
Email: cho@fc.ritsumei.ac.jp, tmiyano@se.ritsumei.ac.jp

Abstract—We have developed a chaos-based cryptographic method using the augmented Lorenz equations. In our method, the secret key is given as an N-dimensional real diagonal matrix that specifies the augmented Lorenz equations, being assumed to be shared between legitimate users using a quantum key distribution. We apply our method to speech encryption and evaluate its security on the basis of the degree of visible determinism in chaotic sequences as pseudorandom numbers generated by the augmented Lorenz equations.

1. Introduction

The augmented Lorenz model is a system of $2N+1$-dimensional ordinary differential equations as a nondimensionalized expression of the equations of motion for a chaotic gas turbine [1]. This dynamical model is represented as a star network of N Lorenz subsystems sharing the variable X as the central node and can simulate the motion of a convective flow in turbulent Rayleigh-Bénard convection at high Rayleigh numbers exceeding 10^6 [2]–[4], in the sense that it can reproduce the statistical properties of the velocity field in an actual turbulent convective flow.

We recently have applied the augmented Lorenz model to chaotic cryptography [5]. In our method, the sender and receiver of a message, called Alice and Bob, respectively, have identical augmented Lorenz oscillators specified by a common N-dimensional real diagonal matrix, denoted as $\mathbf{M}$, in their communication systems. $\mathbf{M}$ works as a secret key, i.e., a symmetric key, which is assumed to be securely exchanged between Alice and Bob using a quantum key distribution (QKD), e.g., the Bennett-Brassard 1984 (BB84) protocol [6]–[9]. Within the limit of quantum physics, QKD guarantees absolutely secure distribution of a secret key that can be used as pseudorandom numbers for message encryption. However, this does not mean that the key securely distributed by QKD is always sufficiently secure when it is used as pseudorandom numbers for message encryption.

To circumvent this problem, we apply QKD to exchange $\mathbf{M}$ as a secret key and use the chaotic sequence generated by the augmented Lorenz oscillators specified by $\mathbf{M}$ as the pseudorandom numbers. Here, we set the dimension N of $\mathbf{M}$ to an appropriate number such that the secret-key space has a large size but it takes a short time to distribute $\mathbf{M}$ using QKD. For instance, N is set to $N = 101$. Then, the size of the secret-key space amounts to $2^{N-1} = 2^{100} \sim O(10^{30})$, which prohibits an eavesdropper (a hostile attacker), called Eve, to identify $\mathbf{M}$ by a brute force attack. Thus, Alice and Bob can make a long sequence of pseudorandom numbers, which is usually much longer than N, and can practically use our cryptosystem as a one-time pad cipher.

In this paper, we evaluate the degree of randomness of chaotic time series generated by the augmented Lorenz equations and show how our cryptographic method would be effective for speech encryption using the time series as a masking signal.

2. Augmented Lorenz Model and Chaotic Cryptography

The augmented Lorenz equations as a dimensionless dynamical model are defined as

$$\frac{dX}{d\tau} = \sigma\left[\mathrm{tr}\left((\mathbf{M}^{-1})^2\mathbf{Y}\right) - X\right] , \quad (1)$$

$$\frac{d\mathbf{Y}}{d\tau} = \mathbf{R}X - \mathbf{M}\mathbf{Z}X - \mathbf{Y} , \quad (2)$$

$$\frac{d\mathbf{Z}}{d\tau} = \mathbf{M}\mathbf{Y}X - \mathbf{Z} , \quad (3)$$

$$\mathbf{R} = R_0\mathbf{M}^2\mathbf{\Phi}\mathbf{W} ,$$

where X is a scalar variable, $\mathbf{Y}$ and $\mathbf{Z}$ are $N \times N$ diagonal matrices whose diagonal components are denoted as Y_n and Z_n with n running from 1 to N, respectively, τ is dimensionless time, $\mathrm{tr}(\cdot)$ denotes the diagonal sum of a matrix, σ and R_0 are bifurcation parameters corresponding to the Prandtl and Rayleigh numbers, respectively. The matrix $\mathbf{R}$ is defined using

$$\mathbf{M} = \mathrm{diag}(M_1,\ M_2,\ \ldots\ ,\ M_N) , \quad (4)$$

$$\mathbf{W} = \mathrm{diag}(\sin\phi, \sin M_2\phi, \ldots, \sin M_N\phi) , \quad (5)$$

$$\mathbf{\Phi} = \mathrm{diag}\Big(\phi - \frac{1}{2}\sin 2\phi\ ,\ \ldots\ ,$$
$$\frac{1}{M_n-1}\sin(M_n-1)\phi - \frac{1}{M_n+1}\sin(M_n+1)\phi\ ,\ldots\ ,$$
$$\frac{1}{M_N-1}\sin(M_N-1)\phi - \frac{1}{M_N+1}\sin(M_N+1)\phi\Big) \quad (6)$$

where ϕ is a bifurcation parameter.

In this study, the bifurcation parameters σ, R_0, and ϕ are set to $\sigma = 25$, $R_0 = 3185$, and $\phi = 0.36$ [rad], respectively. These parameter settings were confirmed to yield chaos [5].

In our cryptographic method, Alice and Bob share $\mathbf{M}$ as a secret key, where M_1 is always set to $M_1 = 1$ and M_n with n running from 2 to N randomly takes n or $n + 1/2$. $\mathbf{M}$ can be mapped to the corresponding binary secret key $\mathbf{Q} = \mathrm{diag}(Q_1, \ \ldots \ , \ Q_N)$ according to $Q_n = 0$ if $M_n = n$ and $Q_n = 1$ otherwise for $n = 1, \ \ldots \ , \ N$. This procedure can be reversed. Indeed, when sharing $\mathbf{M}$, Alice and Bob first exchange N binary numbers Q_n using a QKD and transform $\mathbf{Q}$ into $\mathbf{M}$ by reversing the rule mentioned above.

Alice and Bob perform speech encryption and decryption with the following procedure. The bifurcation parameters σ, R_0, and ϕ, the initial values of X, $\mathbf{Y}$, and $\mathbf{Z}$, and the algorithm for numerical integration of the augmented Lorenz equations as well as the time width Δt and the initial truncation time T_0 are all opened to all users as public keys. Only $\mathbf{M}$ is used as the secret key shared between Alice and Bob.

Alice records a speech signal as a time series in the form of text, denoted as $m(t)$. Here, $t = i\delta t$ with non-negative integers $i = 1, \ \ldots \ , \ L$ and δt represents the sampling time of the speech with a real physical dimension. Alice yields a chaotic time series $X(\tau)$ (i.e., $X(i)$) with dimensionless time $\tau = i\Delta t$ ($i = 1, \ \ldots \ , \ L$) by running her augmented Lorenz oscillator specified by $\mathbf{M}$. She obtains a pseudorandom sequence of $X(\tau')$ with $\tau' = iT$ ($i = 1, \ \ldots \ , \ L\Delta t/T$) and an appropriately chosen sampling time interval T. She transforms the pseudorandom sequence into $X(t)$ as a function of t with the real physical dimension using $\alpha t = T$, where α [s^{-1}] is an appropriately chosen time coefficient. Finally, she performs speech encryption by adding $X(t)$ to $m(t)$ and sends the ciphertext $m + X$ to Bob.

Bob receives $m + X$ and yields X by running his augmented Lorenz oscillator identical to that of Alice with T, δt and α shared between Alice and Bob. Thus, he decrypts the ciphertext by subtracting X from $m + X$.

3. Numerical Results and Discussion

3.1. Time Series Analysis

Randomness in the time series of $X(i)$ is evaluated in terms of the degree of visible determinism using the algorithm introduced by Wayland et al. [10]. Their method is briefly described below. From a time series, we construct d-dimensional embedding vectors denoted as $\mathbf{x}_i$. Then, a vector $\mathbf{x}_{p(0)}$ is randomly chosen and its K nearest neighbors $\mathbf{x}_{p(k)}$ ($k = 1, \ \ldots \ , \ K$) are found. Images of $\mathbf{x}_{p(k)}$, denoted as $\mathbf{x}_{p(k)+T_0}$ for $k = 0, \ \ldots, \ K$, are generated under an appropriate time interval T_0. Finally, the diversity in the directions of neighboring embedding vectors is estimated in terms of the translation error E_{trans} defined by

$$E_{trans} = \frac{1}{K+1} \sum_{k=0}^{K} \frac{| \ \mathbf{v}_{p(k)} - \bar{\mathbf{v}} \ |^2}{| \ \bar{\mathbf{v}} \ |^2} \ , \tag{7}$$

$$\bar{\mathbf{v}} = \frac{1}{K+1} \sum_{k=0}^{K} \mathbf{v}_{p(k)} \ , \tag{8}$$

$$\mathbf{v}_{p(k)} = \mathbf{x}_{p(k)+T_0} - \mathbf{x}_{p(k)} \ . \tag{9}$$

The smaller E_{trans} indicates the more visible determinism in the time series. To reduce the statistical error in estimates of E_{trans}, we take the mean over W medians of E_{trans} for W sets of P randomly chosen $\mathbf{x}_{p(0)}$.

We ran the augmented Lorenz equations with $N = 101$ at a time width of 2.0×10^{-7}. The initial conditions of X, $\mathbf{Y}$, and $\mathbf{Z}$ were given as pseudorandom numbers subject to the standard normal distribution. The key matrix $\mathbf{M}$ was given by randomly assigning n or $n+1/2$ to M_n for $N = 2, \ \ldots \ , \ N$. Initial 250000 data points of the time series were discarded to eliminate initial transient part of the series.

Figures 1(a) and (b) show part of the time series $X(\tau)$ (i.e., $X(i)$) with $T = 100$ and $T = 10000$, respectively ($\alpha = 1000$). Figure 2 shows estimates of E_{trans}, where $L = 1000$, $T_0 = 5$, $W = 10$, and $P = 51$. The determinism underlying the time series with $T = 10000$ is much less visible than that with $T = 100$, and the estimated translation errors are close to those of uncorrelated white noise [11] when $T = 10000$, although the time series have been generated by the augmented Lorenz equations as a fully deterministic dynamical model. These observation indicate that the time series with $T = 10000$ is useful as a masking signal.

3.2. Message Encryption

We used speech data comprising the words "Yes, we can." as a plaintext, The speech was spoken by one of the authors (K. C.) and recorded using a digital voice acquisition system with a signal quantization level of 16 [bit] and a sampling frequency of 44.1 [kHz]. The speech data were transformed into a plaintext $m(t)$ consisting of the numbers representing the air-pressure intensities. The time series $X(\tau)$ with $T = 10000$ was transformed with $\alpha = 1000$ into a masking signal $X(t)$. Message encryption was performed by adding $X(t)$ to $m(t)$.

Figures 3(a) and (b) show the plaintext m and the ciphertext $m+X$, respectively. It can be seen that the plaintext is entirely masked by the chaotic time series. No peaks characteristic of the plaintext could be recognized in the power spectrum of the ciphertext. The

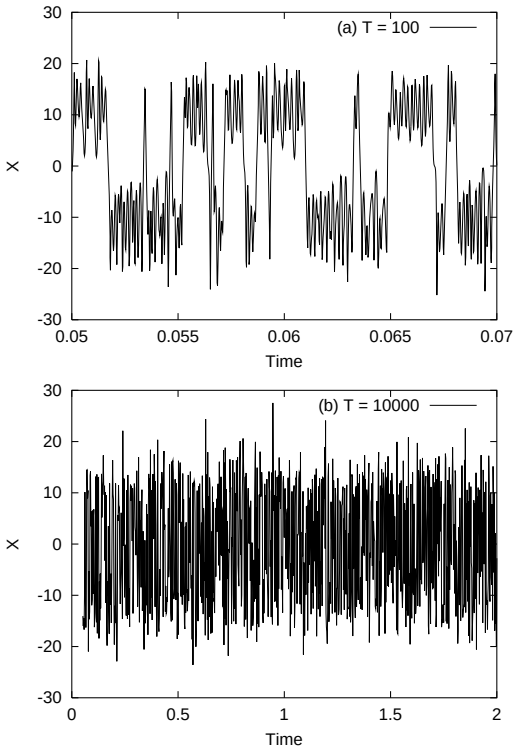

Figure 1: Time series $X(\tau)$ under sampling time intervals of (a) $T = 100$ and (b) $T = 10000$.

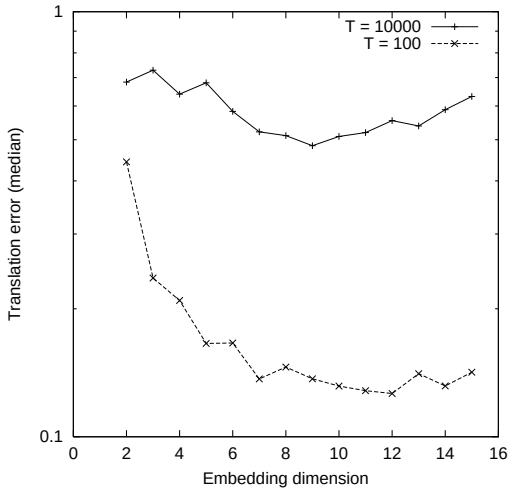

Figure 2: Estimates of the translation error as a function of embedding dimension for the time series with $T = 100$ ($\times$) and $T = 10000$ (+).

decrypted message was confirmed to be identical to the original plaintext. Thus, our cryptographic method is shown to be applicable to encrypting speech data.

4. Conclusions

We have estimated the degree of visible determinism using the diagnostic algorithm by Wayland et al. for the time series X with time intervals of $T = 100$ and $T = 10000$. It has been shown that the time interval $T = 10000$ generates a chaotic time series, the underlying determinism of which is as invisible as those of uncorrelated Gaussian stochastic processes. Such randomness suffices for encryption of speech data. The size of the secret-key space of $\mathbf{M}$ with $N = 101$ amounts to 2^{100}, which is prohibitively large for Eve to break the key by a brute force attack and hence enables us to practically use our method as a one-time pad cryptography. The application of our method to encrypting a binary-coded plaintext is an open question to be investigated in future studies.

Acknowledgments

This study is supported by JSPS Grant-in-Aid for Scientific Research (C) No. 15K000353.

References

[1] K. Cho, T. Miyano, and T. Toriyama, "Chaotic gas turbine subject to augmented Lorenz equations," *Phys. Rev.* E, vol. 86, 036308, 2012.

[2] K. R. Sreenivasan, A. Bershadskii, and J. J. Niemela, "Mean Wind and its Reversal in Thermal Convection," *Phys. Rev.* E, vol.65, 056306, 2002.

[3] F. Fontenele Araujo, S. Grossmann, and D. Lohse, "Wind Reversals in Turbulent Rayleigh-Bénard Convection," *Phys. Rev. Lett.*, vol.95, 084502, 2005.

[4] G. Ahlers, S. Grossmann, and D. Lohse, "Heat transfer and large scale dynamics in turbulent Rayleigh-Benard convection," *Rev. Mod. Phys.*, vol.81, pp.503–537, 2009.

[5] K. Cho and T. Miyano, "Chaotic cryptography using augmented Lorenz equations aided by quantum key distribution," *IEEE Trans. Circuits Syst. I*, vol. 62, no. 2, pp. 478–487, 2015.

[6] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," *Proc. IEEE Int. Conf. Computers, Systems*

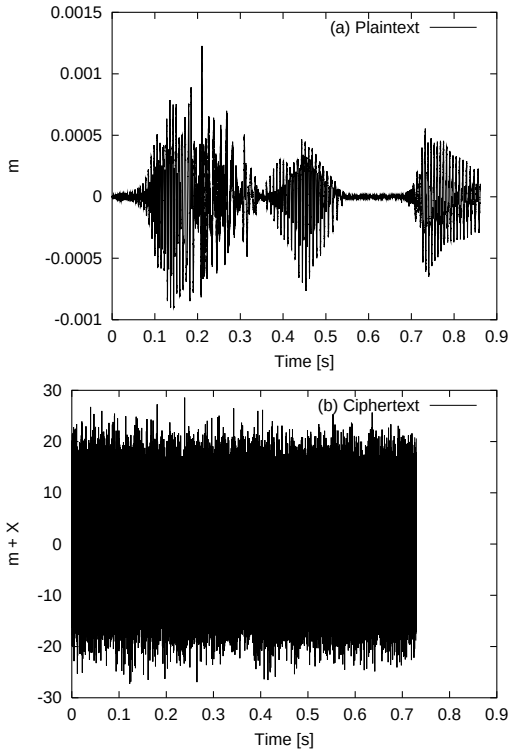

Figure 3: Time series of (a) the plaintext m ("Yes, we can.") and (b) the ciphertext $m + X$.

& Signal Processing (Bangalore, India), vol. 1, pp. 175–179, 1984.

[7] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, 1991.

[8] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, 2002.

[9] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, 2009.

[10] R. Wayland, D. Bromley, D. Pickett, and A. Passamante, "Recognizing determinism in a time series," *Phys. Rev. Lett.*, vol. 70, pp. 580–582, 1993.

[11] T. Miyano, "Time series analysis of complex dynamical behavior contaminated with observational noise," *Int. J. Bifurcation Chaos*, vol. 6, pp. 2031–2045, 1996.