International Journal of Power Control Signal and Computation(IJPCSC)
Vol 8. No.2 Pp.157-165

available at : www.ijcns.com
ISSN: 0976-268X

Encrypted Data Hiding in Cryptography Process using Keyless Algorithm

A.Ahila[1] and T. Bavithra Devi[2]
PG Student[1], Assistant Professor[2]
Department of Computer Science & Engineering
PRIST University
Thanjavur

Abstract
Securing data is a challenging issue in today's technology. Most of the data travel over the internet and it becomes difficult to make data secure. The information security has become one of the most significant problems in data communication. So it becomes an inseparable part of data communication. In order to address this problem, cryptography technique is used for data transmission to making data secure. There arises a need of data hiding. So here we are using a combination of steganography and cryptography for improving the security. All previous methods embed data by random vacating room from the encrypted images, which may be subject to some errors on data extraction and image restoration. In this paper, we propose a novel method by shuffling room in image pixels process before encryption with a traditional Keyless algorithm, and thus it is easy for the data hider to shuffling embed data in the encrypted image. The proposed method can achieve real data hidden in the image process, and it will take less time if the file size is large. The cryptography method can be applied for data encryption and decryption for sending confidential data.

Keywords: Encryption, Decryption, Data Hiding, Keyless, Algorithms

1.Introduction

The main feature of the encryption/decryption program implementation is the generation of the encryption key. Now a day, cryptography has many commercial applications. If we are protecting confidential information then cryptography is provide high level of privacy of individuals and groups. However, the main purpose of the cryptography is used not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation. Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. However, it is a very difficult to find out the specific algorithm, because we have already known that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity. In this technique I am using a random number for generating the initial key, where this key will use for encrypting the given source file using

proposed encryption algorithm with the help of encryption number. Basically In this technique a block based substitution method will use. In the present technique I will provide for encrypting message multiple times. The proposed key blocks contains all possible words comprising of number (n) of characters each generated from all characters whose ASCII code is from 0 to 255 in a random order. The pattern of the key blocks will depend on text key entered by the user. Our proposed system using 512 bit key size to encrypt a text message. It wills us very difficult to find out two same massages using this parameter. To decrypt any file one has to know exactly what the key blocks is and to find the random blocks theoretically one has to apply 2256 trial run and which is intractable. Initially that technique is only possible for some files. In the proposed technique we have a common keyless algorithm between sender and receiver, which is known as keyless algorithm. Basically private key concept is the symmetric key concepts where plain text is converting into encrypted text known as cipher text using private key where cipher text decrypted by same private key into plane text.

2. Existing System

In this framework, a content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider. The data hider can embed some auxiliary data into the encrypted image by randomly vacating some room according to a data hiding key. Then a receiver, may be the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key, But alone cryptography cannot provide a better security approach because the scrambled message is still available to the eavesdropper.

Disadvantages

- All previous methods embed data by randomly or reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration.
- It is difficult for data hider to reversibly hide the data behind the image.

3. Proposed System

Cryptography is the art of achieving security by encoding the data into unreadable form. Data that can be unreadable and not understood with difficulty is called encryption cryptography. Proposed process shuffling the data image pixels from the encrypted images is relatively difficult and sometimes inefficient, If we shuffling the order of encryption and vacating room prior to image encryption at content owner side with a traditional Keyless algorithm, and thus it is easy for the data hider to shuffling embed data in the encrypted image. Encrypted images would be more natural and much easier which leads us to the novel framework for secure data transmission.

Advantages

- In this system it uses traditional keyless algorithm, and thus it is easy for the data hider to shuffling embed data in the encrypted image.
- Using this system data extraction and image recovery are free of any error.
- Security enhancement in the cryptography.
- Efficiency in the encryption and decryption process.
- Very less computation process

4. Literature Survey

Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications

A circuit implementation of the chaotic Lorenz system is described. The chaotic behavior of the circuit closely matches the results predicted by numerical experiments. Using the concept of synchronized chaotic systems (SCS's), two possible approaches to secure communications are demonstrated with the Lorenz circuit implemented in both the transmitter and receiver. In the first approach, a chaotic masking signal is added at the transmitter to the message, and at the receiver, the masking is regenerated and subtracted from the received signal. The second approach utilizes modulation of the coefficients of the chaotic system in the transmitter and corresponding detection of synchronization error in the receiver to transmit binary-valued bit streams. The use of SCS's for communications relies on the robustness of the synchronization to perturbations in the drive signal. As a step toward further understanding the inherent robustness, we establish an analogy between synchronization in chaotic systems, nonlinear observers for deterministic systems, and state estimation in probabilistic systems. This analogy exists because SCS's can be viewed as performing the role of a nonlinear state space observer. To calibrate the robustness of the Lorenz SCS as a nonlinear state estimator, we compare the performance of the Lorenz SCS to an extended Kalman filter for providing state estimates when the measurement consists of a single noisy transmitter component.

A New Approach to Communications Using Chaotic Signals

In this paper, a new approach for communication using chaotic signals is presented. In this approach, the transmitter contains a chaotic oscillator with a parameter that is modulated by an information signal. The receiver consists of a synchronous chaotic subsystem augmented with a nonlinear filter for recovering the information signal. The general architecture is demonstrated for Lorenz and Rossler systems using numerical simulations. An electronic circuit implementation using Chua's circuit is also reported, which demonstrates the practicality of the approach.

Synchronization of Time-Delay Chua's Oscillator with Application to Secure Communication

In this paper, we use a Generalized Hamiltonian systems approach to synchronize the time-delay-feedback Chua's oscillator (hyperchaotic circuit with multiple positive Lyapunov exponents). Synchronization is thus between the transmitter and the receiver dynamics with the receiver being given by an observer. We apply this approach to transmit private analog and binary information signals in which the quality of the recovered signal is higher than in traditional observer techniques while the encoding remains potentially secure.

High bit rate optical communication systems based on chaotic carriers

In this thesis, the potential of using chaotic optical carriers generated by non-linear optical oscillators as an encryption medium of high bit rate pseudorandom sequences - and therefore their application in the development of an innovative platform of secure optical communications - is studied. The operation of chaotic semiconductor laser emitters capable of hiding data and their application within an emitter-receiver system is simulated, underlying the decoding process that leads to a successful message recovery. A complete high bit rate optical communication system based on chaotic carriers is developed, followed by a successful encoding and decoding process. We confirm that the insertion of 100 km conventional optical fiber for telecommunication applications, as the transmission medium, has a minimal effect for bit rates of the order of 1 Gb/s. For the very first time, this experiment is also performed in real-world conditions, using

an installed optical network of 120 km within the metropolitan area of Athens. The successful results are presented in a recent publication of the popular Nature magazine.

Electro-optic phase chaos systems with an internal variable and a digital key

We consider an electro-optic phase chaos system with two feedback loops organized in a parallel configuration such that the dynamics of one of the loops remains internal. We show that this configuration intrinsically conceals in the transmitted variable the internal delay times, which are critical for decoding. The scheme also allows for the inclusion, in a very efficient way, of a digital key generated as a long pseudorandom binary sequence. A single digital key can operate both in the internal and transmitted variables leading to a large sensitivity of the synchronization to a key-mismatch. The combination of intrinsic delay time concealment and digital key selectivity provides the basis for a large enhancement of the confidentiality in chaos-based communications.

Control of Chaos: Methods and Applications.

Reviewed were the problems and methods for control of chaos, which in the last decade was the subject of intensive studies. Consideration was given to their application in various scientific fields such as mechanics (control of pendulums, beams, plates, friction), physics (control of turbulence, lasers, chaos in plasma, and propagation of the dipole domains), chemistry, biology, ecology, economics, and medicine, as well as in various branches of engineering such as mechanical systems (control of vibroformers, microcantilevers, cranes, and vessels), spacecraft, electrical and electronic systems, communication systems, information systems, and chemical and processing industries (stirring of fluid flows and processing of free-flowing materials)).

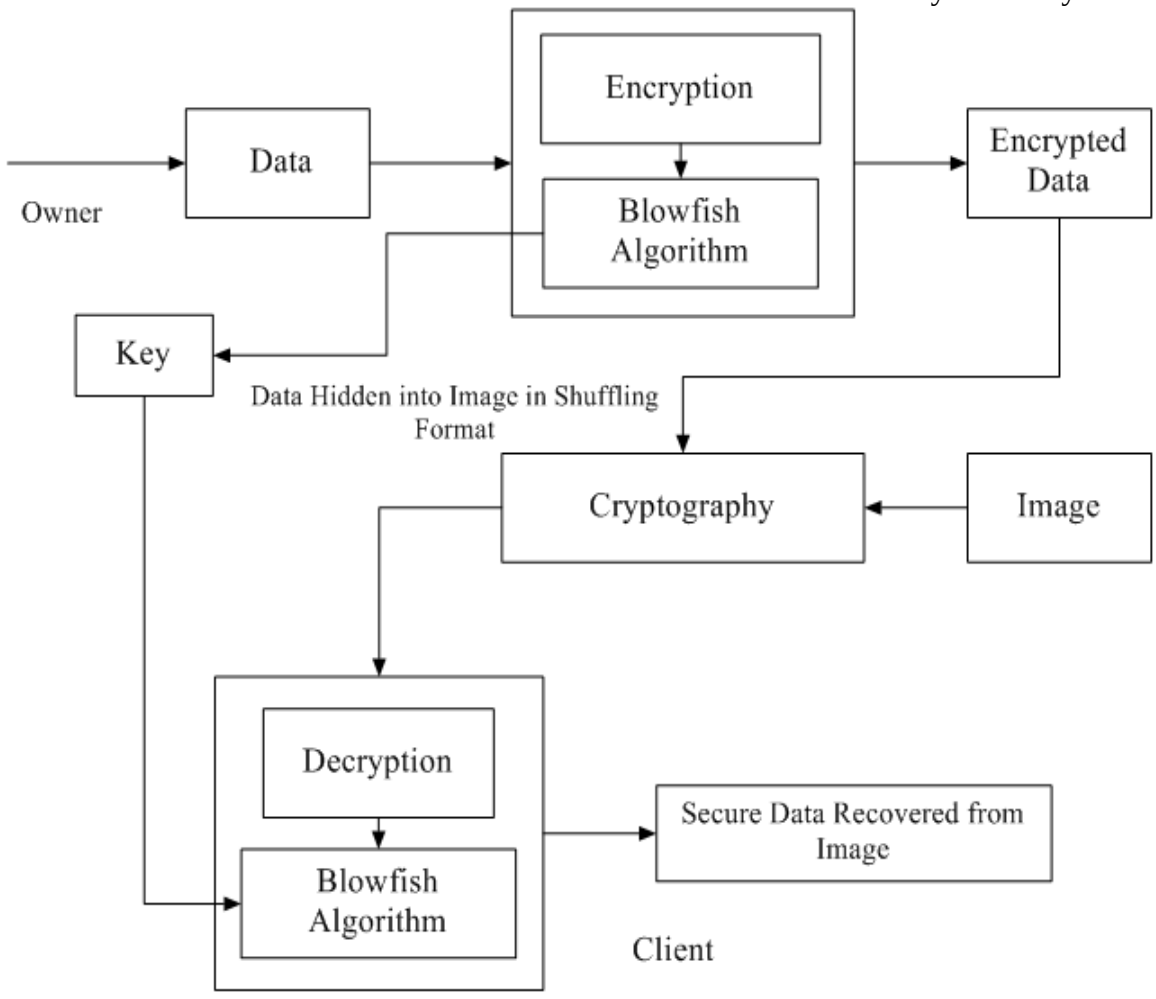
Synchronization and Control of Chaotic Systems. Spatio-Temporal Structures and Applications to Communications.

The field of dynamical systems and especially the study of chaotic systems has been considered as one of the important breakthroughs in science in this century. While this area is still relatively young, there is no question that it is becoming more and more important in a variety of scientific disciplines. Thus, this work starts with an historical overview about nonlinear dynamics and chaotic introduces the motivation for the results presented in the The first part of the present thesis devoted to the phenomenon of synchronization among coupled chaotic systems. This topic results very interesting since it could appear to be almost in contradiction with the definition of chaos which includes the rapid decorrelation of nearby orbits due to the instabilities throughout the phase space. In particular is devoted to show different categories of connections among identical chaotic systems that can lead to synchronized motions of the oscillators, and in we analyze the stability of the global synchronized state in open linear arrays or in rings of chaotic oscillators. We will also pay attention to some stable spatio-temporal structures (periodic rotating waves and chaotic rotating waves) that can arise when a instability appears in the global synchronized state of a ring of chaotic oscillators. The interaction between these structures when two rings are interconnected is investigated as well. Numerical simulations have been carried out with assemblies of Lorenz oscillators and Chua's oscillators, whereas experiments have been carried out in a board of Chua's oscillators. The second part of the thesis with possible applications of chaotic systems to the communications field. In we show some advantageous features that chaotic

behavior can incorporate to conventional digital communication systems and some different schemes that have already been proposed. In we introduce a simple control technique to encode binary sequences of information in a chaotic Lorenz waveform as well as two different methods to reconstruct damaged parts of this chaotic waveform when it is transmitted through a communication channel. Both methods exploit the redundancy provided V by the determinism of chaotic signals. Finally, it is shown how these reconstruction methods allow not only to reconstruct damaged parts of the transmitted signal but they can also be used to increase the rate of the information transmission by means of a time division multiplexing scheme. Finally, conclusions and outlooks of this work are presented.

Dynamics of coding in communicating with chaos

Recent work has considered the possibility of utilizing symbolic representations of controlled chaotic orbits for communicating with chaotically behaving signal generators. The success of this type of nonlinear digital communication scheme relies on partitioning the phase space properly so that a good symbolic dynamics can be defined. A central problem is then how to encode an arbitrary message into the wave form generated by the chaotic oscillator, based on the symbolic dynamics. We argue that, in general, a coding scheme for communication leads to, in the phase space, restricted chaotic trajectories that live on nonattracting chaotic saddles embedded in the chaotic attractor. The symbolic dynamics



of the chaotic saddle can be robust against noise when the saddle has large noise-resisting gaps covering the phase-space partition. Nevertheless, the topological entropy of such a chaotic saddle, or the channel capacity in utilizing the saddle for communication, is often less than that of the chaotic attractor. We present numerical evidences and theoretical analyses that indicate that the channel capacity associated with the chaotic saddle is generally a nonincreasing, devil's-staircase-like function of the noise-resisting strength. There is usually a range for the noise strength in which the channel capacity decreases only slightly from that of the chaotic attractor. The main conclusion is that nonlinear digital communication using chaos can yield a substantial channel capacity even in noisy environment.

Cryptographic requirements for chaotic secure communications

In recent years, a great amount of secure communications systems based on chaotic synchronization have been published. Most of the proposed schemes fail to explain a number of features of fundamental importance to all cryptosystems, such as implementation details, or key definition, characterization, and generation. As a consequence, the proposed ciphers are difficult to realize in practice with a reasonable degree of security. Likewise, they are seldom accompanied by a security analysis. Thus, it is hard for the reader to have a hint about their security and performance. In this work we provide a set of guidelines that every new cryptosystem would benefit from adhering to. The proposed guidelines address these two main gaps, i.e., correct key management and security analysis, among other topics, to help new cryptosystems be presented in a more rigorous cryptographic way. Also some recommendations are made regarding some practical aspects of communications, such as implementation, channel noise, limited bandwith, and attenuation.

Estimating generating partitions of chaotic systems by unstable periodic orbits

An outstanding problem in chaotic dynamics is to specify generating partitions for symbolic dynamics in dimensions larger than 1. It has been known that the infinite number of unstable periodic orbits embedded in the chaotic invariant set provides sufficient information for estimating the generating partition. Here we present a general, dimension-independent, and efficient approach for this task based on optimizing a set of proximity functions defined with respect to periodic orbits. Our algorithm allows us to obtain the approximate location of the generating partition for the Ikeda-Hammel-Jones-Moloney map.

5. Conclusion

Security in the Internet is improving. The increasing use of the Internet for commerce is improving the deployed technology to protect the financial transactions. Extension of the basic technologies to protect multicast communications is possible and can be expected to be deployed as multicast becomes more widespread. Control over routing remains the basic tool for controlling access based on the keyless algorithm. Implementing particular policies will be possible as multicast routing protocols improve. Cryptography is a tool which may alleviate many of the perceived problems of using the Internet for communications.

Reference

[1] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, no. 1, pp. 65–68, 1993.

[2] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process.*, vol. 40, pp. 626–633, 1993.

[3] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fisher, J. Garcia-Ojarvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, "Chaos-based communications at high bit rates using commercial fibreoptic links," *Nature*, vol. 437, pp. 343–346, 2005.

[4] H. Dedieu, M. Kennedy, and M. Hasler, "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process.*, vol. 40, pp. 634–642, 1993.

[5] S. Hayes, C. Grebogi, E. Ott, and A. Mark, "Experimental control of chaos for communications," *Phys. Rev. Lett.*, vol. 73, pp. 1781–1784, 1994.

[6] Y. Lai, E. Bolt, and C. Grebogi, "Communicating with chaos using two-dimensional symbolic dynamics," *Phys. Lett. A*, vol. 255, pp. 75–81, 1999.

[7] T. Miyano, K. Nishimura, and Y. Yoshida, "Chaos-based communications using open-plus-closed-loop control," *IEICE Trans. Fundam.*, vol. E94-A, pp. 282–289, 2011.

[8] R. Tenny, L. S. Tsimring, L. Larson, and H. D. I. Abarbanel, "Using distributed nonlinear dynamics for public key encryption," *Phys. Rev. Lett.*, vol. 90, pp. 047903-1–047903-4, 2003.

[9] R. Tenny and L. S. Tsimring, "Additive mixing modulation for public key encryption based on distributed dynamics," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 52, no. 3, pp. 672–679, 2005.

[10] L. Kocarev, M. Sterjev, A. Fekete, and G. Vattay, "Public-key encryption with chaos," *Chaos*, vol. 14, no. 4, pp. 1078–1082, 2004.

[11] N. Masuda, G. Jakimoski, K. Aihara, and L. Kocarev, "Chaotic block ciphers: From theory to practical algorithms," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 6, pp. 1341–1352, 2006.

[12] F. Anstett, G. Millerioux, and G. Bloch, "Chaotic cryptosystems: Cryptanalysis and Indentifiability," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 12, pp. 2673–2680, 2006.

[13] D. Arroyo, S. Li, C. Li, and V. Fernandez, "Cryptanalysis of a new chaotic cryptosystem based on ergodicity," *Int. J. Mod. Phys. B*, vol. 23, pp. 651–659, 2009.

[14] W. Xu, L. Wang, and G. Chen, "Performance analysis of the CS-DCSK/BPSK communication system," *IEEE Trans. Circuits Syst.I, Reg. Papers*, vol. 61, pp. 2624–2633, 2014.

[15] P. Muthukumar, P. Balasubramaniam, and K. Ratnavelu, "Synchronization and an application of a novel fractional order King Cobra chaotic system," *Chaos*, vol. 24, pp. 033105-1–033105-10, 2014.

[16] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, pp. 2129–2151, 2006.

[17] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, pp. 130–141, 1963.

[18] R. Barrio and S. Serrano, "A three-parametric study of the Lorenz model," *Physica D*, vol. 229, pp. 43–51, 2007.

[19] R. Barrio and S. Serrano, "Bounds for the chaotic region in the Lorenz model," *Physica D*, vol. 238, pp. 1615–1624, 2009.

[20] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–824, 1990.

[21] L. M. Pecora and T. L. Carroll, "Driving systems with chaotic signals," *Phys. Rev. A*, vol. 44, pp. 2374–2383, 1991.

[22] S. Camargo, R. L. Vianna, and C. Anteneodo, "Intermingled basin in coupled Lorenz systems," *Phys. Rev. E*, vol. 85, pp. 036207-1–036207-10, 2012.

[23] S. H. Strogatz, *Nonlinear Dynamics and Chaos*. Reading, MA, USA: Addison-Wesley, 1994, p. 9.
[24] M. Kolár and G. Gumbs, "Theory for the experimental observation of chaos in a rotating waterwheel," *Phys. Rev. A*, vol. 45, pp. 626–637, 1992.
[25] K. Cho, T. Miyano, and T. Toriyama, "Chaotic gas turbine subject to augmented Lorenz equations," *Phys. Rev. E*, vol. 86, pp. 036308- 1–036308-12, 2012.
[26] T. Miyano, K. Cho, Y. Okada, J. Tatsutani, and T. Toriyama, "Augmented Lorenz equations as physical model for chaotic gas turbine," *Procedia IUTAM (International Union of Theoretical and Applied Mechanics)*, vol. 5, pp. 99–107, 2012.
[27] Gas turbine video, [Online]. Available: http://www.ritsumei.ac.jp/se/
~tmiyano/waterwheel09_english.html
[28] J. J. Niemela, L. Skrbek, K. R. Sreenivasan, and R. J. Donnelly, "Turbulent convection at very high Rayleigh numbers," *Nature*, vol. 404, pp. 837–840, 2000.
[29] K. R. Sreenivasan, A. Bershadskii, and J. J. Niemela, "Mean wind and its reversal in thermal convection," *Phys. Rev. E*, vol. 65, pp. 056306- 1–056306-11, 2002.
[30] F. Fontenele Araujo, S. Grossmann, and D. Lohse, "Wind reversals in turbulent Rayleigh-Bénard convection," *Phys. Rev. Lett.*, vol. 95, pp. 084502-1–084502-4, 2005.
[31] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst., Signal Process.*, Bangalore, India, 1984, vol. 1, pp. 175–179.
[32] A. K. Ekert, "Quantum cryptography based o n Bell's theorem," *Phys.Rev. Lett.*, vol. 67, pp. 661–663, 1991.
[33] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, 2002.
[34] 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.
[35] A. Ekert and R. Renner, "The ultimate physical limits of privacy," *Nature*, vol. 507, pp. 443–447, 2014.
[36] A. Einstein, B. Podolski, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Phys. Rev.*, vol. 47, pp. 777–780, 1935.
[37] D. Bohm, *Quantum Theory*. New York: Prentice-Hall, 1951. [38] J. S. Bell, "On the problem of hidden variables in quantum mechanics," *Rev. Mod. Phys.*, vol. 38, pp. 447–452, 1966.
[39] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories,"*Phys. Rev. Lett.*, vol. 23, pp. 880–884, 1969.
[40] A. Aspect, P. Grangier, and G. Roger, "Experimental tests of realistic local theories via Bell's theorem," *Phys. Rev. Lett.*, vol. 47, pp. 460–463, 1981.
[41] D. Dieks, "Communication by EPR devices," *Phys. Lett.*, vol. 92A, pp. 271–272, 1982.
[42] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, 1982.
[43] K. Yoshimoto, K. Cho, Y. Morita, and T. Miyano, "Synchronization of coupled augmented Lorenz oscillators with parameter mismatch," *IEICE Nonlinear Theory Its Appl.*, vol. 4, pp. 341–350, 2013.
[44] G.-P. Jiang, W. K.-S. Tang, and G. Chen, "A simple global synchronization criterion for coupled chaotic systems," *Chaos, Solitons, Fractals*, vol. 15, pp. 925–935, 2003.
[45] M. Porfiri and F. Fiorilli, "Global stochastic synchronization of chaotic oscillators," in *Proc. Amer. Control Conf.*, 2008, pp. 511–516.
[46] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, pp. 644–654, 1976.

[47] R. L. Rivest, A. Shamir, and L. Adleman, "On a method for obtaining digital signatures and public key cryptosystems," *Commun. ACM*, vol. 2, pp. 120–126, 1978.

[48] L. B. Kish, "Totally secure classical communication utilizing Johnson (-like) noise and Kirchoff's law," *Phys. Lett. A*, vol. 352, pp. 178–182, 2006.

[49] L. B. Kish and C. G. Granqvist, "On the security of the Kirchoff-law- Johnson-noise (KLJN) communicator," *Quantum Inf. Process.*, vol. 13, pp. 2213–2219, 2014.

[50] P. W. Shor, "Polynomial-time algorithm for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, pp. 1484–1509, 1997.

[51] A. Bershadskii, "Chaos from turbulence: Stochastic-chaotic equilibrium in turbulent convection at high Rayleigh numbers," *Chaos*, vol. 20, pp. 043124-1–043124-5, 2010.

[52] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, "A step towards global key distribution," *Nature*, vol. 419, p. 450, 2002.

[53] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan,R. V. Penty, and A. J. Sharpe, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," *Phys. Rev. X*, vol. 2, pp. 041010-1–041010-8, 2012.

[54] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," *Nature*, vol. 501, pp. 69–73, 2013.

[55] T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," *Nature*, vol. 509, pp. 475–479, 2014.

[56] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, pp. 057901-1–057901-4, 2003.

[57] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, pp. 230503-1–230503-4, 2005.