IMPROVING CHAOTIC CRYPTOGRAPHIC PRIMITIVES BASED ON MAP'S COMPLEXITY AND PERIOD LENGTH OF THE CHAOTIC MAPS

AMIR AKHAVAN MASOUMI

UNIVERSITI SAINS MALAYSIA

2015

IMPROVING CHAOTIC CRYPTOGRAPHIC PRIMITIVES BASED ON MAP'S COMPLEXITY AND PERIOD LENGTH OF THE CHAOTIC MAPS

by

AMIR AKHAVAN MASOUMI

Thesis submitted in fulfillment of the

requirements for the degree of

Doctor of Philosophy

AUGUST 2015

ACKNOWLEDGEMENTS

First and foremost, I would like to express my sincere gratitude to my dear supervisor Prof. Dr. Azman Samsudin for the continuous support of my study and research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I am short in word to express his contribution to this thesis, with criticism, suggestions and discussions. I could not have imagined having a better supervisor and mentor for my Ph.D. study. I would like to make grateful acknowledgement to the Dean and all staff members of the School of Computer Sciences, USM. Indeed, I am fortunate to be surrounded by kind and helpful staff. There is no word to express my deep feeling to my lovely parents, sister and wife for their strong cooperation and inspirations. I am greatly thankful to God, that I am so much fortunate to have all good things together.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Pages

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
CCM	Combination of Chaotic Maps
DES	Data Encryption Standard (Name of a block cipher algorithm)
CCA	Chosen Ciphertext Attack
HPCM	Higher Precision realization of Chaotic Maps
IEEE	Institute of Electrical and Electronics Engineers
KS	Kolmogorov-Sinai, a type of entropy
LMC	López-Ruiz, Mancini and Calbet complexity measure
MAD	Mean of Absolute Difference
MD5	Message Digest Five
NIST	National Institute of Standards and Technology
NPCR	Number of Pixels Change Rate
NSA	National Security Agency
PRNG	Pseudo Random Number Generator
PWLCM	Piecewise Linear Chaotic Map
PWNLCM	Piecewise Nonlinear Chaotic Map
RC6	Rivest Cipher 6, is a symmetric key block cipher
RSA	Public-key encryption algorithm
SAD	Sum of Absolute difference

SHA	Secure Hash Algorithm (Name of a hash algorithm)
UACI	Unified Average Changing Intensity
USM	Universiti Sains Malaysia

MENINGKATKAN MUTU PRIMITIF KRIPTOGRAFI PETA CAMUK BERDASARKAN KERUMITAN DAN TEMPOH PANJANG PETA

ABSTRAK

Peta camuk berkentuan menghasilkan ciri-ciri seperti determinisme, ergodisiti, perlakuan seperti rawak, ketidaklineran, aperiodisiti, entropi yang tinggi, imbangan, ketak kemerostan, korelasi maklumat yang amat rendah, dan kepekaan/kesensitifan yang amat tinggi terhadap perubahan yang amat kecil daripada keadaan awal dan parameter kawalan. Ciri-ciri ini amat sesuai untuk bidang kriptografi dan menjadikan peta camuk menarik bagi mereka bentuk primitif kriprografi. Berdasarkan ciri-ciri tersebut, sejak beberapa tahun kebelakangan ini, banyak peta camuk berdasarkan primitif kriptografi dicadangkan. Namun demikian, kebanyakannya didapati tidak begitu memuaskan atau mempunyai kekurangan seperti ruang kunci yang amat pendek, keberkesanan dan kelajuan yang rendah, kekuatannya yang tidak begitu baik serta sekuriti yang rendah. Justeru, kajian ini cuba mengkaji kekurangan tersebut dan keadaan awal, parameter kawalan dan trajektori sistem camuk digunakan dalam algoritma kriptografi berasaskan peta camuk dianalisis. Daripada hasil analisis, tiga kaedah baru bagi mereka bentuk primitif kriptografi berdasarkan peta camuk dicadangkan. Dalam usaha mengkaji kecekapan kaedah ini, satu set primitif kriptografi berasaskan peta camuk dicadangkan dengan menggunakan setiap kaedah tersebut. Kaedah pertama adalah aplikasi peta camuk berdimensi tinggi, di mana dimensinya adalah tiga dan ke atas. Kaedah kedua adalah berdasarkan kepada gabungan dua atau lebih peta camuk. Kaedah ini memanipulasi komposisi dua peta camuk untuk menjana satu peta camuk baru dengan ciri-ciri fizikal yang lebih baik dengan kerumitan statistik yang lebih tinggi. Dalam kaedah ketiga, merealisasikan peta camuk dalam ketepatan yang lebih tinggi adalah dicadangkan. Pada kebiasaanya, peta camuk direalisasikan dengan menggunakan ketepatan 32-bit hingga 64-bit, tetapi kaedah ini menggunakan ketepatan yang lebih tinggi (1024-bit hingga 2048-bit). Dalam usaha untuk menyiasat keselamatan dan kecekapan kaedah ketiga, primitif kriptografi berasaskan peta camuk (fungsi cincang, penyulitan imej dan penjanaan nombor pseudo-rawak) direka

berdasarkan ketepatan yang lebih tinggi pada peta camuk yang digunakan. Sekuriti algoritma yang dicadangkan dikaji menggunakan pelbagai jenis tekanan dan ujian sekuriti statistik biasa. Dapatan menunjukkan bahawa algoritma yang terhasil boleh memenuhi keperluan tahap sekuriti yang tinggi dengan halaju yang tinggi dan kos pengiraan yang rendah. Oleh itu, hasil kajian tesis ini menunjukkan bahawa peta serabut dengan cadangan penambahbaikan yang diutarakan boleh digunakan untuk aplikasi kriptografi dalam kehidupan sebenar.

IMPROVING CHAOTIC CRYPTOGRAPHIC PRIMITIVES BASED ON MAP'S COMPLEXITY AND PERIOD LENGTH OF THE CHAOTIC MAPS

ABSTRACT

Deterministic chaotic maps possess profound characteristics such as determinism, ergodicity, random-like behavior, nonlinearity, aperiodicity, high entropy, balance, nondegeneracy, incredibly low correlation of information and extreme sensitivity to very small changes of the initial condition and control-parameters. These characteristics are very favorable for cryptography and make deterministic chaos an interesting candidate in designing of cryptographic primitives. Based on these characteristics, during the recent years many chaos-based cryptographic primitives have been proposed. Unfortunately, a vast portion of them had encountered drawbacks such as shortened key space, low speed, lack of robustness and low security. In this study, these drawbacks are studied and the initial conditions, control-parameters and trajectories of the chaotic systems used in the chaos-based cryptography algorithms are analyzed. Three new methods for the design of chaos-based cryptographic primitives are suggested based on the results of the analysis. In order to study the efficiency of these methods, a set of chaos-based cryptographic primitives are proposed. The first method is the application of higher dimensional chaotic maps, the dimension can be three and above. The second method is based on the combination of two or more chaotic maps. It manipulates the composition of two chaotic maps to achieve to a new chaotic map with physically better characteristics and higher statistical complexity. In the third method, realization of the chaotic maps in higher precision is proposed. Regularly, the chaotic maps are realized using 32-bit to 64-bit precision, whereas this method takes advantage of higher precision (1024-bit to 2048-bit). In order to investigate the security and efficiency of the third method, chaos-based cryptographic primitives (hash function, image encryption and pseudo random number generator) are designed based on the higher precision realization of the chaotic maps. The security of the proposed algorithms is examined

using different types of attacks and common statistical security tests. The results of the cryptanalysis indicate that the presented algorithms satisfy the requirements for a secure system. Therefore, the findings in this thesis indicate that chaotic maps with suggested improvements can be used for real life cryptography applications.

CHAPTER 1: INTRODUCTION

The study of chaotic systems and their application in cryptography has been an interesting subject for the researchers in computer science and physics. In the past two decades plenty of new algorithms, based on different sorts of chaotic maps have been proposed. Most of the algorithms rely on the sensitivity of the chaotic systems to their initial condition and control-parameters. Meanwhile, many of the presented algorithms had been cryptanalyzed and found to be vulnerable against different attacks, either because of dynamical behavior of the chaotic systems used in their structure or because of inefficient utilization of the dynamical system. Besides security problems, many of these algorithms suffer from low speed, high cost of computation and are difficult to implement in real life application.

In this study, the main goal is to find subtle points in the design of a chaos-based cryptographic algorithm using the existing literature and by trying to propose efficient strategies in order to achieve secure and practical algorithms. The study of the literature, suggested three different approaches in designing of secure chaos-based crypto-primitives. The proposed strategies in this work should be studied from both dynamics and security point of view. In order to study dynamical behaviors of chaotic systems, along with regular methods (such as Lyapunov exponent, phase space control, and Bifurcation diagram) an alternative test such as complexity, period length and transient effect analysis are applied. The new cryptographic primitives are designed based on each of these approaches, and the security of the new proposed algorithms are tested against known attacks. The test results are compared with the existing cryptographic algorithms, from security, speed and applicability aspects.

1.1 Motivation

With the fast growth of the Internet in the early years of twenty-first millennium, majority of the people started using internet in their daily lives. The demand for the new image encryption algorithms, with better performance on the bulk data lead to several studies on the design of more secure and flexible image encryption algorithms. Nonetheless, Chaos based image encryption algorithms provide good confusion and diffusion on the bulk data. Therefore, they became an interesting alternatives option for the image encryption purposes. The similarities between nonlinear dynamical systems, namely chaos, and the cryptographic systems have made chaos a natural candidate for designing cryptographic algorithms [1]. During the past few decades dozens of new chaos-based both symmetric [2]–[39] and asymmetric [40]–[54] algorithms have been proposed and several novel view points towards the issue has been suggested. However, there has been plenty of failures and drawbacks in the proposed chaos-based designs [55]–[79].

Moreover, bibliometric statistics, along with a review of the literature imply that there have been many chaos-based algorithms, either symmetric or asymmetric found to be weak against different types of attacks. Security of the chaos-based cryptographic systems, mostly rely on the possibility of recovering initial condition or control-parameters and consequently the information available from the ongoing chaotic orbit. In deterministic chaotic systems, discovering the current state of the system can help finding all the following states.

In many of the cryptanalyzed cases, there exist particular repeated patterns in the design and implementation of chaos-based cryptographic algorithm that are responsible for the security flaws. If these patterns refrained, cryptographic algorithms would be more secure against different types of known attacks. The modified Baptista type algorithm [80] is a good example, which was proposed in order to improve the security of the original Baptista type cryptosystem [81]. Thus,

by identifying the common problems and the corresponding reinforcement it is feasible that chaos cryptography remain as one of the main parts in modern cryptography.

1.2 Problem Statement

Since the mid-nineties, application of chaos in cryptography has attracted many researchers. The similarities between chaos and cryptography such as sensitivity to initial conditions and control-parameters have made chaos a good choice for designing new cryptographic primitives. Nonetheless, many of the presented chaos-based cryptographic algorithms have been cryptanalyzed and proved weak against different types of differential and statistical attacks [39], [55]–[77], [82]–[110]. The main weaknesses of these algorithms were consequence of several issues such as:

- Unexpected short period length of the digitalized discrete nonlinear chaotic systems in finite space [85].
- Low sensitivity of the chaotic maps to the changes of initial conditions and control-parameters in some areas of the phase space and control-parameter chaotic range [76].
- Unsecure and inefficient design of the existing chaos-based cryptographic algorithms [67], including careless implementation [39], lack of knowledge about the strange attractor's behavior [69] and slow speed of the chaos-based algorithms [111].

In order to resolve these issues, several strategies are proposed in the past decade, but most of these strategies were only suggestions and prescriptions and have rarely been applied in practice on cryptographic primitives, thus it is very hard to provide any comparison between them. In this study, in order to tackle the problems mentioned above, three strategies based on appropriate chaotic systems are suggested and their dynamical characteristics are carefully analyzed under the finite precision implementation. Based on each of these strategies, three chaos-based cryptographic primitives are carefully designed. Moreover, the security of each of the algorithms

is analyzed against statistical and differential attacks. The security analysis, speed and flexibility of each of the algorithms are compared to conclude the effectiveness study of each of the algorithms.

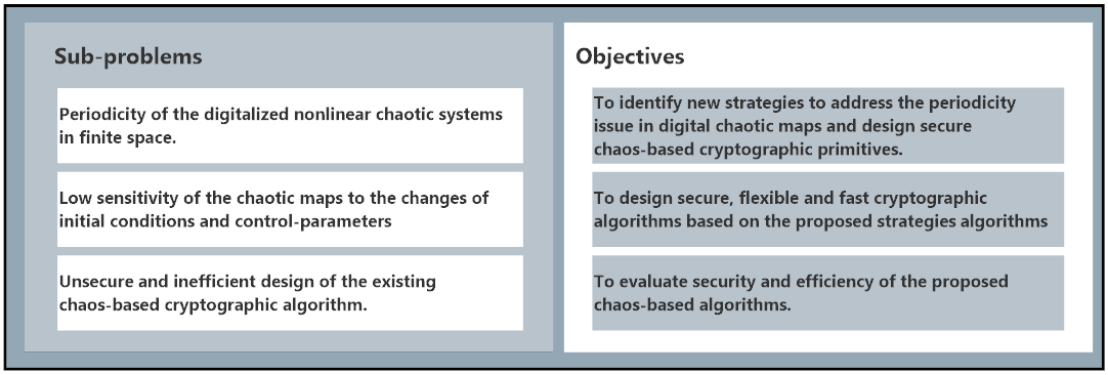

Figure 1.1: Sub-problems and Research Objectives

1.3 Research Objectives

According to the problem statement, the security, flexibility and speed of the chaos-based algorithms need to be improved. However, the proposed strategies and prescriptions in the past have not been applied in the newly proposed algorithms [4], [33], [39], [94], [112]. The main objective of this research is to propose strategies and design new cryptographic primitives based on each of the proposed strategies to improve the effectiveness, security, speed and flexibility of the chaos-based cryptographic algorithms. The objectives of this thesis can be categorized as below (Figure 1.1):

- To identify strategies to address the periodicity issue in digital chaotic maps.
- To design secure, flexible and fast cryptographic algorithms based on the proposed strategies.
- To evaluate security and efficiency of the proposed chaos-based algorithms.

1.4 Research Scope

The main scope of this study is to suggest strategies to improve the security of symmetric chaos-based cryptographic algorithms. In order to achieve this initial step is to find and investigate cryptanalyzed chaos-based cryptographic algorithms proposed in the past two decades. The investigation in this study mainly focuses on the discrete chaotic maps (unimodal, one dimensional, coupled map lattice and hyperchaotic maps, higher dimensional maps and finally quantum chaotic maps).

In order to investigate adequacy and efficiency of the proposed strategies, new chaos-based cryptographic primitives following the suggested strategies are designed. The proposed algorithms are under the category of hierarchy of polynomial chaotic maps (one dimensional, coupled map and 3D chaotic maps). The asymmetric cryptographic algorithms, stream ciphers, watermarking and steganography are not in the scope of this study. Meanwhile only Tent map and a class of hierarchy of polynomial chaotic maps are used in the structure of the proposed algorithms and other chaotic maps are not in the scope of this research.

1.5 Research Methodology

The methodology used in this research is conducted by finding the evidence available in the literature and analyzing the existing data in order to achieve the expected results such as design of new cryptographic algorithms with higher capabilities and faster operation time. The literature review consists of few major sections, such as identifying major literature from the main publishers and famous authors, tracking down, storing and reviewing all the closely related documents to the topic/scope.

According to the reviewed literature, groups and categories from the chaos-based cryptographic algorithms with the same concepts are categorized. Moreover, the problems and drawbacks of each category is listed. In order to overcome the problems and eliminate the

drawbacks, new strategies are proposed. According to the objectives of this study, the proposed methods are applied in order to design new chaos-based cryptographic algorithms. Finally, the security and efficiency of the proposed chaos-based cryptosystems are analyzed and the results of the analysis are compared with other chaotic and conventional cryptographic algorithms. Figure 1.2 provides an overview of the steps of the research. The major steps in deciding the strategies are based on the following issues:

- Selecting and modifying chaotic maps to fit the requirements of a highly sensitive chaotic map with long period length.
- Study the effect of realization of the chaotic maps in finite precision.
- Analyze the dynamical behaviour of the chaotic maps with respect to the evolution of the trajectories.
- Design new algorithms based on the structure and characteristic of the chaotic maps.
- Design experiments to investigate statistical characteristics and speed of the proposed algorithms.
- Design experiments to analyze security of the algorithms against different types of attacks.

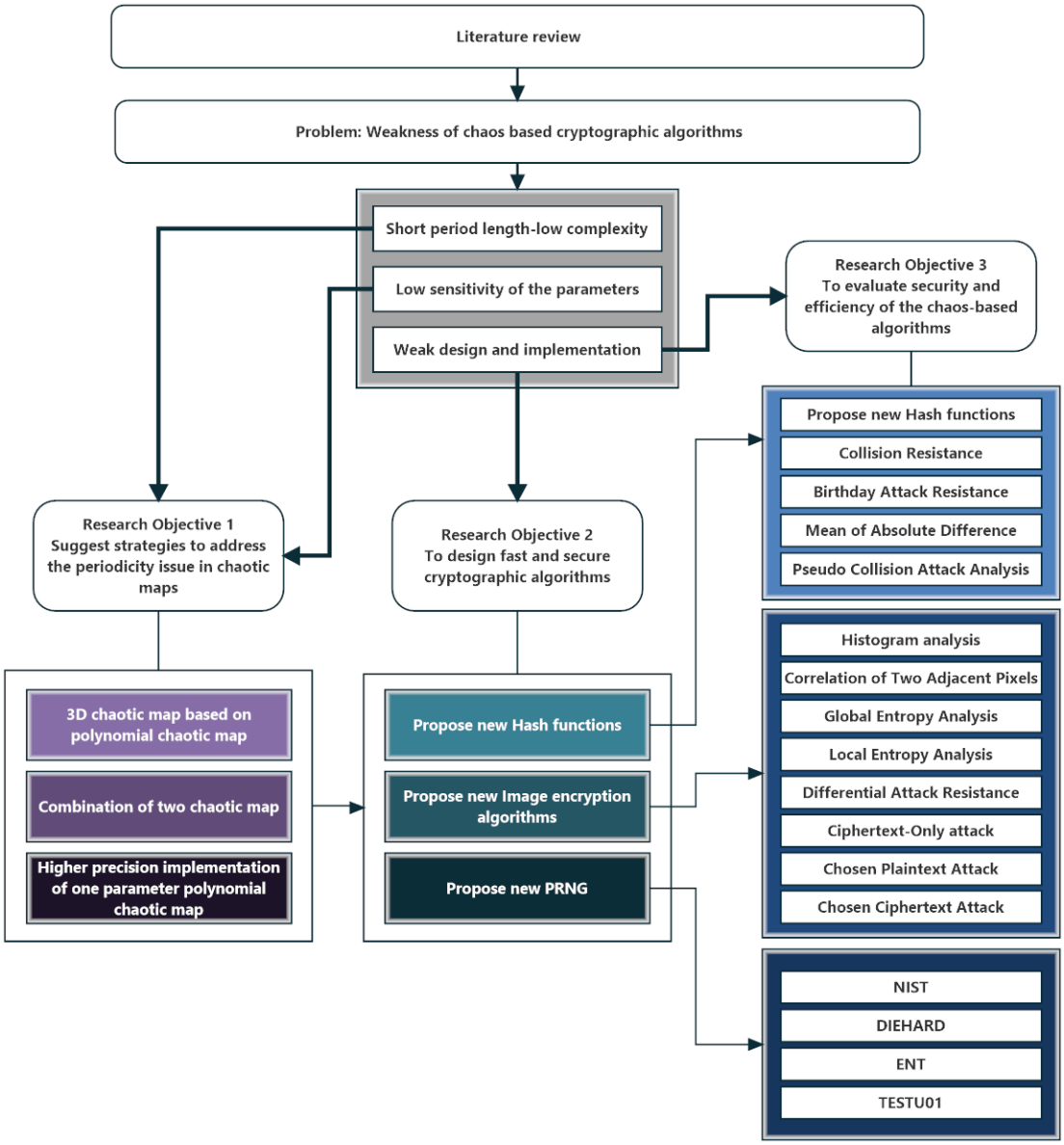

Figure 1.2: Framework of the study

1.6 Research Contribution

In the process to achieve the objectives of the thesis, three major contributions are made. The main contribution of this thesis is design of new chaos-based cryptographic primitive based on the suggested strategies. The algorithms can be categorized as below:

1) Application of higher dimensional chaotic maps in cryptography:

- Parallel hash function on application of higher dimensional chaotic maps
- Image encryption algorithm based on application of higher dimensional chaotic maps
- Pseudo random number generator (PRNG) based on application of higher dimensional chaotic maps

2) Application of combinational chaotic maps in cryptography:

- Hash function based on application of combinational chaotic maps
- Image encryption algorithm based on application of combinational chaotic maps
- PRNG based on application of combinational chaotic maps

3) High precision realization of one-dimensional polynomial chaotic maps:

- Parallel hash function based on application of higher precision realization of chaotic maps
- Image encryption algorithm based on application of higher precision realization of chaotic maps
- PRNG based on application of higher precision realization of chaotic maps

There are new original methods applied in each of the algorithms in order to achieve speed and flexibility along with the security, which will be described in detail in the following chapters.

1.7 Outline of the Thesis

The presented thesis is organized in seven chapters. The outline of each of the chapters can be described as below:

Chapter 1 provides a brief decription about the concepts, problems, objectives and the contributions of the research. Chapter 2 reviews the related literature and presents a description about the concepts and tools used in this research. Chapter 3 provides a review of methods used in designing of the cryptographic algorithms. Chapter 4 studies the characteristics of the chaotic

maps applied in this study. Meanwhile, in this chapter the following issues are discussed: the transient effect, precision change effect and sensitivity to intial conditions and also contorl parameters. In addition, a new combinational chaotic map is proposed in this chapter. Chapter 5 discusses the application of higher dimensional chaotic maps, newly generated combinational chaotic map and higher precision implementation of the hierarchy of polynomial chaotic maps. This chapter also provides details about designing and analysis of three cryptographic primitives based on each strategy. Moreover, several tests and details are presented for the security and speed analysis of each of the proposed algorithms. Chapter 6 provides a discussion on the research results. In this chapter the security and speed of the proposed algorithms in the previous chapters are pointed out. Chapter 7 presents the summary, conclusion and future work of this study.

CHAPTER 2: BACKGROUND AND LITERATURE REVIEW

2.1 Introduction

Cryptography has an ancient history, which can go as far as Ancient Egypt [113]. This offers the idea that the desire for concealing writings has been a demand for thousands of years. With the fast improvement in the information technology and emergence and rapid growth of the internet, the demand for secure communication increased dramatically. Thus, design of faster and more secure algorithms gained extra importance. Therefore, numerous new algorithms were developed in a short span and chaos-based cryptography was one of the most controversial methods suggested in the meantime.

Chaos-based cryptography is a relatively new field of study. However, it has been a very active field during the past two decades according to the bibliometric information. Chaos and cryptography are very similar to each other. Both conventional methods of cryptography and chaos-based cryptographic algorithms are in favor of the maximum possible entropy [114]. Chaotic maps in most of the scenarios of chaos-based cryptography algorithms are considered as means of providing confusion and diffusion [115]. The unpredictable and random like behavior of the chaotic systems along with their strong sensitivity to changes in the control-parameters and initial conditions makes them very interesting candidates for the purpose of cryptography.

2.2 Cryptographic Algorithms

In general, in order to provide a secure communication between two parties on two sides of a channel (usually called as Alice and Bob), the message has to be converted, concealed or modified (i.e.: scrambled, transformed or permutated). This operation should be carried out in such a way that a third party in the middle (Eve or Eavesdropper) cannot find access to the content of the information or modify it without receiver noticing it. According to the Kerckhoffs's

principle, the man in the middle should not be able to recover the message even if he has access to the ciphering and deciphering algorithms [116].

Cryptology, on the other hand, is the science of information security and privacy. It deals with both selection of the tools and methods for concealing information and also evaluation of the achieved encryption systems [114]. The first stage of cryptology, which deals with selecting suitable methods and frameworks, is called *cryptography*. The term *cryptography* is taken from the Greek language, meaning "secret writing" and the second stage concentrates on the security of the proposed methods (*the cryptanalysis*).

Cryptographic algorithms can also be divided into several groups based on their concept of the work and demands. The first group and perhaps most used method is *encryption algorithm*, which are designed to cipher message in one side so that the other party can decipher it. The second group is called *one-way hash function.* Hash function, practically acts like a compression algorithm, while the compressed information cannot be retrieved anymore. In this study, the term hash function is used as MAC (Message Authentication Code).

2.2.1 Hash Functions

Hash functions are commonly used for information integrity, message authentication and storing sensitive information in databases such as usernames and passwords. A hash function should have several key characteristics, while weakness in any of them can lead to an unsecure design and as a result can be broken. A hash function has to be strongly sensitive to the message, irreversible, collision resistant and it has to be infeasible to find a message with the same corresponding hash value [117]. The terms "digest" and "checksum" are sometimes used alternatively for the hash value of a message. Size of the hash value may vary between 64 to 512-bit for different hash functions based on their structure and purpose, whereas the message size is

arbitrary. Amongst all the conventional hash functions, SHA-1 is the most famous hash function with 160 bits digest size.

Hash functions are unkeyed and if they come with keys they are usually called MAC (Message Authentication Code) [118], and are used both in cryptography and other fields of computer science such as data mining, genetic algorithms and neural networks. A keyed hash function (MAC) can be defined as below:

$$H_k: M \rightarrow D \tag{2.1}$$

where $K = \{k_1, k_2, .. k_l\}$ is the set of the keys, $M = \{m_1, m_2, .. m_n\}$ is the set messages to be digested using the hash function H_k and the key for the hash function $k \in K$ and the resulting hash value $D = \{d_1, d_2, .. d_m\}$. $l = |D|$ is cardinality of the digest size, which is normally a fixed value between 64 to 512-bits and $n = |M|$ is the cardinality of the arbitrary message size.

Cryptographic hash functions are frequently used in the structure of more complicated algorithms such as digital signatures, fragile watermarking algorithms and secure network layers, therefore their security is of great importance. Almost all of the secure transactions and communications on the internet rely on the security and correlation resistance of the hash functions. SHA1 and MD5 are the most commonly used hash functions in the structure of internet protocols and it can be claimed that they have been the two of the most used algorithms in history of online transactions. Although SHA1 and MD5 have been cryptanalyzed by Wang et al. [119], [120] and found weak against collision attack but they are still widely used in different types of protocols. However, SHA1 and MD5 should be replaced and therefore design of new hash functions with larger digest size and stronger correlation resistance for higher security has been of great importance. During the last decade numerous conventional and chaotic cryptographic hash functions have been proposed [11], [27], [94], [108], [118], [121]–[134].

2.2.2 Encryption Algorithm

While hash functions are one-way operations, encryption algorithms are designed to work two sided, meaning that an encrypted message with a key "K_e" can be decrypted by a decryption algorithm and key "K_d". In the case that the encryption and decryption keys are the same, the encryption algorithm is symmetric otherwise it is asymmetric. Until the mid-seventies and the invention of public key cryptography by Diffie and Hellman in their famous paper "*New directions in cryptography*" [135] all the encryption algorithms were symmetric and the sender and the receiver had to share a secret key through a secure channel. After that many other public key cryptographic algorithms such as Knapsack, RSA and El-Gamal [40] are introduced, however most of them rely on the idea of infeasibility of solving a hard problem to access private key. Based on this idea, several chaos-based cryptographic public key algorithms using semi-group characteristics of the Chebyshev polynomial based chaotic maps are suggested that most of them have been cryptanalyzed [40]–[54], [136]. An encryption algorithm can be defined as below:

$$E_{k_e}: P \rightarrow C, \tag{2.2}$$

E_{k_e} is an encryption function, $k_e \in K_e$ and K_e is the key space for this mapping. Key space defines all the possible keys for this particular mapping, which maps plaintext $P = \{p_1, p_2, .. p_n\}$ to $C = \{c_1, c_2, .. c_m\}$, $n = |P|, m = |C|$. P and C are the plaintext space and ciphertext space respectively.

Recovering message can be carried out using following function:

$$D_{k_d}: C \rightarrow P, \tag{2.3}$$

D_{k_d} is the decryption function, $k_d \in K_d$ and K_d is the key space for this mapping. In symmetric encryption both encryption and decryption keys are the same. A symmetric cryptosystem can be

either *block cipher* or *stream cipher*. One of the main differences between a block cipher and a stream cipher cryptosystem is the size of the data chunks encrypted in each round, usually if the size of the data chunk is larger than 64 bits; it is considered as block cipher. In many cases size of the processes chunk by the stream ciphers are as small as one byte [114].

2.2.3 Pseudo Random Number Generator

Pseudo random number generators (PRNG) are used in many of the research fields. A PRNG is a deterministic algorithm, which generates deterministic sequences of numbers. A close relative of PRNGs are the pseudo random bit generators (PRBG). A PRNG can be defined with five tuples $\{S, R, \varphi, \psi, P_A\}$ involving a finite set of generator states S, a set of possible outputs R, a state function ($\varphi: S \to S$), an output function ($\psi: S \to R$), and probability metric of random distribution of the seed (P_A) [137].

A cryptographically secure pseudo random number generator is a type of random number generator that the attacker cannot guess the next random number having access to a long stream of previously generated numbers. Such an algorithm can be used in the cryptographic applications such as stream ciphers. Several statistical tests such as Runs test, Parking lot test and Crabs test can be applied to investigate the randomness of a PRNG. Some randomness test batteries such as NIST SP800-22 [137], Diehard [138], TestU01 [139] and ENT tests are designed to perform set of several statistical tests on the random numbers generated by the PRNG. In between these batteries, TestU01 has a larger set of statistical tests with three major tests (Small Crush, Crush and Big Crush) [139].

2.3 Nonlinear Dynamic Systems and Chaos

Dynamics as an interdisciplinary subject was originally a branch of Physics [140] and began in the seventeenth century with Newton's invention of differential equation, discovery of laws of

motion and universal gravitation and their combination with Kepler's law of planetary motion [141]. Newton also could solve the two-body diagram, motion of the earth and sun. Later many mathematicians and physicists tried applying the same idea for three-body problem. However, it turned out to be more difficult until late nineteen century that Poincare introduced a new viewpoint and suggested a geometric approach towards analyzing the idea. Consequently, the modern approach towards dynamics came into existence. In his work, he also mentioned the concept of chaos, in which a deterministic system is aperiodic and very sensitive to initial conditions and control-parameters and therefore it is almost impossible to predict the state of the system in the long term. In the geometric way of studying the nonlinear dynamics, pictures are usually more helpful than the formulas [140]. Poincare also suggested a new method of drawing phase space diagram and bifurcations for cases with higher than three dimension using a sectioning method, which was later called Poincare sectioning [142]. This method is very useful while studying a chaotic system of more than one dimension as the phase space exceeds three dimensions and makes it very hard to visualize the geometric diagrams for the phase space.

Field of nonlinear dynamics has a very wide scope and there are many chaotic systems which some of them have been modeled from the nature. The neglected points in the design of the chaos-based symmetric cryptographic primitives are the concern of this study. In order to come up with a secure cryptosystem, during this research, complexity of the chaotic systems used in the field of discrete chaos-based symmetric cryptography is analyzed and the results are used as to refrain from faulty implementations. Nonlinear dynamics tries to simulate aperiodic nonlinear dynamical systems in the real world in different fields such as population growth, mechanical systems, biology, chemistry, weather forecast, planetary motions and several others subjects, also the mathematical equations suggested based on differential equation modeling of the systems can be considered as a source of high entropy information [143].

It is almost two decades that chaotic systems have been used for designing secure communication methods and cryptography algorithms and based on the literature review, there exist many chaos-based algorithms that have been proved to be either unsecure, slow, hard to implement or in general inefficient [55]–[79], [82]–[104], [106]–[110], [144]. The behavior of chaotic maps is very appealing for researchers in the field of cryptography and that might be because cryptographic algorithms, especially the symmetric algorithms with nonlinear characteristics, are actually chaotic deterministic systems without a particular differential equation describing their chaotic behavior. It can be claimed that all the nonlinear systems in the real world are algorithmic pseudo chaotic systems [140].

Until the last few decades that computer realization of the chaotic systems became possible, the field of nonlinear dynamics was not very active [145]. Lorenz in 1963 proposed a model for the thermal convection, which were three ordinary differential equations (Equation 2.4) [146]. In the same document, he has mentioned, "lack of periodicity is very common in natural systems". This sentence, eventually points to existence of chaotic non-periodic characteristics of natural systems. Furthermore, in an interview, Lorenz mentioned the metaphor of the "Butterfly effect", a flap of butterfly's wing in Brazil, could influence a hurricane several weeks later in Texas.

$$\begin{aligned} \dot{x} &= \sigma(y - x), \\ \dot{y} &= rx - xz - y, \\ \dot{z} &= xy - \beta z. \end{aligned} \qquad 2.4$$

The phase space for the Equation 2.4 if drawn, the famous Lorenz attractor (the Lorenz Butterfly) would be generated. The parameters (r, σ and β) are the control-parameters and the values for the (x, y and z) are the initial conditions. Figure 2.1 demonstrates Lorentz attractor for initial conditions ($x=8$, $y=3$, $z=33$) with the time frame of 100 and precision of 10^{-5} and control-parameters ($\sigma=10$, $r=28$, $\beta=2.66666666$).

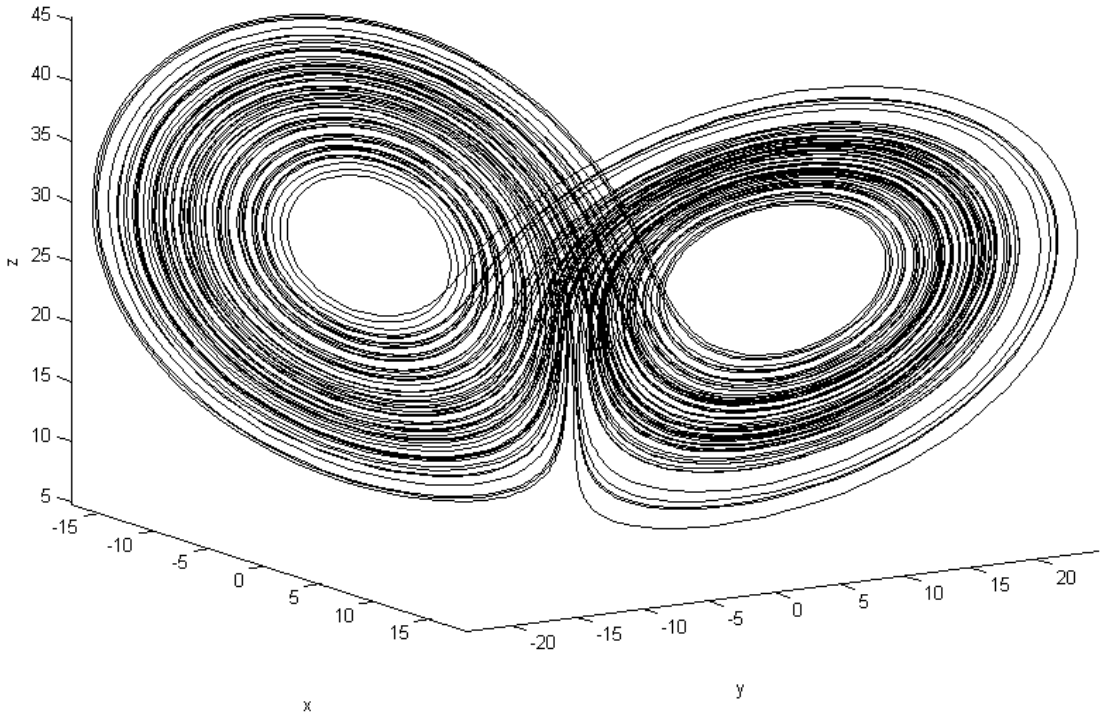

Figure 2.1: Lorenz attractor (using the Lorenz map)

The Lorenz map, (Equation 2.4) was first used for generating chaotic signals using a circuit (Figure 2.1) and a message, non-chaotic containing meaningful information, was masked by the chaotic signal and unmasked by an identical system which was synchronized and the message was retrieved in the receiver side [140].

2.4 Chaos-Based Cryptography

Although the main factors attracting researchers to chaos-based cryptography algorithms were almost the same and limited to few mutual characteristics, but there has been numerous different efforts and approaches towards this field [4], [9], [11], [16], [17], [19], [20], [23]–[26], [28], [33], [34], [36], [37], [39], [122], [126], [147]–[156]. These approaches can be categorized as chaos-based symmetric [2], [4], [5], [9], [15], [16], [20], [26], [27], [29], [30], [37], [118], [147], [150], [157], [158] and chaos-based asymmetric cryptographic algorithms [40]–[54], [136].

Analog chaos-based secure communication method was first introduced in the mid-1980s and in 1990 it was developed by Pecora and Carrol [159]. Their method was mostly based on chaos masking, the data as analog signals were masked under a very high frequency of chaotic signals generated by a circuit [140], [160]. In [160] the Lorenz map chaotic circuit was represented and used to generate chaotic mask for the wave carrying information.

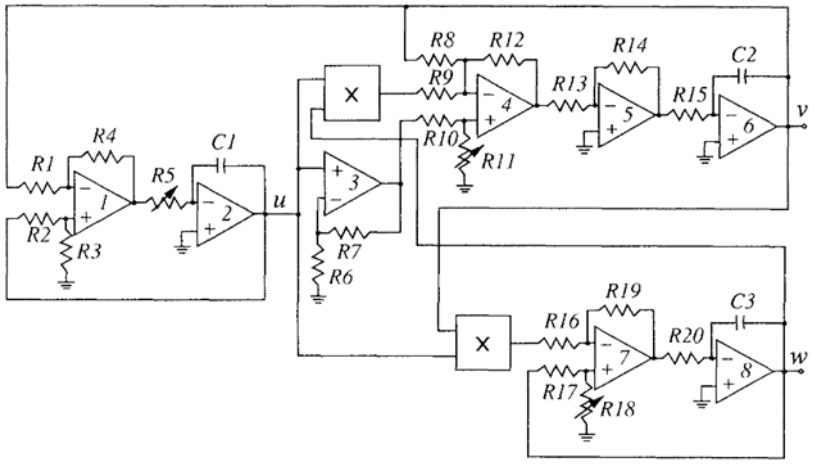

Figure 2.2: Lorenz based chaotic circuit [160]

Most of the analog chaotic cryptosystems, apart from masking mostly are based on chaos synchronization [102], [140], [160]. The basic idea of analog synchronization secure communication methods rely on synchronization of two or more chaotic systems in the transmitter and the receiver side [161]. However, the digital chaotic cryptosystems usually concentrate on the deterministic characteristics of the chaotic systems. In the other words, analog chaotic secure communication schemes and digital chaotic cryptosystems are based on two different techniques [102], while both of them depend on sensitivity to initial condition, control-parameters, complex behavior, unpredictability and determinism of chaotic systems. The first one uses the synchronization methods whereas the second one relies on the deterministic sensitivity of the chaotic trajectories to the initial conditions and control parameters.

The digital chaotic cryptosystems are mostly based on the discrete chaotic systems. They generally try to utilize discrete dynamical systems and encrypt the messages using the generated chaotic trajectories. Just few years after the emergence of analog secure communication methods based on chaotic systems, the idea of using discrete chaotic maps for encryption of digital data or as mentioned in [162], digital communication was developed. The idea was very simple and straightforward, both chaos and cryptography have mutual counterparts, such as sensitivity to initial conditions, control-parameters in chaos, random like behavior, unpredictability and finally determinism, which are very favorable for cryptographists and researchers in physics community.

2.4.1 Symmetric Chaos-Based Cryptographic Algorithms

Cryptography can in large scale be divided into two major categories, symmetric and asymmetric [163]. Chaos-based cryptographic schemes can be categorized as asymmetric and symmetric systems. Habutsu [164] was the first to introduce the chaos-based asymmetric cryptographic algorithm. His method was cryptanalyzed at the same conference by Biham [89].

In the last two decades a lot of research has been conducted on the symmetric chaos-based cryptographic algorithms and many new algorithms are proposed [2]–[39], [118], [122], [147]–[150], [157], [158], [165]–[169]. Figure 2.3 and Figure 2.4 demonstrate the number of articles found on the Scopus and Web of Science databases that are directly related to chaos and cryptography. The solid line represents all articles (both cryptography and cryptanalysis documents) and the hashed line demonstrated the cryptanalysis related documents. It can be seen that there has been a sudden increase in the number of publication from mid-nineties.

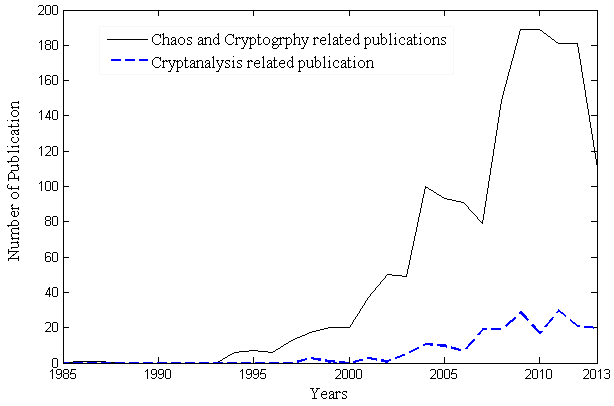

Figure 2.3: Number of publication on the Scopus database related to chaos and cryptography

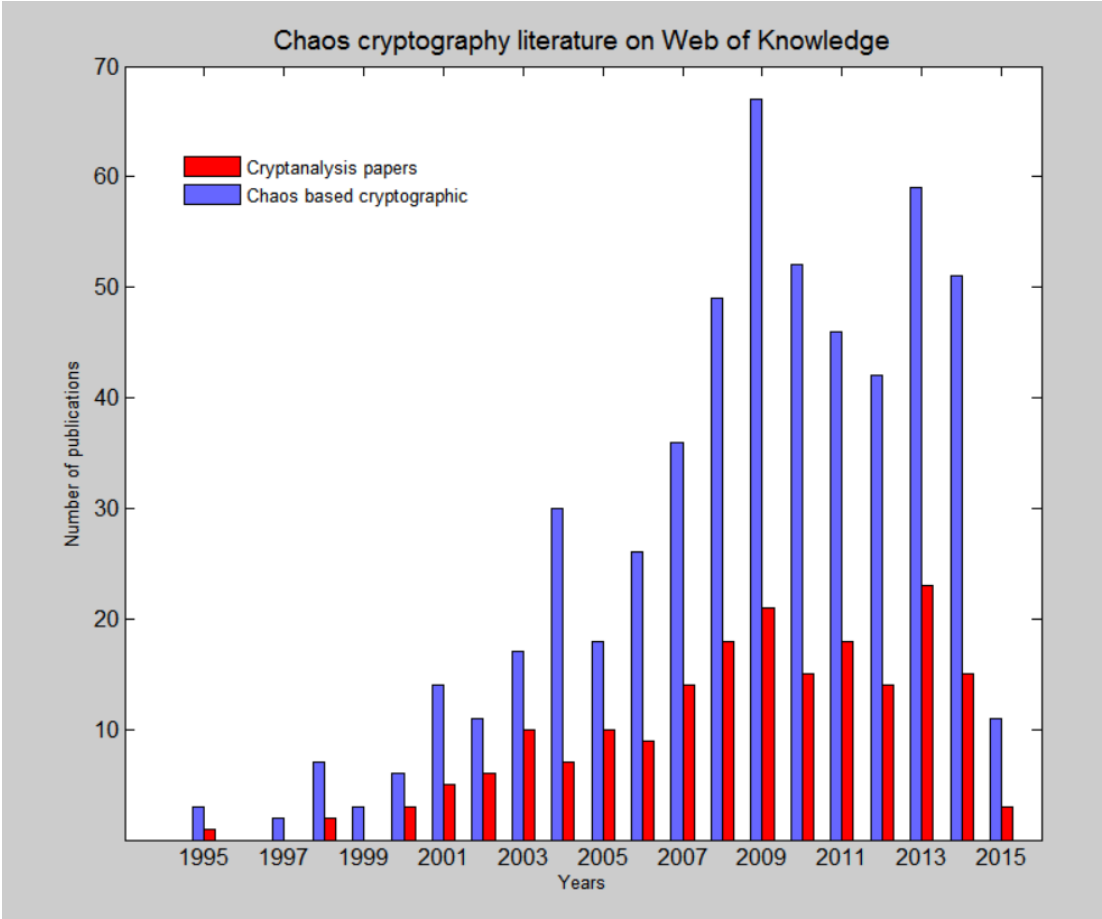

Figure 2.4: Documents on Web of Science database related to chaos and cryptography

Unfortunately, a large portion of these algorithms are cryptanalyzed and are proved to be unsecure [57], [59]–[62], [65], [67], [69]–[72], [74], [78], [82]–[84], [86], [87], [89]–[104], [106],

[110], [144]. The big amount of attention, accompanied with plenty of number of cryptanalyzed algorithms, suggests that, there exist some typical problems in the algorithms. This common problem makes them weak against different types of attacks. On the other hand, some of these algorithms not only are unsecure but also are very slow and inefficient. Most of the mentioned algorithms are image encryption algorithms and the rest are one-way hash functions and pseudo random number generators. Without loss of generality, it can be said that, just like symmetric cryptography, chaos-based symmetric cryptography can be technically categorized into two categories: block cipher algorithms and stream cipher.

The available chaos-based symmetric algorithms can be divided into five major categories: First category of algorithms, which are more primitive, manage to apply the random like behavior of nonlinear dynamic systems (namely chaotic systems) to shuffle the position of the data blocks (either as small as one bit or as large as several bytes). Most of the early image encryption algorithms that are proposed as premiers in the field follow the same idea. Their main strategy is shuffling or permuting the pixels (of a grayscale image) or the bits (of a black and white image) position to reach a scrambled output [170].

The second category of algorithms are the image encryption algorithms that are based on skewing the image files in several rounds with Arnold or Cat map. The second type algorithms are very famous for their direct connection between the image pixels and nonlinear systems. Besides security issues, most of the algorithms in this category have slow speed of encryption and need several rounds of encryption to provide a random output without any visible patterns in it. One of the famous algorithms of the second type is the Fridrich type algorithms, mainly based on Fridrich method proposed in his paper in 1998 [171]. In this method a two dimensional chaotic map (the Baker map) is applied to generate a block cipher algorithm mainly for image encryption. Later this type of algorithms were cryptanalyzed by Solak et al. [59].

The algorithms in third category are usually referred as Baptista type, which are mostly inspired by the creative encryption algorithm first proposed by Baptista [81]. The main concern in this algorithm is the number of iteration. Therefore, encryption of each block of data needs several iterations and consequently the encryption speed decreases dramatically. Many modified methods were presented based on Baptista method [55], [66], [107]–[109], [172] and most of them were also cryptanalyzed [67], [82], [173]–[175].

The forth type of the chaos-based cryptosystems possesses more complex structure and are stronger from the security point of view and clearly try to reconstruct the traditional cryptographic algorithm by the aid of chaotic maps. Xiang et al. [176] proposed a new chaos-based cryptographic algorithm, which applies a two dimensional chaotic map in order to generate S-Box for the cryptosystem [176]–[179], meanwhile some of these algorithms found to be not secure enough and were cryptanalyzed [79], [144].

The fifth type and the final type are the image encryption algorithms and one-way cryptographically secure hash functions based on a hybrid combination of control-parameters initial conditions and the plaintext. These methods provide more security because of their nature. They possess a complex structure and take advantage from the ergodic characteristics of the chaotic maps along with the mixing property and sensitivity to initial conditions in several directions [35], [37], [147], [166]. Some of the algorithms designed on this strategy were cryptanalyzed because of the problems in the applied chaotic maps in their structure [62], [65].

$$x_{n+1} = \alpha x_n(1 - x_n) \tag{2.5}$$

Chaos-based stream cipher cryptosystems and also chaos-based pseudo random number generators as other classes of symmetric chaos-based cryptographic algorithms have also been discussed a lot in the last couple of decades [14], [72], [92], [149], [180]–[193]. Most chaotic stream cipher algorithms directly depend on the pseudo-random number/bit generators based on

chaotic maps. One of the most famous methods of generating a chaos-based sequence of random bits is the symbolic dynamic representation of the Logistic map. In this particular method, a threshold is chosen (usually $x_t=0.5$) and the chaotic Logistic maps is iterated while in order to avoid attractors, the values of the initial conditions are normalized to stay in the safe zone, apart from *0.0*, *0.5* and *1.0*. The initial condition (x_0) and control-parameter (α) are typically taken as the secret key and in the simplest condition, the Logistic map (Equation 2.4) the generated bits are XORed with the plaintext values to generate the ciphertext. In more advanced stream cipher methods, a set of several chaotic maps are manipulated in order to generate higher complexity and reduce the possibility of predicting the bits.

2.4.2 Asymmetric Chaos Based Cryptographic Algorithms

Asymmetric cryptography has fundamental differences with the symmetric cryptography and therefore chaos-based asymmetric cryptographic algorithms also manipulate different characteristics of the chaotic maps [64]. First time in 1976, Diffie and Hellman proposed "*New Directions in Cryptography*" [135], which gave the revolutionary idea of key exchanging method. Later on 1977 Ron Rivest, Adi Shamir and Leonard Adleman proposed the RSA public key cryptography algorithm based on difficulty of factoring large integers.

Most of the asymmetric chaotic cryptography schemes, try to get advantage from the semi-group characteristics of the Chaotic-Chebyshev polynomial maps [41], [44], [45], [47], [48], [53] while most of the algorithms base the traditional asymmetric cryptographic schemes are based on the hard mathematical problems [114]. Some of the asymmetric chaos-based cryptographic algorithms have tried to take advantage of both the hard mathematical problems and semi-group characteristics of the Chaotic-Chebyshev polynomial maps simultaneously. In 1993, a chaos-based public key algorithm based on a method similar to ElGamal asymmetric encryption algorithm was presented [194]. But there was a problem in making it practical, as there is no

practically efficient fast method to iterate up to the *n-th* value of the chaotic map presented in it while the value of *n* is extremely large [64]. Later on, Kocarev et al [41] established a new method based on the commutative characteristics of Chaotic-Chebyshev polynomials over real numbers. But very soon was cryptanalyzed by Bergamo et al. [63]. It was proved unsecure as an adversary can find the plaintext from a given ciphertext. The main problem in asymmetric chaos-based cryptographic algorithms arises from in appropriate use of the real number implementation [63].

In order to improve the cryptosystem against the suggested attack, in another research, Kocarev et al. [48] modified the algorithm and manipulated the Chebyshev polynomials over the finite field Z_N, also Lima et al. [48] with another modification proposed the a new algorithm with prime finite field [48], [195]. In 2005, Xiao et al. proposed a new key agreement protocol based on chaotic maps [43]. This protocol was supposed to resist the known attacks, which were earlier suggested by Bergamo et al. [63]. Nevertheless, very soon Xiang et al. [68] and Han et al. [77] suggested a new attack which proved protocol proposed by Xiao et al. is unsecure[43]. In 2011, Lee et al. proposed a new extension to chaotic maps-based key agreement protocol. It took advantage of the semi-group characteristics of the Chebyshev polynomials to overcome all the attacks presented for the previous chaos-based public key cryptosystems [51].

2.5 Drawbacks and Limitations of Chaos-Based Cryptography

There have been many attempts in the field of cryptography with chaos in the last two decades, some of the methods and ideas although very brilliant and innovative have been successfully cryptanalyzed and their security has been proved to be practically inefficient [55]–[79], [82]–[104], [106]–[110], [144]. Nonetheless, the similarities between chaos and cryptography, such as ergodicity, aperiodic system evolution, sensitivity to initial conditions and control-parameters together with easy and quick implementation capabilities have been so strong