Chaos-based Cryptography: A Brief Look Into An Alternate Approach to Data Security

Amer Sharif¹, Nur Intan Raihana², and Azman Samsudin³

¹Dept. of Computer Science, Faculty of Computer Science & Information Technology, University of Sumatera Utara, Jl. Alumni no. 9-A, Medan 20155, Indonesia
²,³School of Computing Sciences, University of Science Malaysia, 11800 Pulau Pinang, Malaysia

Email: amer.sharif@usu.ac.id

Abstract. The present scale of computing inevitably demanded increased level of data security, which is the concern of cryptography. Security of the cipher depends on the strength of the key and the algorithm used to generate the keys. Many modern cryptographic algorithms are based on Number Theory, but in recent years the alternative approach has been studied which is based on Chaos Theory. Many properties of chaotic systems such as nonlinearity, randomness, and sensitivity to initial conditions bear resemblance to those required by cryptography such as diffusion and confusion. Implementations of chaos-based cryptosystems have been proposed by other researchers and yet the strength of these systems from cryptographic point of view has not been thoroughly considered. This paper discusses the appeal of chaos-based cryptography, some of the researches already done, and the challenges that this approach faces to be established as a fully secure method for data security.

1. Introduction

Cryptography is concerned with securing data, whether during transmission or at rest. Security (i.e. confidentiality) is achieved by encryption, which is transforming original data (plaintext) into an unintelligible form (ciphertext) by means of a cryptographic algorithm and a particular data (key). This ciphertext is thus transmitted or stored. To transform ciphertext back into plaintext, the intended or authorized receiver performs decryption by means of the same cryptographic algorithm and the same private key (symmetric cryptography) or using different (private) but related to the initial public key (asymmetric cryptography).

There are many cryptographic algorithms, long since the classical era up to today’s modern times. Many of the modern cryptographic algorithms were developed by utilizing Number Theory or some algebraic concepts as [7] pointed out. Cryptographic algorithm must satisfy some basic requirements to be considered as secure, among which are confusion and diffusion [10]. Confusion refers to making the relationship between key and ciphertext as complex as possible, while diffusion scatters the statistical structure of the plaintext over the ciphertext. Confusion resulted in any small change in the key must result in a major change of the ciphertext; while diffusion demands any small change in the plaintext must cause huge and nonlinear changes in the ciphertext. These requirements indicate high sensitivity of the ciphertext as output in relation to input, namely the plaintext and the key.
2. Chaos theory
Chaos theory has a root in mathematical science and focuses on the behavior of dynamic systems that are highly sensitive to initial conditions [5]. Chaos phenomena in nature include weather, stock market, and earthquakes.

Chaos theory gained its popularity when in 1960 meteorologist Lorenz repeated a weather simulation using previously obtained data and obtained highly different results compared to the previous simulation run [9]. The difference in simulation outcome was caused by a difference of 0.000127 in the second run input. This indicated that chaotic systems have a high sensitivity to initial conditions: the slightest change in input will result in a dramatic change in the output, making long-term predictability impossible.

Another appealing chaotic characteristic is ergodicity, in which the trajectory in phase space eventually returns arbitrarily close (but never the same) to its initial states. The trajectory forms an attractor, where in Lorenz simulation has the shape similar to that of a butterfly wings. Hence perhaps the popular nickname of the theory, the butterfly effect.

Ergodicity also indicated that chaotic systems are not entirely random, as the term chaos suggested. The (pseudo) random output resulted from the slightest variation in input somehow demonstrates some subtle regularities, as shown in the trajectory attractor [7].

3. Cryptography and Chaos Theory
There are strong similarities between Chaos Theory and requirements for cryptographic algorithms, as listed by [1]

| Chaotic Property                          | Cryptographic Property                  | Remarks                                           |
|------------------------------------------|-----------------------------------------|--------------------------------------------------|
| Sensitivity to initial parameters        | Confusion & Diffusion in key and/or plaintext | Any small change in the input resulted in major change in the output |
| Ergodicity                               | Confusion                               | Input is equally distributed over the output      |
| Deterministic dynamics                   | Deterministic pseudo randomness          | Pseudo-random behaviour resulted from deterministic process |
| Mixing                                   | Diffusion                               | Small local change may cause a large change in overall output |

These similarities made chaos an appealing alternative as basis for cryptographic algorithms.

There have been many researches proposing chaos-based cryptography in recent years. From the literature, the chaos-based cryptographic implementations can be generally divided into two classes:
analog-based and digital-based. The analog approach is built upon the concept of chaos synchronization put forward by [8] where the transmitter and receiver synchronize chaotic signals used for communication. A number of researches in this area were mentioned in [1] as well as in [13] which utilizes a nonlinear function for encryption & decryption; [6] proposes a synchronization based chaotic keystream & modulation; [12] implemented a Lorenz-like system to encrypt speech; [3] discussed some chaos-based techniques to improve security in wireless communication; [4] proposed image encryption using Lorenz-like system with varying parameters; Belkhouja wrote a paper on securing Implantable/Wearable Medical Devices (IMD/WMD) using synchronized chaotic Henon Map.

Digital-based chaos cryptography utilizes chaotic maps to encrypt the plaintext, as several researches indicated in [1]. An alternate approach by [2] secured TCP data packet using keystream from a chaos-based PRNG. [11] conducted an extensive literature and comparison survey on 62 researches where chaos-based cryptography were utilized for security in many areas of application; parameters being compared included Security, Cipher Type, Application Area, Space Complexity, Efficiency, Speed, Key Length, Cost, Accuracy [11]. The comparison is extensive but failed to mention in detail the method used for measuring each parameter.

4. Suitability of chaos-based cryptography approaches

All the above mentioned papers indicated that chaos-based cryptography has appealed to many researchers and may prove to be a feasible alternate approach to data security. Although the researchers reported satisfactory results in their papers, many did not discuss in detail the implementation and security level from the cryptographic point of view. As mentioned in [1] these may present problems in adopting a particular chaos-based cryptography system.

[1] therefore suggested 17 Rules as guideline in implementing chaos-based algorithms to meet acceptable cryptographic standards. These guidelines cover the following areas:

- Implementation (details, cost, simplicity, speed)
- Key (definition, space, avalanche effect, generation)
- Security (resistance to statistical analysis)
- Strength as in resistance to:
  - Cryptographic attacks such as known-plaintext, chosen-plaintext or chosen-ciphertext attacks, and differential and linear cryptanalysis
  - Chaos-specific attacks (such as message extraction, chaotic signal extraction, and parameter estimation)
  - Application-specific attacks (such as toward image data)
  - Brute-force attacks
- Statistical properties of the PRNG

The above mentioned guidelines by [1] may serve as basis to determine the security of a chaos-based system from cryptographic standards.

5. Conclusion

Chaos theory demonstrated a lot of similarity in properties to cryptography which made it appealing to serve as an approach to developing novel cryptography systems. This has been demonstrated by a significant number of researches in the past years. Cryptographic implementation based on chaos theory may be categorized into analog-based and digital-based. The analog approach are mostly based on synchronization principles laid out by [8]. However in many of the researches some aspects still need to be explored further to determine its suitability and security from cryptographic standards. To this end, [1] have suggested some guidelines in determining how suitable the suggested chaos-based approach
from a cryptographic point of view. Observing these guidelines may prove substantial in building a better and more secure chaos-based cryptography system.

References

[1] Alvarez, G. Li, S. "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems", *Int. J. Bifurc. Chaos* 2006; 16 (8): 2129-2151.

[2] Çavusoglu, U. Akgül, A. Kaçar, S. Pehlivans, I. Zengin, A. "A Novel Chaos-Based Encryption Algorithm Over Tcp Data Packet For Secure Communication". *Security Comm. Networks* 2016, 9:1285–1296. John Wiley & Sons

[3] Haroun, M. "Secure Communications based on Chaotic Systems". Ph.D dissertation in Dept. of Electrical and Computer Engineering. University of Victoria 2015

[4] Huang, L. Shi, D. Gao, J. "The Design and Its Application in Secure Communication and Image Encryption of a New Lorenz-Like System with Varying Parameter". *Math. Problems in Eng.* 2016; Hindawi Publishing Corporation

[5] Kattan, P.I. "Chaos Theory Simply Explained (Basic Fractals/Chaos Series)". Petra Books, 2012.

[6] Kharel, R. Busawon, K. Ghassemlooy, Z. "A Novel Chaotic Encryption Technique for Secure Communication". *2nd IFAC Conference on Analysis and Control of Chaotic Systems (CHAOS 09)* 2009; Northumbria Research Link (http://nrl.northumbria.ac.uk/1278/)

[7] Lawande, Q.V. Ivan, B. R. Dhodapkar, S.D. "Chaos Based Cryptography: A New Approach to Secure Communications". *BARC Newsletter* 2005; 258:1-12

[8] Pecora, L. M. Carroll, T. L. [1990] “Synchronization in Chaotic Systems”. *Phys. Rev. Lett.* 1990; 64(8): 821–824.

[9] Poe, H. L. Davis, J. H. “Science and Faith: An Evangelical Dialogue”. Broadman and Holman Publishers: Nashville Tennessee, 2000.

[10] Shanon, C. “Communication Theory of Secrecy Systems,” *Bell Sys. Tech. J.* 1949; 28: 656–715.

[11] Shukla, P. K. Khare, A. Rizvi, M. A. Stalin, S. Kumar, S. "Applied Cryptography Using Chaos Function for Fast Digital Logic-Based Systems in Ubiquitous Computing", *Entropy* 2015, 17: 1387-1410

[12] Ye, F. Zhou, J. Luo, J. Gao, X. "The Secure Communication Technique Based on Lorenz Chaos System", *2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013)*, 2013

[13] Zaher, A.A. "A New Secure Communication Technique Using A Novel Chaos-Based Nonlinear Cryptography Function", *16th European Signal Processing Conference (EUSIPCO 2008)*, EURASIP, 2008