Chaos Based RFID Authentication Protocol

Hau Leung Harold Chung

A thesis submitted to the Faculty of Graduate and Postdoctoral Studies
in partial fulfillment of the requirements for the degree of

MASTER OF APPLIED SCIENCE

in Electrical and Computer Engineering

School of Electrical Engineering and Computer Science
Faculty of Engineering
University of Ottawa

Abstract

Chaotic systems have been studied for the past few decades because of its complex behaviour given simple governing ordinary differential equations. In the field of cryptology, several methods have been proposed for the use of chaos in cryptosystems. In this work, a method for harnessing the beneficial behaviour of chaos was proposed for use in RFID authentication and encryption. In order to make an accurate estimation of necessary hardware resources required, a complete hardware implementation was designed using a Xilinx Virtex 6 FPGA. The results showed that only 470 Xilinx Virtex slices were required, which is significantly less than other RFID authentication methods based on AES block cipher. The total number of clock cycles required per encryption of a 288-bit plaintext was 57 clock cycles. This efficiency level is many times higher than other AES methods for RFID application. Based on a carrier frequency of $13.56Mhz$, which is the standard frequency of common encryption enabled passive RFID tags such as ISO-15693, a data throughput of $5.538Kb/s$ was achieved.

As the strength of the proposed RFID authentication and encryption scheme is based on the problem of predicting chaotic systems, it was important to ensure that chaotic behaviour is maintained in this discretized version of Lorenz dynamical system. As a result, key boundaries and fourth order Runge Kutta approximation time step values that are unique for this new mean of chaos utilization were discovered. The result is a computationally efficient and cryptographically complex new RFID authentication scheme that can be readily adopted in current RFID standards such as ISO-14443 and ISO-15693. A proof of security by the analysis of time series data obtained from the hardware FPGA design is also presented. This is to ensure that my proposed method does not exhibit short periodic cycles, has an even probabilistic distribution and builds on the beneficial chaotic properties of the continuous version of Lorenz dynamical system.

Acknowledgements

I wish to acknowledge the encouragement of various individuals who have helped me during the process of completing this degree. First, I wish to thank Dr. Ali Miri for his unflagging support throughout this long process. Thank you for all of your encouragement, suggestions and wisdom throughout my Master's studies. A sincere thank you is also offered to my co-supervisor, Dr. Nancy Samaan, whose support allowed me to bring this work to completion.

Thank you also to my parents, Helena and Bernard, for supporting me throughout my undergraduate degree and for encouraging me in my studies. Your love and commitment truly helped me to have a better future.

Finally, thank you to my wife, Lindsay, for your understanding and love. It was at times a long and difficult process but your encouragement and understanding were most appreciated.

Contents

1 Introduction **1**

2 Background on RFID and Chaos **5**

2.1 RFID principle of operation 5

2.2 Authentication schemes in RFID 7

2.2.1 Lightweight authentication protocols 7

2.2.2 Classical cryptographic authentication protocols 8

2.2.3 Improvements to existing authentication methods 9

2.3 Chaos 10

2.3.1 Sensitive to Initial Conditions 11

2.3.2 Aperiodic time-asymptotic behaviour 11

2.3.3 Deterministic 11

2.4 Analog chaos based cryptography 12

2.4.1 Chaotic masking 12

2.4.2 Chaos shift keying (CSK) 13

2.4.3 Chaotic modulation 13

2.4.4 Chaos suppression techniques 14

2.4.5 Noise and chaos control 15

2.4.6 Limitations of direct analog chaos use in RFID 16

2.5 Digital chaos based cryptography 17

2.5.1 Stream ciphers employing chaos-based pseudo-random number generators 17

2.5.2 Chaotic stream ciphers via inverse system approach 18

2.5.3 Block ciphers based on chaotic round function or S-boxes 18

2.5.4 Limitations of direct discrete chaos use in RFID 19

2.6 Design issue one: induced voltage requirements 20

2.7 Design issue two: tag design complexity 21
2.8 Design issue three: increased manufacturing costs 21

3 Chaos based RFID authentication **23**
3.1 Authentication scheme 24
3.2 Lorenz dynamical system 25
3.3 States generation 27
3.4 Number format representation 28
3.5 Implementation on FPGA 30
3.5.1 Performance and resource utilization 37
3.6 Secret key 38
3.6.1 Lyapunov exponent 40
3.6.2 Optimal selection of time step h 43
3.6.3 $\boldsymbol{\rho}$ boundary conditions 52
3.6.4 System divergence from $\boldsymbol{\rho}$ 57
3.6.5 x_0, y_0 and z_0 boundary conditions 58
3.6.6 System divergence from initial conditions 63
3.6.7 Key size 69
3.7 Encryption and decryption rate 71
3.7.1 Direct x state utilization 71
3.7.2 x state permutation 72
3.7.3 x state selection 74

4 Security Evaluation of Proposed Scheme **77**
4.1 Statistical analysis 77
4.1.1 Short cycle periodic pattern verification 78
4.1.2 Statistical distribution verification 80
4.1.3 Rules and guidelines to follow to ensure the security of chaos based cryptosystems 81

5 Conclusions and Future Work **87**

A Additional rules and guidelines **90**

List of Figures

2.1 Hash function-based authentication protocol 7
2.2 HB+ authentication protocol 8
2.3 AES Challenge response authentication protocol 9
2.4 Bifurcation diagram of Hénon map with $\alpha = 1.4$ and $\beta = 0.3$ 15
2.5 ISO-14443A PCD carrier measurement 21

3.1 Proposed authentication scheme 24
3.2 Plot of $x - z$ showing the Lorenz butterfly attractor 26
3.3 IEEE-754 single precision format 28
3.4 Inputs and outputs of the FPGA implementation 32
3.5 FPGA implementation state machine 34
3.6 Xilinx ISim simulation of the Lorenz chaotic engine 35
3.7 Plot of x states generated by our HDL chaotic engine versus time in h time increments 36
3.8 Post place and route view of the design on Xilinx Virtex 6 xc6vlx75t . . 37
3.9 Plot of strange attractor with parameters $\sigma = 10$, $\rho = 28$, $\beta = 8/3$ and initial conditions $x_0 = 0.1$, $y_0 = 0.1$, $z_0 = 0.1$ 39
3.10 Plot of x states with parameters $\sigma = 10$, $\rho = 28$, $\beta = 8/3$, $x_0 = 1.001$, $z_0 = 15.001$ and $h = 0.001$ 45
3.11 Plot of x states with parameters $\sigma = 10$, $\rho = 28$, $\beta = 8/3$, $x_0 = 1.001$, $z_0 = 15.001$ and $h = 0.01$ 46
3.12 Plot of $S(\Delta n)$ with different values of ϵ having dimensions of 3, 4, 5, 6 and $\Delta h = 0.001$ 47
3.13 Plot of $S(\Delta n)$ with $\Delta h = 0.1$ having dimensions of 3, 4, 5 and 6 48
3.13 Plots showing different Δh values as the x states of the system approache chaotic range 50
3.14 Plot of $S(\Delta n)$ showing $\lambda \approx 0.19$ 52

3.15 Lorenz dynamical system orbit when $\rho = 0.5$ 53
3.16 Lorenz dynamical system orbit when $\rho = 10$ 53
3.17 Lorenz dynamical system orbit when $\rho = 14$ 54
3.18 Plot of x state variables with $\rho = 14$ 55
3.19 Plot of x state variables with $\rho = 24.06$ 55
3.20 Lorenz dynamical system orbit when $\rho = 100.5$ 56
3.21 Plot of x state variables with $\rho = 100.5$ 56
3.22 Plot of x states with $x_0 = 100$, $y_0 = 100$, $z_0 = 100$ and $\Delta\rho = 0.1$ 57
3.23 Plot of x states with $x_0 = 100$, $y_0 = 100$, $z_0 = 100$ and $\Delta\rho = 3$ 58
3.24 Plot of $x[Pleaseinsertintopreamble]z$ state with $x_0 = 1$, $y_0 = 15$, $z_0 = 15$ 59
3.25 Plot of $x - z$ state with $x_0 = 50$, $y_0 = 15$, $z_0 = 15$ 59
3.26 Plot of $x - z$ state with $x_0 = 100$, $y_0 = 15$, $z_0 = 15$ 60
3.27 Plot of $x - z$ state with $x_0 = 500$, $y_0 = 15$, $z_0 = 15$ 60
3.28 Plot of x states with $x_0 = 50$, $y_0 = 1$, $z_0 = 1$ and $h = 0.0001$ 61
3.29 Plot of x states with $x_0 = 50$, $y_0 = 1$, $z_0 = 1$ and $h = 0.013462$ 61
3.30 Plot of $|\Delta x_i|$ for initial conditions $y_0 = 1$, $z_0 = 1$, $x_0 = [1, ..., 250]$ and $h = 0.0201$ 62
3.31 Plot of $|\Delta x_i|$ for initial conditions $y_0 = 180$, $z_0 = 180$, $x_0 = [1, ..., 200]$ and $h = 0.0201$ 63
3.31 x states with different initial conditions of x 66
3.32 Plot of x states for time shortly after start of Lorenz dynamic system . . 66
3.33 Logarithmic Plot of x states for time shortly after start of Lorenz dynamic system 67
3.34 Plot of x states with $x_0 = 100$, $y_0 = 100$, $z_0 = 100$ and $\Delta x = 0.1$ 68
3.35 Plot of x states with $x_0 = 100$, $y_0 = 100$, $z_0 = 100$ and $\Delta x = 7$ 68
3.36 Plot of x, y and z states with a $\Delta x = 0.0201$ and $h = 0.0201$ 70
3.37 Permutation and XOR operations between sets of M 73
3.38 Plot of Lorenz x states in its chaotic region 74
3.39 Plot showing x states peak to peak Δh 76

4.1 FFT of Lorenz dynamical system with $\Delta h = 0.029$ 79
4.2 FFT of Lorenz dynamical system with $\Delta h = 0.0201$ 79
4.3 x state distribution over 1000 seconds from my proposed Lorenz chaotic engine 80

Chapter 1

Introduction

The use of radio frequency identification (RFID) devices has surged over the past two decades. From the simple one bit transponders used in almost all commercial merchandise for inventory control to wireless sensor networks, RFID is a technology that has proved to be invaluable because of its small footprint and low cost. However, with the widespread use of RFID technology in sensitive applications such as passports and financial payment methods, there are on-going concerns about the security of such RFID devices [1]. The security flaws of widely used commercial proprietary authentication schemes such as MIFARE have been published [43] and this has seriously affected the adoption of RFID in applications requiring enhanced security. The ability to distinguish a legitimate device from a rogue device necessitates RFID tag authentication. Because of the inherit production cost and physical size limitations of passive RFID tags, the amount of power and hardware resource available are limited. This is a unique challenge in cryptology for RFID devices and ultimately, the measure of success of any given RFID authentication scheme is a ratio of level of security offered over total amount of required hardware resource.

The state of the art in RFID authentication methods offers two widely published and distinct paths: lightweight authentication schemes such as HB+, and block cipher based methods such as AES. Over the past decade, many different implementations employing those methodologies have been suggested. Any market survey can reveal the lack of adoption of those authentication schemes in commercial use despite the fact that those authentication methodologies have already been suggested for a long time. The reason for this limited level of adoption in real world RFID systems is two fold. Weaknesses in

man-in-the-middle attacks against HB+ limits the level of security offered for this very efficient type of method. In the case of AES methods, the amount of ROM required for the S-box implementation and RAM needed for storing in-between stages values are expensive for RFID tags.

The use of chaos in the field of cryptology has been widely published and the intrinsic properties of chaos are, in fact, extremely desirable for cryptology. However, with respect to the application of chaos in RFID systems, it has not been researched extensively. From the results obtained in my research, a novel authentication method based on a chaotic challenge-respond scheme is proposed. This method has a high ratio of level of security over resource utilization, which suits well in RFID applications. I believe the accomplishments of my work during my research in this new avenue of RFID authentication offers a well-rounded and balanced approach in RFID security. Those accomplishments are:

1. An estimated use of 470 Xilinx Virtex 6 slices with zero block RAM usage for my hardware implementation of chaos based RFID authentication scheme. This level of hardware resource usage is well within current means of RFID manufacturing limits. This compares with 5673 Xilinx Virtex slices of a typical AES implementation [16]. It is important to note that there has been other AES implementations suggested that use fewer FPGA slices [11]. However, those implementations also require the use of dedicated block RAMs within the FPGA, which is not a possible mean to reduce resource utilization when implemented in actual RFID tags.

2. The amount of time necessary for each authentication session falls well within the practical realm of RFID usage. When implemented on FPGA, the chaos based RFID authentication requires only 57 clock cycles per authentication. This is compared with latency of 1000 clock cycles with other high security RFID authentication protocols [18].

3. A systematic way in the security evaluation of chaos based RFID system is shown with the aid of both numerical models and statistical analysis and the security of my proposed RFID authentication scheme is ensured. This acknowledges the fact that traditional analytical methods are unsuitable for security analysis of chaotic systems.

4. The first practical use of discretized chaos from a continuous time based dynamical

system in real world implementable hardware.

The material contained in this thesis for unveiling this novel chaos based approach in RFID authentication is organized in three stages. To begin, chapter two takes a look at the research that is being done so far in RFID authentication and discusses the reasons behind limited use of those suggested methods in real world RFID applications. The concept of chaos is introduced with a brief background in chaos theory and why properties of chaos are so beneficial to cryptology. Despite this fact, because of the unsuitability of analog chaotic signals in band limited wireless communication systems, most analog chaos based cryptosystems proposed thus far are not practical for use in RFID systems. In the discrete chaos based cryptology domain, piecewise-linear maps have been suggested but the level of security offered was proven to be limited because of dynamic degradation issues.

Chapter three focuses on my proposed chaos based RFID authentication scheme beginning with the first and foremost question regarding how continuous time chaotic signals can be generated in digital format inside the IC of a RFID tag. By using those chaotic signals, a challenge response RFID authentication scheme is introduced and an actual implementation in FPGA is demonstrated. This detail hardware design provides an excellent estimate in hardware resource required for manufacturing my proposed authentication scheme in a real world RFID tag. From the timing results in Xilinx ISim, it was shown that the number of clock cycles needed per authentication is significantly less than other block cipher based RFID authentication schemes. During authentication between a RFID reader and a tag, a secret key that is shared between both the reader and the tag is used. An explanation is then given regarding the composition of such key, which is composed of the system parameters of the Lorenz chaotic system. It was discovered that the boundaries of such chaotic system parameters play a crucial role in ensuring continued chaotic behaviour throughout the authentication process and must be respected during key selection

Because of the complex nature of chaotic systems, chapter four discusses several different methods that this work has proposed in the security evaluation of my chaos based RFID authentication scheme. By taking the fast Fourier transform of actual Lorenz chaotic states generated from my FPGA implementation, the absence of small periodic cycles can be proven given a very large pool of Lorenz chaotic states. A statistical analysis of those states are also examined to determine whether there is an uneven distribution of

states, which can render some states weaker than others. Finally, my proposed authentication method is verified against the rules for the design of a secure chaos cryptosystem suggested in [25] in order to make sure that there are no weaknesses in my interpretation of chaos in digital hardware.

Chapter 2

Background on RFID and Chaos

Radio frequency identification, as the name indicates, is a technology that facilitates the verification of authenticity of individuals and devices. The particularity with this type of verification of authenticity is in the physical nature of the devices used. Unique to RFID, passive tags require no battery to operate and it obtains all the power that it needs to power its IC via induction with the authenticating device called a reader. Another characteristics that is also unique to RFID is its small physical size and low cost to produce. Those major advantages have made RFID the future in authentication for everyday commercial devices. To really understand the security implications of RFID systems, it is necessary to first understand the components that make up an RFID system.

2.1 RFID principle of operation

In a RFID system, there are three core components that work together to provide identification functions: the database, the reader and the tag.

The database:
Since there can be literally thousands of items/devices that require unique identification, it is often impossible to retain all those information at the point of access; typical of an offline system. For this reason, such information is often stored at a location farther away from the point of access that can be easier to manage and control. Such structure, called online system, are what is most widely used today in large scale deployments.

The reader:
One of the most important difference between RFID systems and other identification systems is the fact that power can be supplied simply by inducing a voltage using coils. This permits tag designs to be extremely small and cost efficient. The reader produces an alternating magnetic field which induces a voltage to the coil of the tag to power up its ICs.

The tag:
The tag is the part of a RFID system that has the most physical and computational constraint because it is the item that will be mass produced. In a passive RFID system, power is induced by the reader as mentioned above. However, when the reader is in receive mode, the unmodulated alternating magnetic field is load modulated by the tag for data transmission from the tag to the reader. There exists active RFID systems such as sensor networks, which the tag has its own power source in the form of an internal battery. However, because of the less stringent power requirements, it is not the focus of this research.

In an attacker's point of view, the weakest link in any RFID system is between the communication between the reader and the tag. This is because the reader is often expose to the public and is susceptible to rogue tags attempting to be a legitimate device/user. Consequently, RFID authentication mechanisms have been used to distinguish legitimate tags from rogue tags. From evaluating the technologies that are currently being used in everyday RFID tags, one can observe that the majority of RFID authentication schemes are proprietary methods that rely on the secrecy of the underlying encryption mechanism to maintain its security. Strangely, over the past decade, there has been many RFID authentication methods that have been proposed ranging from efficient methods that requires comparable hardware resources with proprietary authentication schemes to robust methods utilizing block ciphers such as AES. By looking deeper into the technological trends in RFID authentication mechanisms, one can see that there are limitations to public authentication methods that have been proposed so far and that has made proprietary authentication methods still the unanimous choice in commercial applications. But this type of method also has its limitations because a physical inspection of logic implementation inside the tag itself via methods such as X-ray photography can reveal the algorithm of the underlying authentication method with relative ease. Before the introduction of chaos for the purpose of cryptography, one has to perform a wide angle evaluation of public RFID authentication methods suggested in order to have a baseline

to compare to in terms of level of efficiency and security.

2.2 Authentication schemes in RFID

Over the past decade, numerous authentication protocols have been studied with various degree of design complexity. They generally fall within three categories, namely: lightweight authentication protocols and classical cryptographic authentication protocols.

2.2.1 Lightweight authentication protocols

The basis behind hash function-based authentication protocols is a translation between a given key and its hashed value. Such hash value is considered unique in a sense that it is highly unlikely for two different keys to yield an exact same hashed value. The principle of operation in RFID is as follows: The reader activates the tag by inducing

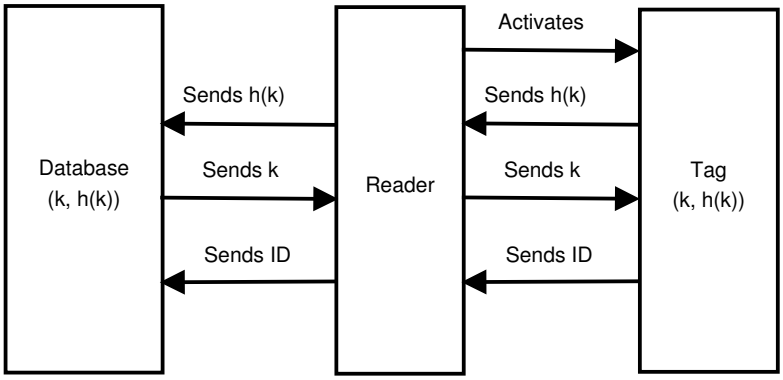


Figure 2.1: Hash function-based authentication protocol

a voltage across its coils. Then, once the capacitors in the tag has been fully charged, it sends a hashed version of the key k to the reader by load modulation. The reader forwards the key k to the database, which holds all the hashed values accepted by this system. If the database finds this hashed value, it will forward the corresponding key k to the reader for transmission back to the tag. The tag has build-in logic to calculate the hashed value of k and compares with the hashed value stored in its memory. If it is a match, the tag will send its identification to the reader to complete the transaction.

Another notable implementation is called the HB+ protocol. It only uses bitwise operations such as "XOR" and "AND" that are not resource intensive to implement [35].

HB+ protocol:
Keeping in mind the same reader and tag topology as the hash function authentication protocols, both the reader and the tag shares k-bit secret keys x and y. The tag starts by sending a k-bit blinding vector A over the air to the reader. The reader then sends over a k-bit challenge B to the tag. The tag calculates $z = (a \bullet x) \oplus (b \bullet y) \oplus v$ and sends over z to the reader for the first round. This exchange of values A and B continues for r rounds and the tag purposely injects noise into its response such that it sends the wrong response back to the reader with constant probability $\eta \in (0, \frac{1}{2})$. The reader accepts the tag as legitimate if fewer than ηr of the tags response is incorrect.

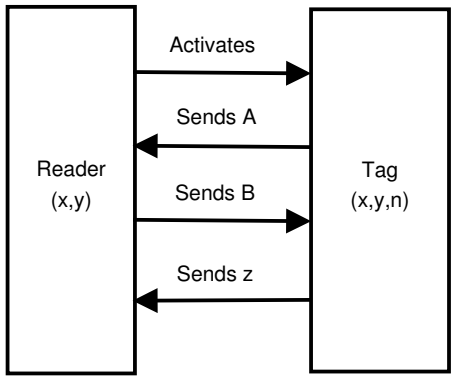


Figure 2.2: HB+ authentication protocol

2.2.2 Classical cryptographic authentication protocols

Advanced Encryption Standard (AES) has been deemed the successor to Data Encryption Standard (DES) and its use has been widely accepted as a secure cryptographic standard. From a RFID application perspective, classical cryptographic algorithms such as AES can be used in a challenge response scheme. After being powered up by the reader, the tag sends a random number A to the reader. The reader performs AES encryption on the random number A and send that value together with another random number B to the tag. The tag decrypts it to verify the authenticity of the reader and gets random number B in the process. Then, the tag changes the sequence of the random numbers A and B, encrypts it by using AES and sends it over to the reader. The reader decrypts it and verifies the correctness of random number B [18].

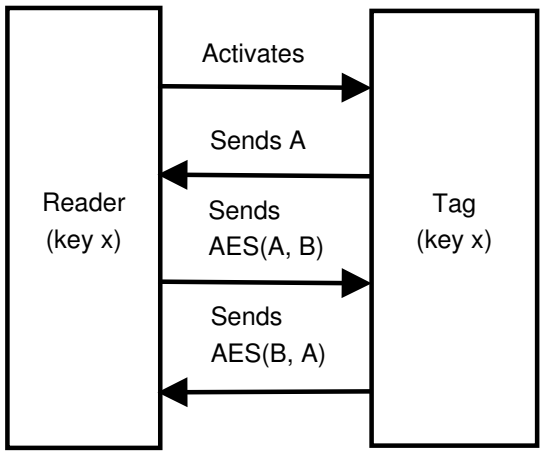


Figure 2.3: AES Challenge response authentication protocol

2.2.3 Improvements to existing authentication methods

As a baseline to gauge the level of success of any improvements to the authentication methods outlined above, one has to know the limitations of previously proposed solution. In the case of lightweight authentication protocols such as HB+, it is a very efficient method that can easily fit into modern passive RFID tags. On the security of this method, it has been demonstrated that it cannot resist man-in-the-middle attacks and active attacks that can query both the reader and the tag [69][24]. Despite this fact, HB+ protocol still receives a lot of attention because of its low cost of implementation. For protocols utilizing block ciphers such as AES, it offers proven level of security when applied in a challenge response type of authentication protocol. On its resource utilization side, however, it is not as efficient as HB+. Ever since the adoption of the Rijndael algorithm as AES, there has been many AES FPGA implementations. They range from implementations emphasizing on throughput to area optimized versions. Obviously, in the context of RFID authentication, throughput is of secondary concern since data throughput is usually quite low for each authentication session. The size of implementation, on the other hand, plays a much bigger role in the successful adoption for use in real world RFID systems. As a mean to estimate hardware resource requirements, FPGA implementations are often used to predict actual RFID resource usage. A typical AES implementation that sacrifices latency for a smaller implementation size uses on average 5000 Xilinx logic slices [16].

Knowing these facts, the goal in any new methods aiming at improving existing RFID authentication schemes should focus on an authentication method that is more secure than HB+ and more efficient than AES. That is precisely the highlight of my research and results from my proposed chaos based RFID authentication implementation shows that this new approach indeed satisfies the above requirements and offers an improvement over existing methods. But what is chaos and why is it so beneficial for RFID authentication? To answer this question, one has to understand the special properties of chaos, which make it an ideal candidate for use in cryptology.

2.3 Chaos

Since the awareness of the existence of chaos in natural phenomenons such as heat dissipation and oscillating chemical reactions to the rate of heart beat, researchers have been fascinated by it's simple, yet complex behaviour. The repeated application of simple non-linear equations has given us non-deterministic results that is different than just random noise. Edward Norton Lorenz published "Deterministic non periodic flow" in 1963 that began the widespread interest in the research of chaos. This has simply opened the door to a much wider field and up to this day, the ripple effect of chaos theory is still being investigated in dynamical systems. Research in the field of chaos has been divided in two distinct fields that ultimately has two different goals. The first one is the modelling of real world systems with the knowledge gained from chaos whereas the latter is creating cryptographic systems by exploiting chaotic properties. In a way, although these two fields of research do apply the same principals of chaos, their end goals are completely different. For instance, physicists have the difficult task of trying to identify and model chaotic behaviour given data obtained from natural real world systems. With an unknown system dimension, parameters and initial system state, this task often becomes impossible to solve analytically and numerical models have their limitations. This degree of difficulty, when it is applied to the application of chaos in cryptography, is also true and that is precisely what makes chaos so interesting for cryptosystems. Given a cryptosystem with a proper and robust application of chaos, it can be as strong as the underlying chaotic dynamical system itself. If an attacker were to circumvent this cryptosystem based on chaos, the task that they face will be the same challenges that physicists face in modelling natural phenomenons. To quantify a dynamical system as chaotic, all of the following properties have to be present.

- Sensitive to initial conditions
- Aperiodic time-asymptotic behaviour
- Deterministic

2.3.1 Sensitive to Initial Conditions

Given a dynamical system θ in a i dimensional state space, two points differing by an infinitesimally small distance d at time t_0 will eventually diverge exponentially in their orbits such that as $t \rightarrow t_n$, $d_0 \gg 0$. When applied in cryptology, this is the most beneficial property of chaos because a slight change in any of the parameters in a chaotic cryptosystem will translate into a very big change in its encrypted output. For example, if an attacker is off by one bit in guessing the secret key of a chaotic cipher, the ciphertext generated would be completely different from the legitimate encrypted ciphertext.

2.3.2 Aperiodic time-asymptotic behaviour

The trajectory of a given chaotic dynamical system has to be aperiodic and cannot settle to any single point in its phase space. This includes a trajectory that is tending to either positive infinity or negative infinity. What this means is the chaotic signal that is used to encrypt a particular message would not follow a predetermined periodic pattern and that makes the probability in predicting future ciphertexts to be $2^{1/2}$.

2.3.3 Deterministic

A chaotic dynamical system has to be governed by a set of inputs and only that set of inputs. The entire dynamic system trajectory has to be reproducible each and every time given the exact same initial conditions and system parameters. In other words, it is not simply a random occurrence of points in phase space. This fact is extremely important because otherwise, it would be impossible to decrypt chaotic messages.

Given the highly unpredictable behaviour of chaotic dynamical systems and its many beneficial properties suitable for cryptology, previous research have suggested implementations of chaos in cryptosystems both in analog and digital systems. Out of those implementations, very few of them has their target application geared towards RFID

systems. To my knowledge, the research that I have undertaken in chaos based cryptography for RFID systems is only one in harnessing the beneficial properties of chaos for use in RFID that is practical for actual real world use. But first, it is necessary to understand what is current out there in terms of chaos based cryptosystems and to know whether it is possible to adopt those systems for RFID authentication. The following is a literature review of currently suggested analog and digital chaos based cryptosystems and an explanation of the particular challenges in chaos based RFID cryptography.

2.4 Analog chaos based cryptography

The application of chaos in analog systems has been around for a longer period of time than digital systems. In the most direct application of chaos, it has been suggested that chaotic signals can be used to obfuscate analog signals. To achieve this goal, chaotic signal synchronization is used and it forms the basis of the majority of analog chaos based communication cryptography. More precisely, there are three main methods that are widely published to this effect: chaotic masking, chaos shift keying, and chaotic modulation.

2.4.1 Chaotic masking

Given a n dimensional chaotic system modelled by a set of differential equation $\dot{u} = f(x)$ where $u = (u_0, u_1, u_n)$ and $f(x) = (f(x_0), f(x_1), f(x_n))$. Two arbitrarily stable subsystems can be divided from u, resulting in $u = (v, w)$ where:

$$\begin{aligned} v &= (u_0, u_1, u_m) \\ w &= (u_m, u_{m+1}, u_n) \end{aligned} \tag{2.1}$$

From [58], it was shown that if both systems v and w are coupled with the same system parameters and if their initial conditions difference is no more than 5%, as $t \to \infty$, both systems will eventually arrive at the same state and remained synchronized. This is the basis of identical synchronization. Now, chaotic masking schemes such as [52] and [15] builds on this synchronization scheme and applies it to an application model. Simply stated, given $s(t)$ as the original message, $i(t)$ as the received message and the Lorenz chaotic states variable x as the driving signal, the sender combines state variables $x(t)$ with an analog message $s(t)$ such that the amplitude of $s(t)$ is much lower than state variable x. Then, through a communication medium, this signal is transmitted to a

receiving party. By synchronizing the underlying chaotic system parameters between the sender and the receiver, their system states will be at the same point as mentioned previously. The receiver having the received message $i(t)$ subtracts the dominant chaotic signal $x(t)$ away from $i(t)$ and the result is the original analog message.

This type of system, although it is relatively easy to implement at the beginning, has a few difficult to tackle challenges. In [70], Short showed that such additive modulation scheme can be easily broken by using multi-step predictions or a re-summing process on the residuals after one step predictions.

2.4.2 Chaos shift keying (CSK)

In [57], the author again draws from the synchronization method by [58]. As an example, given two Chua's dynamical systems [14] defined by the same differential equations:

$$\begin{aligned} \frac{dv_1}{dt} &= \frac{1}{C_1}\left[\frac{v_2 - v_1}{R} - f(v_1)\right] \\ \frac{dv_2}{dt} &= \frac{1}{C_2}\left[\frac{v_1 - v_2}{R} + i_3\right] \\ \frac{di_3}{dt} &= \frac{1}{L}\left[-v_2 - R_0 i_3\right] \end{aligned} \tag{2.2}$$

System A has its set of system parameters, system B has some other different system parameters and both systems are in a stable state. Let v_1 be the driving signal. Chaos shift keying is based on the difference of these two dynamical systems that are of the same class but numerically different. When the sender wants to transmit a binary zero, v_1 from system A is used as the driving signal. On the other hand, if the sender wants to send a binary one, v_1 from system B is instead used to drive the subsystem. The result is the receiver getting a series of signals corresponding to two sets of v_1. Consequently, by attempting to apply chaos synchronization of the received v_1 with dynamical systems A or B, v_1 will synchronize with either one of the dynamical systems. Hence, a binary bit stream can be transmitted and the signal travelling over the communication medium would appear noise-like.

2.4.3 Chaotic modulation

In [8], the authors suggested a communication scheme based on modulating phase synchronized Rossler dynamical systems (x_i, y_i, z_i) where $i = (1, 2, 3)$. The subsystems

(x_1, y_1, z_1) and (x_2, y_2, z_2) are the drive subsystems and are defined by the following equations:

$$\begin{aligned} \dot{x}_{1,2} &= -(\omega + \delta\omega)y_{1,2} - z_{1,2} + \epsilon(x_{2,1} - x_{1,2}) \\ \dot{y}_{1,2} &= (\omega + \delta\omega)x_{1,2} + 0.15y_{1,2} \\ \dot{z}_{1,2} &= 0.2 + z_{1,2}(x_{1,2} - 10) \end{aligned} \tag{2.3}$$

The response subsystem (x_3, y_3, z_3) is defined by:

$$\begin{aligned} \dot{x}_3 &= -\omega' y_3 - z_3 + \eta(r_3 cos(\theta_m) - x_3) \\ \dot{y}_3 &= \omega' x_3 + \alpha y_3, \\ \dot{z}_3 &= 0.2 + z_3(x_3 - 10) \end{aligned} \tag{2.4}$$

The signal that is being transmitted from the drive subsystem to the response subsystem is the phase θ_m defined by:

$$\theta_m = arctan\left(\frac{(y_1 + y_2)/2}{(x_1 + x_2)/2}\right) \tag{2.5}$$

In order to transmit a binary sequence, the angular difference $\Delta\theta$ is being modulated accordingly and in the receiver system, if the amplitude of θ_3 is mostly positive, it denotes a binary 1 and the opposite yields a binary 0.

2.4.4 Chaos suppression techniques

Until recently, chaos suppression has been suggested in [12] as a mean to control chaos. Choe *et al* used Lorenz dynamic system defined by the usual set of three ordinary differential equations. When a small amplitude periodic signal is used to influence the parameter of the Lorenz dynamical system, it was observed that chaotic states will converge to and remain in a particular fixed state. Then, when that small amplitude periodic signal is removed from the Lorenz system, chaotic behaviour quickly resumes and the strange attractor resumes its normal trajectory. When employed in cryptography, the sender can transmit a message that is embedded within the chaotic signal. Given prior communication between the sender and the receiver in another communication regarding the phase and amplitude of this small amplitude signal, the receiver can potentially suppress the chaos in the transmitted chaotic signal and recover the real intended message.

2.4.5 Noise and chaos control

[56] states that in order to obtain better system performance, we, in fact, want the system to be in chaotic state. This is because the chaotic attractor of a dynamical system has embedded within it, many stable periodic orbits. With a small disturbance of an accessible system parameter, one can make the chaotic system stabilize around a periodic orbit. On the contrary, if the dynamical system is already in a stable orbit, it is only possible to deviate the trajectory slightly.

Hénon Map

Both [56] and [13] utilized the Hénon map as their discrete dynamical system of choice. Hénon map is a two-dimension dynamical system characterized by the map:

$$\begin{aligned} x_{n+1} &= 1 - \alpha {x_n}^2 + y_n \\ y_{n+1} &= \beta x_n \end{aligned} \tag{2.6}$$

Depending on the values of the parameters α and β, the trajectory behaves differently. Below is a plot of the bifurcation diagram of the Hénon map with $\alpha = 1.4$ and $\beta = 0.3$.

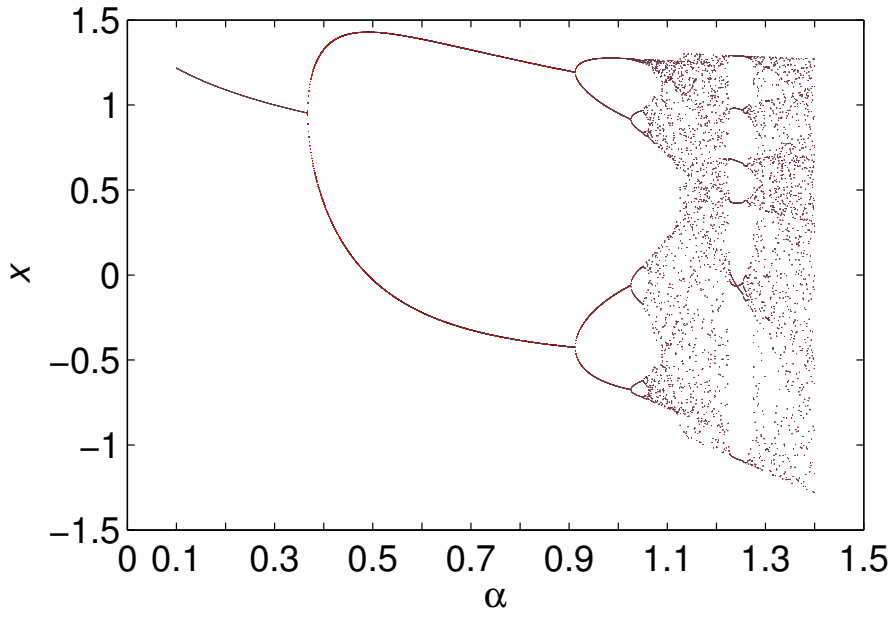


Figure 2.4: Bifurcation diagram of Hénon map with $\alpha = 1.4$ and $\beta = 0.3$

As shown in figure 2.4, as α increases, the period doubling property of the Hénon map takes effect and when α reaches past 1.1, it interleaves between multiple periodic and chaotic trajectories. [56] uses a Poincaré map of a three dimensional continuous dynamical system as their discrete map of choice to illustrate their point. In general, the dimension of the surface of section M given D is the dimension of the continuous dynamical system is $M = D - 1$. In the case of [56], the surface of section is a 2-dimensional plane. They begin by selecting a preferred unstable periodic orbit that improves on the performance of the dynamical system in question. Then, for each point that intersects the surface of section, they look at whether that point falls within a range that is close to the unstable periodic orbit in question. If it is, then they would alter the externally accessible parameter p so that the intersecting point intersects the point of the unstable periodic orbit. In a numerical example, [56] uses a slightly different form of the Hénon map, which is:

$$\begin{aligned} x_{n+1} &= \alpha - {x_n}^2 + \beta y_n \\ y_{n+1} &= x_n \end{aligned} \tag{2.7}$$

with $\beta = 0.3$. In that example, they have shown that it is possible to force the chaotic trajectory into following an unstable periodic orbit. Referring back to Christini & Collins' paper, they used the principle of the control method detailed in [56] but instead of setting α of the Hénon map to 1.29 where the dynamical system is in its chaotic region; they picked α to be 1.00 which can be observed from the above plot that the system is in an unstable period-4 orbit. With this method, it was observed by Christini and Collins that the transient time required for the dynamical system to fall within the desired unstable periodic orbit is almost instantaneous.

2.4.6 Limitations of direct analog chaos use in RFID

The main issue that prevents a direct adoption of the above strategies in RFID is that signal transmission is limited to a broadband communication medium since chaotic signals are not periodic. For any practical use in modern radio-frequency systems, this simply cannot be employed because it is impossible to confine an analog chaotic signal into a certain frequency band. The aperiodic nature of chaotic dynamical systems would imply a monopolization of the entire radio frequency medium and this would make the use of direct application of analog chaos based cryptosystems impossible for real world wireless communication use.

In addition to this problem, synchronization between the chaotic system of the sender and receiver is often easier said than done and there has been numerous works published in regards to this subject [58][62]. Of them all, identical synchronization is considered as more robust and the most widely used synchronization method. However, regardless of the type of synchronization used, synchronization has to be continuously maintained between the sender and receiver. In a real world system, noise can easily affect the quality of the signal that the receiver obtains, which in turn, will affect how well synchronization is maintained. If re-synchronization is necessary, this could dramatically reduce the throughput of such communication system and the increase in bit-error-rate. For chaos suppression techniques, it is difficult to proof that only one particular type of small periodic signal has a given unique suppressed trajectory because there is a chance that another small periodic signal disturbing this same chaotic communication channel can yield a similar or the exactly same suppressed trajectory. Such consequence would be detrimental to the security of any implementation that are based on this type of suppression technique. For chaotic cryptosystems employing noise control methods, they are very hard to implement in practice because they necessitate strict manufacturing standards that are hard to control and this is true especially for resource constrained RFID devices.

2.5 Digital chaos based cryptography

In general, discrete chaos ciphers do not make use of synchronization between the sender and receiver as was the case with analog chaotic ciphers. Instead, certain parameters of the dynamical system serves as the secret that is not known to a third party and that is often used as a key in the encryption and decryption process. The following explains three notable chaos based digital cryptosystems that have been proposed.

2.5.1 Stream ciphers employing chaos-based pseudo-random number generators

By using a chaotic map, it was shown in [44] that a pseudo-random number generator can be based on chaos and a subsequent simple exclusive OR operation can be used to encrypt images. Given the following difference equation, which defines the logistic map:

$$x_{n+1} \equiv \mu x_n(1 - x_n) \tag{2.8}$$

where,

$$x \in (0, 1) \tag{2.9}$$

When $\mu_{\text{inf}} \simeq 3.57$ and $\mu_{\text{inf}} < \mu \leq 4$, the behaviour of the logistic map gives a mixture between chaos and order. Given careful examination of the selection of μ_{inf} ensuring that chaos is present in the response of the system, x states are always bounded between zero and one. By first multiplying the resulting x state with 10^7 and then multiplying by modulo 256, a pseudo-random number between 0 and 255 can be generated. Subsequently, this number is used to encrypt a grey scale image array by using the XOR operation between the two values in binary.

2.5.2 Chaotic stream ciphers via inverse system approach

Given two nonlinear dynamic systems, the first system is the transmitter and the second system is the receiver in a communication system. The input to the transmitter is $u(t)$ and its output is $y(t)$. On the receiver side, the input is $y(t)$ and its output is $u'(t)$. The relationship between the input at the transmitter and the output of the receiver is given by:

$$\begin{aligned} y &= \sigma(u, x_0) \\ u\prime &= \sigma^{-1}(y, \xi_0) \end{aligned} \tag{2.10}$$

At the receiver, the original information can only be decrypted when:

$$|u - u'| = 0, \qquad as\ t \to \infty \tag{2.11}$$

2.5.3 Block ciphers based on chaotic round function or S-boxes

In traditional symmetric ciphers, such as DES and AES, desirable diffusion and confusion properties in a cryptosystem are implemented by a repetition of simpler rounds of ciphers. Several works have suggested that chaotic maps do carry both diffusion and confusion properties as the number of iterations tends to infinity. In [73], by iterating the Logistic map given by:

$$\tau(x) = \mu x(1 - x), \qquad x \in I = [0, 1] \tag{2.12}$$

and using a Boolean function, an 8-bit binary table is obtained and it contains 2^8 values. Then, by repetitively applying the discretized version of the following Baker map:

$$\begin{aligned} B(x, y) &= (2x, y/2) && 0 \leq x \leq 1/2 \\ B(x, y) &= (2x - 1, y/2 + 1/2) && 1/2 \leq x \leq 1 \end{aligned} \tag{2.13}$$

a 8x8 substitution box is obtained.

2.5.4 Limitations of direct discrete chaos use in RFID

The limitations of each of those previously discussed discrete chaotic ciphers has render the use of chaos in digital systems non practical for real world applications. For cryptographic ciphers utilizing chaos based pseudo-random number generators, selection of a μ value, which consistently exhibits chaotic behaviour, is not linear and the risk of low μ variance is a concern. In chaotic stream ciphers employing the inverse system approach there are weaknesses demonstrated in [77]. In the event that the chaotic mappings between the transmitter and receiver are known to an attacker, reconstruction of subsequent communications can be easily decrypted. In addition, synchronization can still be achieved despite a mismatch in system parameter. As an example, the system described in [19] can be decrypted with a differene of $2nF$ in the capacitance value. Cross-correlation between the plaintext and ciphertext of this method also introduces significant security flaws in practical applications. In block ciphers using chaos based s-boxes, the very special characteristics of chaos, such as sensitive to initial conditions, are not being exploited. Improving on an already cryptographically strong cipher such as the AES block cipher via chaos based s-boxes without making such block cipher more efficient is simply a redundant effort that is not taking proper advantage of chaos. One dimensional piece-wise linear chaotic maps offer an efficient way of implementing chaos in digital communications particularly because it's simple addition and division operations are efficient to be implemented in hardware. However, it has been shown in [47] that piece-wise linear chaotic maps suffer two major problems in finite computer precision:

- In discrete chaotic dynamical maps, when the calculations are realized in fixed-point arithmetic, the digital orbits will all converge to zero [45].
- Since digital chaotic orbits, such as those in Tent maps, are bounded by 2^n, where n is a finite number that a computer system is bounded by, the orbit is destined to repeat itself. In other words, small cycles can occur and that would jeopardize the unpredictability factor of the chaotic system.

From these results of chaos based cryptographic methods, one can see that there is room for improvement both in the level of security offered and the practicality of implementations in real world systems. When chaos is applied in the application of RFID, some very specific requirements in design has to be considered. They are:

1. Voltage requirements in a passive PICC device;
2. Due to the RFID intrinsically small design footprint, minimal design complexity is necessary; and
3. Increased PICC manufacturing costs.

2.6 Design issue one: induced voltage requirements

In a passive RFID system, the tag receives its power from the voltage induced on its antenna to power up the integrated circuits within the card to begin the challenge response process. One can easily see that a direct use of analog chaotic signal is impractical for wireless communication systems. This is because chaotic signals looks just like noise and will not be able to provide enough induced voltage for the tag to function in a passive RFID system.

From Faraday's Law, we know that the magnitude of an electric current is proportional to the change in magnetic flux of a closed loop circuit. To verify mathematically means that we have to solve for:

$$\mu = +\frac{d\Psi_2}{dt} \tag{2.14}$$

$$= M\frac{di_1}{dt} - L_2\frac{di_2}{dt} - i_2R_2 \tag{2.15}$$

where μ is the voltage, M is the mutual inductance, L is the conductor loop, Ψ is the magnetic flux and i is the current. However, since the signal is no longer a sinusoidal waveform, we cannot reduce this equation any further. As a more practical approach, one can evaluate the actual voltage levels of a well established ISO-14443A integrated circuit, the MF1-IC-S70 by Philips Semiconductor. Figure 2.5 depicts the measurement of the carrier emitted from the MF1-IC-S70 as a PCD. The peak to peak amplitude shows $2V$ at the antenna output and if one looks at the specification of the ISO-14443A standard, the magnetic field strength H of any given system should be between $1.5Amperes/meter$ (rms) and $7.5Amperes/meter$ (rms) [32]. Given a chaotic signal comprised of its state variable x appears noise like, its frequency counterpart occupies a wide band. For this reason, the transmitter side necessitates a very large power spectrum in order to drive the overall noise-like chaotic signal into a narrow band receiver. The real-world implementation of this approach is unrealistic because frequency bands are tightly controlled and unregulated transmission in such a large frequency spectrum is impractical.

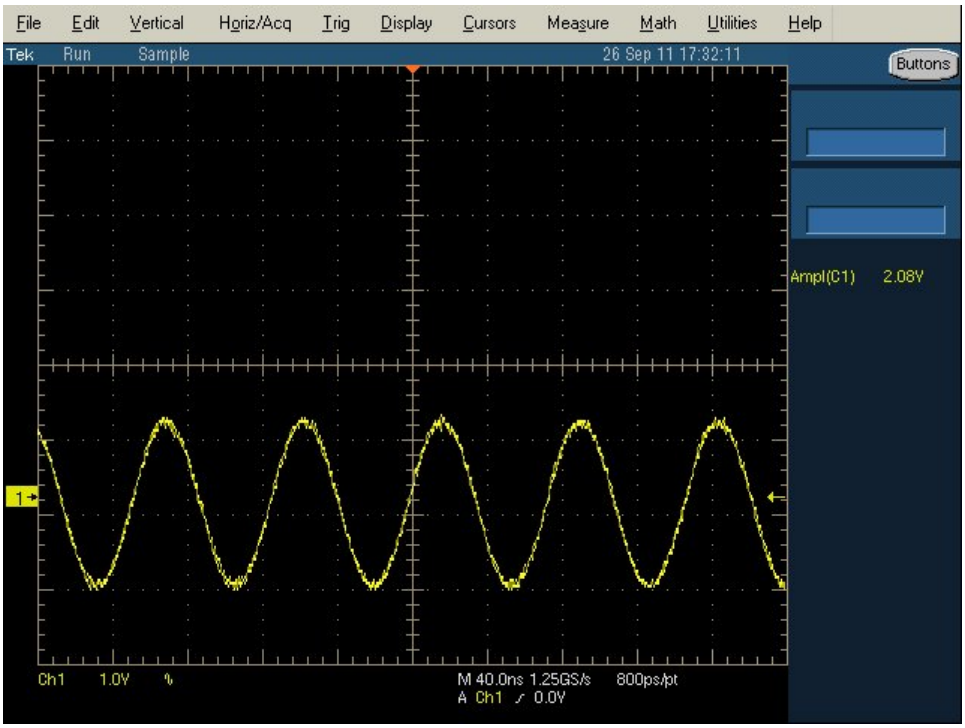


Figure 2.5: ISO-14443A PCD carrier measurement

2.7 Design issue two: tag design complexity

The level of complexity on the reader is not a real issue because, although the size and power requirements have to be reasonable, it is not a resource constrained device. The tag, on the other hand, has to adhere to strict design limitations because:

1. With added computational complexity, the amount of power required to power up the integrated circuits on the tag could exceed the amount that the reader can provide by induction; and

2. The size of the tag could be too large for it to be portable enough to be used in practice.

2.8 Design issue three: increased manufacturing costs

The single most important factor of why RFID authentication systems are so widely adopted in the industry is because of the low cost associated with its implementation.

We know for a fact that current ASIC manufacturing capabilities allow for a cost effective adoption of encryption algorithms like DES. NXP's line of proximity card reader integrated circuit, namely, the Mifare DESFire using DES encryption and the Mifare Plus utilizing 128-bit AES encryption are good examples of current manufacturing capabilities. To put those encryption schemes into real numbers, 15 microAmps of power and 5000 gates for a .35 micrometer CMOS process is typical for current RFID tag security mechanism [18].

In the following chapter, an explanation of my proposed chaos based RFID authentication scheme, which satisfies the above requirements will be given. It will be shown that such authentication scheme offers drastic improvement in RFID hardware resource efficiency without sacrificing on security.

Chapter 3

Chaos based RFID authentication

My proposed RFID authentication system is based on a challenge response scheme utilizing chaos as the driving force for providing security in the encryption of data between the RFID reader and the tag. A secret key is shared between the reader and the tag for encryption and decryption and it is composed of parameters of the chaotic system. This chaotic system in question is the continuous time Lorenz dynamical system utilized in the discrete domain via fourth order Runge Kutta approximation. By using this novel approach, it was shown that 288 bits of data can be encrypted with a secret key containing 32 bits within 56 clock cycles and the entire implementation consumes only about 470 Xilinx Virtex 6 slices. This is compared to the utilization of 5673 Xilinx Virtex slices [16] and 1000 clock cycles for an encryption of 128 bits of data [18].

In this chapter, we begin with an explanation of the challenge response exchanges between the RFID reader and the tag which makes up the frame of my proposed authentication scheme. Then, focus will shift to the underlying Lorenz chaotic state generation mechanism that provides the much needed level of security in the encryption and decryption of messages between the reader and the tag. A complete hardware implementation in FPGA will be provided to show the design choices made in order to make this chaos based authentication scheme so compact, highly efficient and requiring little hardware resource to implement.

3.1 Authentication scheme

The authentication scheme proposed uses a challenge response system that enables bi-directional authentication of both the reader and the tag. Figure 3.1 provides a graphical explanation of the exchanges between the reader and tag during a successful authentication session.

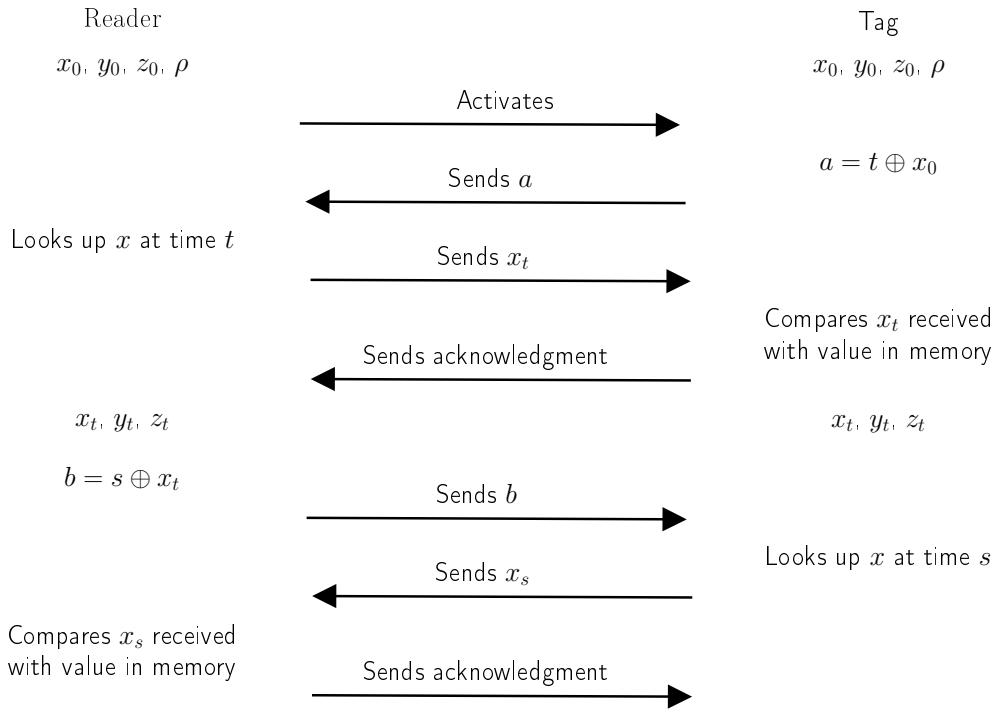


Figure 3.1: Proposed authentication scheme

1. The reader and the tag both have their previously agreed upon secret key. Suppose that a tag wants to authenticate with a particular reader. The reader sends out an alternating magnetic field from its coil to power up the ICs of the tag. While this is taken place, the reader calculates a set of discrete Lorenz chaotic states x and stores them in memory.

2. Once the capacitors are fully charged inside the tag, the latter load modulates the carrier wave to tell the reader that it is ready to begin authentication.

3. The reader sends out a certain value a as challenge to the tag to begin the authentication process for the verification of the authenticity of the tag.

4. The tag receives this challenge and provides a valid response to the reader by load modulating the reader's carrier signal.

5. The reader verifies that this response is correct and sends out an acknowledgement to the tag by applying amplitude shift keying of its carrier signal.

6. The tag then takes its turn to send out a challenge to the reader to perform the verification of authenticity of the reader.

7. The reader sends a response back to the tag and upon the successful verification of this response by the tag, mutual authentication is then complete.

8. Now, having secured the identification of both the reader and the tag, the same secret key is used in encrypting data sent between the reader and the tag.

From the explanation of this RFID challenge response authentication scheme, one can see that the security of this protocol relies on the level of security offered by the method of generating those challenge response messages and its contents. By making use of chaos in the generation of those challenges and responses, it is demonstrated later in this chapter that the level of security offered is high given the low hardware resource requirements. This novel way of making use of analog chaos in digital system is the primary reason why such accomplishment is possible. In order to demonstrate how these challenge response messages can be generated from Lorenz chaotic dynamical system, one has to first understand the composition of such chaotic system and its characteristics. The following sections will provide a brief overview on this subject.

3.2 Lorenz dynamical system

Lorenz's chaotic dynamical system is one of the more well known and researched chaotic system. Partly because it is one of the earliest chaotic system discovered and also because of its wide variety in behaviour depending on its system parameters. Originally in 1963, when Edward Lorenz published his paper called "Deterministic nonperiodic flow", he used his model in an attempt to determine the pattern of atmospheric convection flow. Ever since then, Lorenz's dynamical system has been applied to numerous other real world systems. Similar to other chaotic systems, the Lorenz dynamical system is defined

by a set of ordinary differential equations:

$$\begin{aligned} \frac{dx}{dt} &= \sigma(y - x) \\ \frac{dy}{dt} &= x(\rho - z) - y \\ \frac{dz}{dt} &= xy - \beta z \end{aligned} \tag{3.1}$$

This system has initial conditions at time $t = t_0$, $x = x_0$, $y = y_0$ and $z = z_0$. The values σ (Prandtl), ρ (Rayleigh) and β are static parameters of the Lorenz dynamical system. It is important to note that x, y and z do not refer to x, y and z in three dimensional space [49]. Rather, they are defined as:

- x: Relative speed of air convection
- y: Temperature difference between rising warm air and falling cold air
- z: Measurement of lateral temperature difference

Similarly, the σ, ρ and β parameters are related to Lorenz's air convection model. Following a paper previously published by Barry Salzman on thermal turbulances [66], Lorenz adopted the system parameter values of $\sigma = 10$, $\rho = 28$ and $\beta = 8/3$ in his numerical evaluation of the system output. For those values, it has been demonstrated that Lorenz's dynamical system do indeed behave chaotically [5][71][34]. Figure 3.2 shows the well-known Lorenz butterfly attractor pattern that is a classic example demonstrating the sophisticated trajectory of Lorenz's dynamical system in its chaotic region.

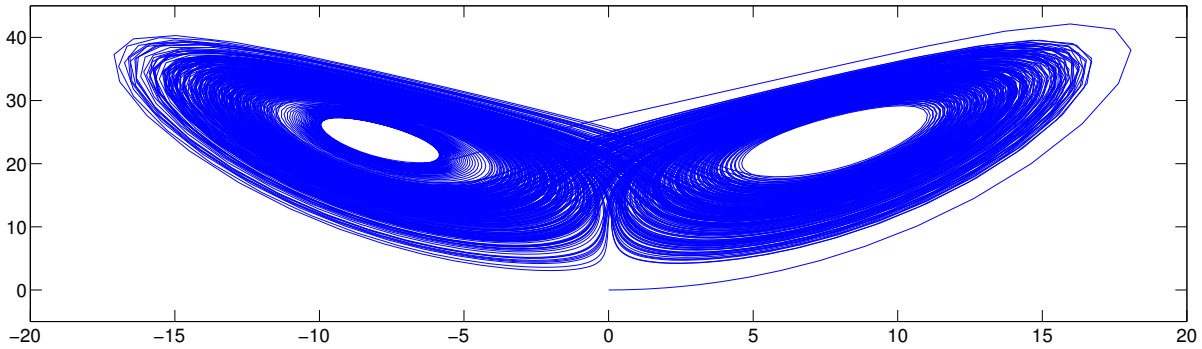


Figure 3.2: Plot of $x - z$ showing the Lorenz butterfly attractor

Recalling the sensitive to initial conditions property of chaotic systems. The trajectory of the Lorenz dynamical system is impossible to predict when it is operating in

its chaotic region. The set of its initial conditions and system parameters completely define its trajectory, which means that given the exact same input values to the Lorenz dynamical system, it will always follow the same trajectory. When these two observations are applied together, they provide an ideal method for use in cryptography. In my proposed RFID authentication scheme, the challenge messages are the set of Lorenz initial conditions and system parameters and the expected responses are the x, y and z state values of a particular point along this Lorenz chaotic trajectory. Given a Lorenz dynamical system operating in its chaotic region, the state progressions along its trajectory is extremely complex and this fact provides the security challenges needed to make it my proposed RFID authentication scheme secure.

As demonstrated in the previous chapter, for bandlimited frequency applications such as RFID, one cannot simply transmit an analog chaotic signal over the air. This means that a direct application of Lorenz dynamical system is not a possibility for use in RFID. Because of this limitation, a discrete version of the Lorenz dynamical system has to be used. This is accomplished by utilizing the fourth order Runge Kutta approximation method to calculate each state transition of the chaotic trajectory in digital hardware. The following section demonstrates this implementation in FPGA and confirms that the hardware resource required falls well within current passive RFID tag manufacturing limits. Furthermore, when compared with other AES FPGA implementations, it occupies much less Xilinx Virtex slices and requires less clock cycles to perform each Lorenz state calculation.

3.3 States generation

The first step in the realization of the Lorenz dynamic system in digital hardware is to apply an approximation of its state calculations. Given the three sets of ordinary differential equations that defines the Lorenz dynamic system, approximation of Lorenz states x, y and z can be performed by applying the fourth order Runge-Kutta method. Let:

$$F(t, v) = \frac{dv}{dt} \tag{3.2}$$

where, $v = [x, y, z]$ and x, y and z correspond to the three states of the Lorenz dynamic system. Let h be each time step of the fourth order Runge-Kutta method. Hence:

$$x_{i+1} = x_{i+h} \tag{3.3}$$

The approximate next state value v_{i+1} is given by:

$$v_{i+1} = v_i + h \times \frac{1}{6}(k_1 + 2k_2 + 2k_3 + k_4) \tag{3.4}$$

where,

$$\begin{aligned} k_1 &= h \times f(t_i, v_i) \\ k_2 &= h \times f\left(t_i + \frac{h}{2}, v_i + \frac{k_1}{2}\right) \\ k_3 &= h \times f\left(t_i + \frac{h}{2}, v_i + \frac{k_2}{2}\right) \\ k_4 &= h \times f(t_i + h, v_i + k_3) \end{aligned} \tag{3.5}$$

With the repeated application of the fourth order Runge-Kutta method, a trajectory of the Lorenz dynamic system can be traced and the x, y and z states of the Lorenz dynamic system can be obtained. On a passive RFID tag, the type of resources available for implementing the Lorenz dynamical system is different from a software type of implementation done on a microprocessor based system running high-level computer language. The limited number of logic gates on a RFID tag means that the only hardware resources available are bitwise logical operations. Similarly, on a FPGA, those mathematical operations have to be performed by logic implemented via look-up tables and flip-flops inside configurable logic blocks called slices. In order to represent fractional numbers and perform fractional mathematical operations with limited digital hardware resources, the floating point number representation method was used to achieve this goal.

3.4 Number format representation

Floating-point representation, as the name implies, has a floating decimal point based on the magnitude of the value to be represented in powers of two. Figure 3.3 shows a graphical view of the single precision IEEE-754 floating point number representation format.

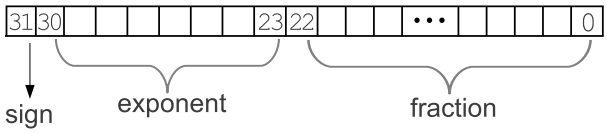


Figure 3.3: IEEE-754 single precision format

There is a total of 32 bits for each number with the first bit being a sign bit, the following 8 bits being the exponent and the last 23 bits represent the fractional part of the number. To quickly demonstrate the way how to convert a decimal number with a fractional part into IEEE-754 single precision format, let us look at an example.

Given decimal number 54.625. The whole part of the number is first converted into binary representation:

$$54_{10} = 110110_2$$

Then the fractional part is converted into binary. Given the limit of 23 fraction bits for the IEEE-754 single precision format, the maximum precision possible for a single precision floating point number is also 23 bits.

$$\begin{aligned} 0.625_{10} &= \sum_{n=1}^{23} d_n \times 2^{-n} \\ &= [(1 \times 2^{-1}) + (0 \times 2^{-2}) + (1 \times 2^{-3})] \\ &= 101_2 \end{aligned}$$

Hence:

$$54.625_{10} = 110110.101_2$$

The next step is to normalize this binary number:

$$110110.101 = 1.10110101 \times 2^{exponent-127}$$

Therefore, the exponent is $127 + 5$ and fraction is 10110101_2. This gives a final single precision number of:

$$0\ 10000100\ 10110101000000000000000_2$$

This floating point format has the flexibility of representing a wide range of numbers and can provide up to 24 significant bits of accuracy. To actually perform the required addition, subtraction and multiplication in FPGA, Xilinx do offer an IP core optimized for the calculation of floating point numbers. The Xilinx floating-point arithmetic core v5.2 uses either solely FPGA fabric resources or a combination of FPGA fabric and specialize DSP48 blocks. Since the goal of this FPGA implementation is to approximate

actual hardware resource usage on a passive RFID tag, it is important to not use any specialized resources of the Virtex FPGA in order to make the resource usage estimatate as accurate and as straightforward as possible for the ease of comparing different RFID authentication method.

From the evaluation of other fractional number representation methods, such as fixed point number representation, it was found that the amount of resource savings, when implemented in hardware, does not justify the lost of significant bits. For that reason, the Xilinx floating-point arithmetic core was the best method in performing fractional calculations on an FPGA.

3.5 Implementation on FPGA

In actual RFID applications, cost is a major factor in the practical usefulness of any authentication scheme. In a direct implementation of the fourth order Runge Kutta approximation on FPGA, the amount of resources can quickly add up. Table 3.1 summarizes the total number of mathematical operations required for the approximation of each Lorenz chaotic states x, y and z. One quickly realizes that the direct implementation of 16 subtractions, 21 additions, 25 multiplications and 9 division operations will never fit into a passive RFID tag. However, by optimizing the mathematical operations performed and using implementation area focused hardware design techniques, the amount of hardware resources required can be drastically reduced. As a first step in reducing design size, one can observe that the second operand of the division operations are always fixed at 2 and 6. Those can be replaced by corresponding multiplication operations of 0.5 and 0.1666667 respectively. By doing so, an instantiation of the Xilinx floating point arithmetic core performing division operations can be eliminated. Since the time step value h is always fixed, the results of the $h/2$ and $h/6$ operations never change during Lorenz chaotic state calculations. Therefore, those values can be stored in the tag's memory to further reduce design complexity. For the addition and subtraction instantiations of the Xilinx floating point arithmetic core, the same hardware resources are shared and the selection of the operation to be performed depends only on a $6 - bit$ wide signal called *operation*. The means that the most resource efficient design only requires one addition/subtraction and one multiplication Xilinx floating point arithmetic core. Then, by rearranging the order of performing the fourth order Runge Kutta operation, it is possible to calculate one full set of Lorenz dynamical system states x, y and z

Operations to perform	$+$	$-$	$\times$	$\div$
$\frac{dx}{dt} = \sigma(y - x)$ for $K1$ step		1	1	
$\frac{dy}{dt} = x(\rho - z) - y$ for $K1$ step		2	1	
$\frac{dz}{dt} = xy - \beta z$ for $K1$ step		1	2	
$x_i + \frac{x_{k1}}{2}$ for x in $K2$	1			1
$y_i + \frac{y_{k1}}{2}$ for y in $K2$	1			1
$z_i + \frac{z_{k1}}{2}$ for z in $K2$	1			1
$\frac{dx}{dt} = \sigma(y - x)$ for $K2$ step		1	1	
$\frac{dy}{dt} = x(\rho - z) - y$ for $K2$ step		2	1	
$\frac{dz}{dt} = xy - \beta z$ for $K2$ step		1	2	
$x_i + \frac{x_{k2}}{2}$ for x in $K3$	1			1
$y_i + \frac{y_{k2}}{2}$ for y in $K3$	1			1
$z_i + \frac{z_{k2}}{2}$ for z in $K3$	1			1
$\frac{dx}{dt} = \sigma(y - x)$ for $K3$ step		1	1	
$\frac{dy}{dt} = x(\rho - z) - y$ for $K3$ step		2	1	
$\frac{dz}{dt} = xy - \beta z$ for $K3$ step		1	2	
$x_i + x_{k3}$ for x in $K4$	1			
$y_i + y_{k3}$ for y in $K4$	1			
$z_i + z_{k3}$ for z in $K4$	1			
$\frac{dx}{dt} = \sigma(y - x)$ for $K4$ step		1	1	
$\frac{dy}{dt} = x(\rho - z) - y$ for $K4$ step		2	1	
$\frac{dz}{dt} = xy - \beta z$ for $K4$ step		1	2	
$x_i + \frac{h}{6}(x_{k1} + 2x_{k2} + 2x_{k3} + x_{k4})$ for final step	4		3	1
$y_i + \frac{h}{6}(y_{k1} + 2y_{k2} + 2y_{k3} + y_{k4})$ for final step	4		3	1
$y_i + \frac{h}{6}(z_{k1} + 2z_{k2} + 2z_{k3} + z_{k4})$ for final step	4		3	1
Total	**21**	**16**	**25**	**9**

Table 3.1: Table showing mathematical operations required

in 57 clock cycles. This is illustrated in a step-by-step approach in table 3.2. Using the Xilinx ISE development platform tools version 13.3, the entire design was successfully synthesized over the smallest version of Xilinx Virtex 6 FPGA, the xc6vlx75t. In order to accomplish the reuse of Xilinx floating point arithmetic cores as shown in table 3.2, the hierarchy of each K step has been removed and a flattened design was used. Figure 3.4 shows the inputs to and outputs of the top level design.

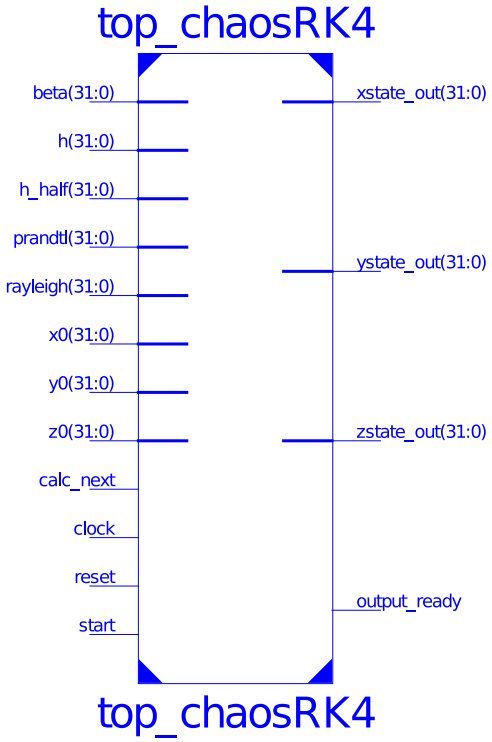


Figure 3.4: Inputs and outputs of the FPGA implementation

The *top_ chaosRK4* HDL module contains a Moore-type state machine to control the order of each mathematical operation in the fourth order Runge Kutta approximation and there is a total of 18 states within the flow control state machine. A flow chart of the processes inside the FPGA implementation is shown in figure 3.5 and a simulation in Xilinx ISim is shown in figure 3.6.

Clock Cycle	Operation performed by		Clock Cycle	Operation performed by	
	Add/Sub Core	Mult Core		Add/Sub Core	Mult Core
1	$y - x = x_a$	$x \cdot y = z_a$	20	$y_b - y$	$\sigma \cdot x_a$
2	$\rho - z = y_a$	$\beta \cdot z = z_b$	21		$x_{K3} \cdot h_{half} = x_{K3h}$
3	$z_a - z_b$	$x \cdot y_a = y_b$	22	$x_{K3h} + x_n = x_{K4}$	$y_{K3} \cdot h_{half} = y_{K3h}$
4	$y_b - y$	$\sigma \cdot x_a$	23	$y_{K3h} + y_n = y_{K4}$	$z_{K3} \cdot h_{half} = z_{K3h}$
5		$x_{K1} \cdot h_{half} = x_{K1h}$	24	$z_{K3h} + z_n = z_{K4}$	
6	$x_{K1h} + x_n = x_{K2}$	$y_{K1} \cdot h_{half} = y_{K1h}$	25		$2 \cdot x_{K2}$
7	$y_{K1h} + y_n = y_{K2}$	$z_{K1} \cdot h_{half} = z_{K1h}$	26	$x_{K1} + 2x_{K2} = x_{n+1}$	$2 \cdot x_{K3}$
8	$z_{K1h} + z_n = z_{K2}$		27	$x_{n+1} + 2x_{K3} = x_{n+1}$	$h \cdot 1/6 = h_{sixth}$
9	$y - x = x_a$	$x \cdot y = z_a$	28	$x_{n+1} + x_{K4} = x_{n+1}$	
10	$\rho - z = y_a$	$\beta \cdot z = z_b$	29		$h_{sixth} \cdot x_{n+1} = x_{n+1}$
11	$z_a - z_b$	$x \cdot y_a = y_b$	30	$x_{n+1} + x_n = x_{n+1}$	$2 \cdot y_{K2}$
12	$y_b - y$	$\sigma \cdot x_a$	31	$y_{K1} + 2y_{K2} = y_{n+1}$	$2 \cdot y_{K3}$
13		$x_{K2} \cdot h_{half} = x_{K2h}$	32	$y_{n+1} + 2y_{K3} = y_{n+1}$	$h \cdot 1/6 = h_{sixth}$
14	$x_{K2h} + x_n = x_{K3}$	$y_{K2} \cdot h_{half} = y_{K2h}$	33	$y_{n+1} + y_{K4} = y_{n+1}$	
15	$y_{K2h} + y_n = y_{K3}$	$z_{K2} \cdot h_{half} = z_{K2h}$	34		$h_{sixth} \cdot y_{n+1} = y_{n+1}$
16	$z_{K2h} + z_n = z_{K3}$		35	$y_{n+1} + y_n = y_{n+1}$	$2 \cdot z_{K2}$
17	$y - x = x_a$	$x \cdot y = z_a$	36	$z_{K1} + 2z_{K2} = z_{n+1}$	$2 \cdot z_{K3}$
18	$\rho - z = y_a$	$\beta \cdot z = z_b$	37	$z_{n+1} + 2z_{K3} = z_{n+1}$	$h \cdot 1/6 = h_{sixth}$
19	$z_a - z_b$	$x \cdot y_a = y_b$	38	$z_{n+1} + z_{K4} = z_{n+1}$	
			39		$h_{sixth} \cdot z_{n+1} = z_{n+1}$
			40	$z_{n+1} + z_n = z_{n+1}$	

Table 3.2: Table showing RK-4 calculation flow

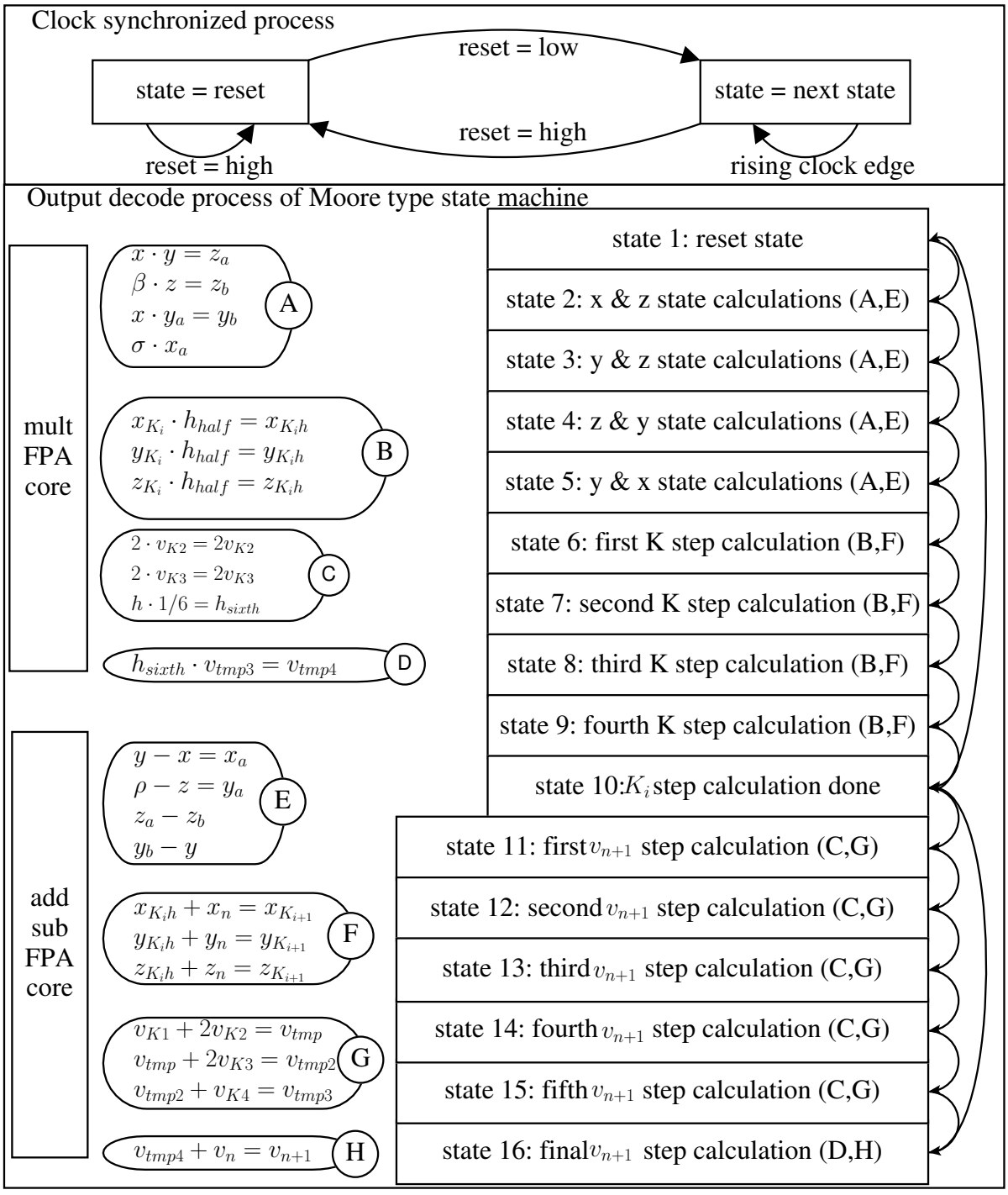


Figure 3.5: FPGA implementation state machine

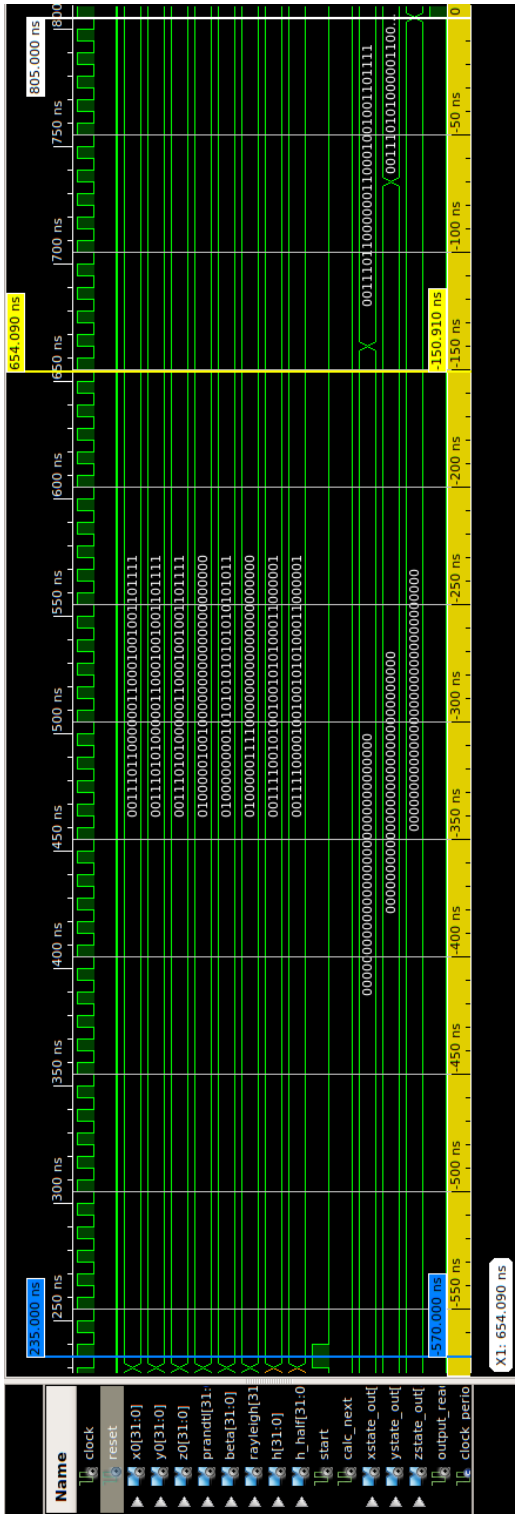


Figure 3.6: Xilinx ISim simulation of the Lorenz chaotic engine

The inputs to the discrete Lorenz chaotic engine are σ, ρ, β, initial conditions x_0, y_0, z_0 and the pre-calculated fourth order Runge Kutta time step values h and $h/2$. All numbers follow the floating point number format and are 32-bit long. When signal *start* goes high, the Lorenz chaotic engine commences its calculations by stepping into its state machine. After all the required calculation are completed for obtaining the next state values of x_{n+1}, y_{n+1} and z_{n+1}, signal *output_rdy* goes high to reflect this result. For the purpose of simulating the design, a default clock period of $10ns$ was used. It can be seen from figure 3.6 that the time required for the generation of each state is $570ns$. This verifies the earlier claim that each Lorenz chaotic state generation can be performed in $570ns/10ns \approx 57$ clock cycles.

The correctness of the states generated by the Lorenz chaotic engine was confirmed by using Xilinx ISim and Matlab. With initial conditions $x_0 = 0.002, y_0 = 0.001, z_0 = 0.001$, time step of $h = 0.001$ and $\sigma = 10, \rho = 3/8, \beta = 28$, x, actual states represented in IEEE-754 single precision format are generated from the Lorenz chaotic engine and are written into a hex file. Using Matlab, a *m-file* script was created to convert those single precision formatted x states into decimal floating-point representation for ease of manipulation within Matlab. Figure 3.7 shows those decimal floating-point x state values plotted against time in steps of $h = 0.001$ increments.

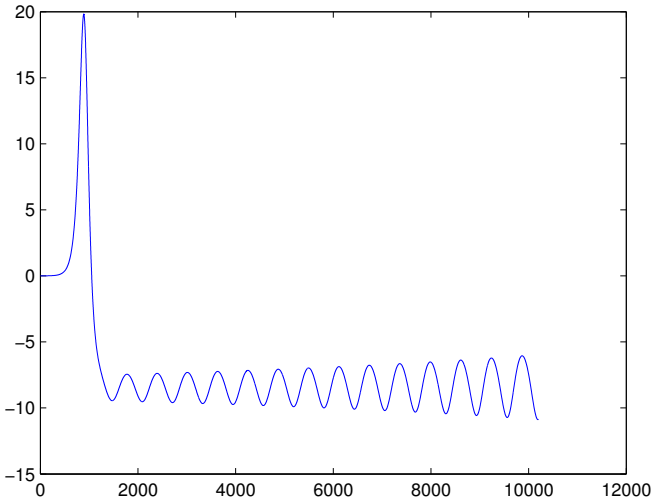


Figure 3.7: Plot of x states generated by our HDL chaotic engine versus time in h time increments

This output matches exactly those x states that were generated with Matlab and therefore, confirms the proper functioning of the design of the Lorenz chaotic engine in FPGA.

3.5.1 Performance and resource utilization

The resource utilization level of this Lorenz chaotic engine implementation on FPGA is considerably more efficient than RFID authentication methods such as AES. In table 3.3, one can see that the number of Xilinx slice used is considerably lower with the challenge response authentication scheme based on Lorenz chaotic system.

Authentication Scheme	**Xilinx slice usage**
based on Lorenz chaotic system	469
based on AES [16]	5673

Table 3.3: Lorenz chaotic engine device utilization on Virtex 6 xc6vlx75t FPGA

When implemented on the smallest version of the Xilinx Virtex 6 FPGA, the xc6vlx75t, figure 3.8 shows the post place and route view of the physical FPGA. It can be seen that the entire implementation barely used 1/24th of the space available.

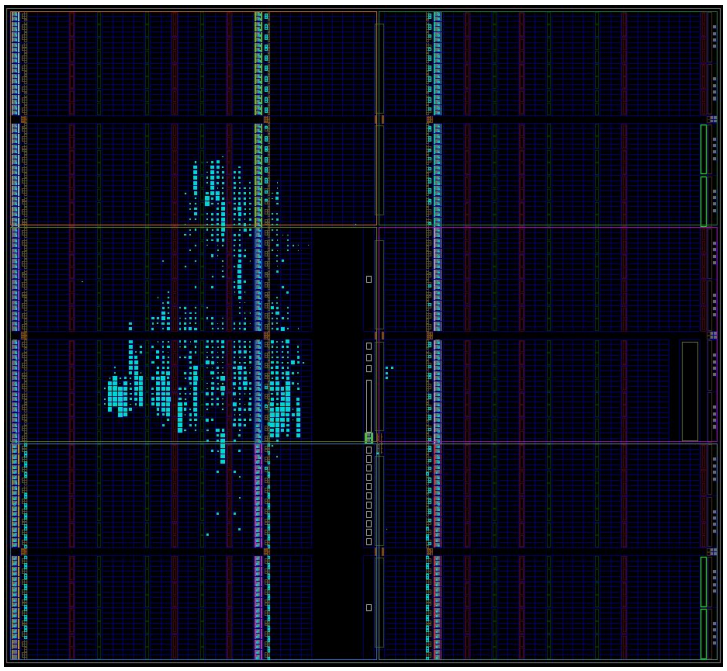


Figure 3.8: Post place and route view of the design on Xilinx Virtex 6 xc6vlx75t

Currently, one of the most efficient AES RFID encryption method suggested that included hardware resource evaluation requires 1000 clock cycles to encrypt each 128-bit block [18]. Another AES based RFID authentication method uses 356 clock cycles per encryption of 128 bits but is of theoretical nature without concrete implementation [59]. The 57 clock cycle performance of the Lorenz chaotic engine is many times faster and can make the authentication of multiple RFID tags possible in real world implementation. The most widely used passive RFID tags with encryption capabilities follows the ISO-14443 and ISO-15693 international standards. Both of these standards have a carrier frequency of $13.56Mhz$ for signal transmission. For unencrypted RFID tags, they mostly operate with a $125Khz$ carrier frequency. On a passive RFID tag, the clock of the internal integrated circuits often run at the same frequency as the carrier frequency with the help of a phase-locked loop circuit. This also means that RFID authentication circuitry would also run at the same frequency as the carrier frequency. The effective duration for the authentication of the tag is:

$$\begin{aligned} t_{tag} &= 57 \cdot (1/13.56 \times 10^6) \\ &= 4.204\mu sec \end{aligned}$$

Similarly, the time required for the authentication of the reader is also $4.13\mu sec$. The total time required for each authentication of both the reader and the tag is:

$$\begin{aligned} t_{auth} &= t_{tag} + t_{reader} \\ &= 4.204\mu sec \times 2 \\ &= 8.408\mu sec \end{aligned}$$

In a typical RFID authentication session, this delay is very short and makes simultaneous RFID authentication of multiple tags possible.

3.6 Secret key

One distinguishing observation from the majority of chaotic ciphers suggested is the lack of detail implementation methods for concrete practical use. The sole effort of demonstrating a single narrow focused aspect of chaos for digital communications is one of the reason the lack of depth in presentation has hindered the wider acceptance of chaos in cryptography. In my proposed Lorenz chaotic RFID authentication scheme, the key serves the secret between a transmitting device and a receiving device. This secret key

is composed of Lorenz dynamic system parameters and initial conditions x_0, y_0, and z_0. But because of the unique characteristics of chaos, there are many questions that need to be answered in order to translate those Lorenz dynamical system parameters and initial conditions into a binary secret key that can be used in real world RFID implementations.

1. What are the implications of selecting a finer or corser fourth order Runge Kutta time step h?

2. Does the entire range of Lorenz dynamical system parameters and initial conditions offer the same level of security?

3. Given that the security of the Lorenz based authentication scheme relies on the chaotic behaviour of the Lorenz dynamical system, there has to be a method to ensure that chaotic behaviour is maintained for all possible key values.

Figure 3.9 shows an $x-y$ plot of a Lorenz dynamical system with $t_s = 0.001$, $\rho = 28, \sigma = 10, \beta = 8/3$ and initial conditions at $x_0 = 0.1, y_0 = 0.1, z_0 = 0.1$.

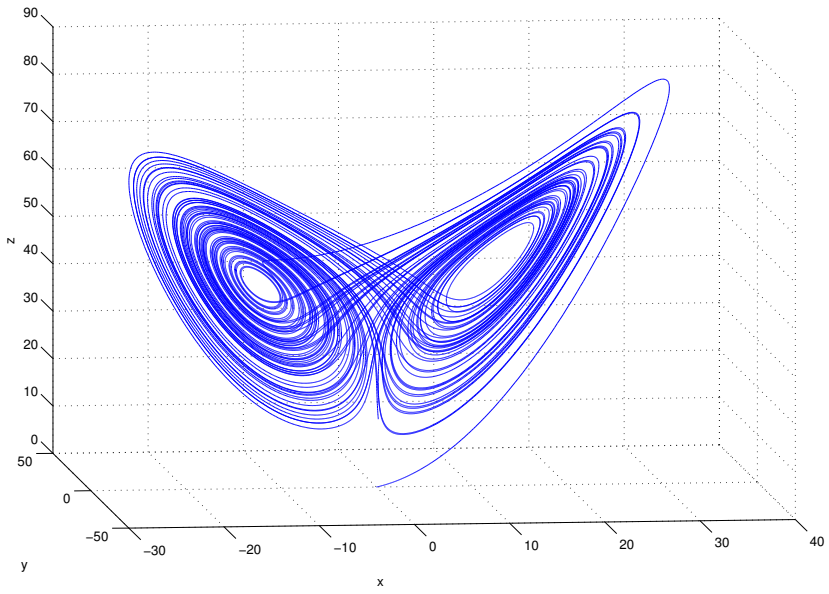


Figure 3.9: Plot of strange attractor with parameters $\sigma = 10$, $\rho = 28$, $\beta = 8/3$ and initial conditions $x_0 = 0.1$, $y_0 = 0.1$, $z_0 = 0.1$

From the appearance of the orbits, the system seems to be in its strange attractor state. However, the mere appearance of a strange attractor does little to solidify the

chaotic behaviour and is not acceptable as proof. From my research, it was discovered that in order to satisfy the above questions, the following boundaries and selection of specific values were made:

1. The time step value $h = 0.0201$ is the optimal time step in the fourth order Runge Kutta approximation that provides the maximum key space.

2. System parameter ρ bounded by $24.06 < \rho < 99.5$ and initial conditions $0 < x < 170$, $0 < y < 170$, $0 < z < 170$ will ensure sustained chaotic behaviour in the Lorenz dynamical system.

Given those Lorenz dynamical system boundaries, it was found that chaotic behaviour was consistently maintained. This is the most crucial requirement in ensuring the security of the chaos based RFID authentication protocol. The following sections will demonstrate the proofs behind the selection of those chosen system parameter and initial conditions boundaries. We begin by first providing an understanding of how to quantify when chaotic behaviour is present by explaining the Lyapunov exponent, which is a key characteristic of chaotic systems.

3.6.1 Lyapunov exponent

The Lyapunov exponent is given as the rate of divergence between two trajectories $x(t)$ and $x'(t)$. The first trajectory $x(t)$ has initial conditions $x(0)$, and the second trajectory $x'(t)$ has initial conditions $x'(0)$. Given a very small difference between $x(0)$ and $x'(0)$, there will be a set of Lyapunov exponents that is called a Lypapunov spectrum characterizing the rate of divergence of each stage of the dynamic system. The number of Lyapunov exponent(s) of a given dynamical system is determined by its dimension. For a one dimensional map such as the logistic map, there is exactly one Lyapunov exponent. Given $\Delta(t)$ to be the difference in distance between a reference trajectory and a disturbed trajectory in a chaotic attractor, the maximum Lyapunov exponent λ_{max} is given by:

$$\lambda_{max} = \lim_{x \to \infty} \lim_{\Delta(0) \to 0} \frac{1}{t} \ln \left(\frac{\Delta(t)}{\Delta(0)} \right) \tag{3.6}$$

In our case, the Lorenz chaotic dynamical system in three dimensions will have three Lyapunov exponents, each corresponding to the x, y and z phase space. A positive Lyapunov exponent tells us that the dynamical system in that particular phase space

behaves chaotically. On the other hand, if the Lyapunov exponent approaches zero, that dynamical system is said to be periodic. Finally, if the Lyapunov exponent is negative, the dynamical system approaches to a single point in space. From the combination of the three Lyapunov exponents of a Lorenz dynamical system, we can get a sense of the attractor form. Namely, if it is $(+, 0, -)$ then the dynamical system has a strange attractor orbit, which shows the signature butterfly form in the $x - z$ plane; if it is $(0, 0, -)$, the dynamical system has a two-torus orbit, which is a trajectory rotating between two stable points; if it is $(0, -, -)$, the dynamical system has a limit-cycle orbit, which is a type of periodic orbit; if it is $(-, -, -)$, the dynamical system simply approaches a fixed point in space.

From this observation, it is obvious to note that the only state in the Lorenz dynamic system that can be used as part of a secret key are the Lorenz dynamical system x states because it is the only state that has a positive maximum Lyapunov exponent. In addition, to ensure that x states remain chaotic, the trajectory of the Lorenz dynamic system should follow a strange attractor orbit permanently. Therefore, the chaotic behaviour of the Lorenz dynamical system relies on not just one single system parameter but rather the combination of the all system parameters and initial conditions.

For concretely calculating the Lyapunov exponent of the hardware implemented Lorenz dynamical system, an analytical approach in solving for the maximum Lyapunov exponent is not going to provide the necessary proof of chaos. The reason is because analytical methods suggested for continuous time Lorenz dynamical systems do not take into account the imperfections introduced by approximating Lorenz dynamical system states using the fourth order Runge Kutta method. To solve this problem, numerical method is used instead to calculate the Lyapunov exponent from the states obtained in the FPGA implementation.
The task of calculating Lyapunov exponents from experimental data is drastically different than calculation by analytic means. There has been a few papers written on this subject and there currently exists primarily two methods of approaching this problem: Jacobian-based methods and direct methods. The first approach requires the knowledge of the equations of the underlying system by fitting the experimental time series data obtained into such model. The second approach [75] and [63] uses the exponential divergence between two closely located points of the orbit to estimate the Lyapunov exponent of the system from its time series data. The latter is, by far, the most widely used

method in determining the Lyapunov exponent from a time series and there has been a few modifications to it over the years. For the evaluation of chaotic behaviour in the hardware implemented Lorenz chaotic engine, the second method will be used to find the maximum Lyapunov exponent from generated Lorenz states.

Wolf's method

In [75], Wolf et al. showed that for two points in a dynamical system that are either on two different orbits or that are within the same orbit but separated in time by at least one orbital cycle, will diverge exponentially if the system is chaotic. To perform the estimation of the Lyapunov exponents, a fiducial trajectory is selected ,which begins at time t_0. Then another point $L(t_0)$ is selected, satisfying the above mentioned criteria. Given θ_M is the orientation error between the point on the fiducial trajectory and the point on the other orbit and t_r is the time between replacements of the point $L(t_0)$ after it has exceeded the maximum distance between itself and the point on the fiducial trajectory; the relative error in estimating λ_1 is:

$$\theta_M{}^2/\lambda_1 t_r \tag{3.7}$$

In a dynamical system, one can observe that the faster the decay of the orientation error θ_M, the more chaotic a system is and that chaotic behaviour is guaranteed.

Rosenstein's method

In [63], Rosenstein's method is based on [67] and is basically a generalization of Sato's approach with improvements in calculation efficiency. The Lyapunov exponents are estimated by using the prediction error $p(k)$ given by

$$p(k) = \frac{1}{Nt_s}\sum_{n=1}^{N}\log_2\left(\frac{||y^{n+k} - y^{nn+k}||}{||y^n - y^{nn}||}\right) \tag{3.8}$$

where y^{nn} is the nearest neighbour of y^n, k is the number of time steps and t_s is the actual value of the time step. When the prediction error is plotted against time step k, a linear approximation of the curve from the beginning of k where the distance of two points grow exponentially by $\exp^{(\lambda t_s k)}$ to a stage where the linear approximation exceeds the reference orbit y^{n+k} [72] gives the approximate value of the Lyapunov exponent.

For the implementation of those two methods in determining the Lyapunov exponents, there are tools developed in software that uses [75], [67] and [63] to perform this task.

They are the TISEAN package developed for the UNIX operating system and TSTool developed for running inside Matlab. Given a reference point s_{n0} and a neighbourhood of surrounding points $U(s_{n0})$ within a diameter ϵ, the maximum Lyapunov exponent can be approximated by fitting a linear model to $S(\Delta n)$ where

$$S(\Delta n) = \frac{1}{N}\sum_{n_0=1}^{N} ln\left(\frac{1}{|U(s_{n0}))|}\sum_{s_n \in U(s_{n0})} |s_{n0+\Delta n} - s_{n+\Delta n}|\right) \tag{3.9}$$

The challenge in applying this method to accurately determining the maximum Lyapunov exponent rests in the selection of ϵ that is neither too big nor too small. This is because if the diameter of the sphere surrounding our reference point s_{n0} is too large, points from other unrelated orbital cycles would contaminate the accuracy of the exponential expansion of our reference point. Conversely, if the diameter of the sphere is too small, then the only points within our reference point sphere would only consist of that same reference point and this will not yield any meaningful results.

In TSTool, there is a significant shortcoming in the completeness of its implementation that does not allow the selection of this ϵ value. This problem is not present in the TISEAN toolset because it is possible to manually adjust the selection of ϵ. For this reason, subsequent Lyapunov calculations are conducted using the TISEAN toolset.

3.6.2 Optimal selection of time step h

The inaccuracy in the estimation of each fourth order Runge Kutta step can be seen as a small signal disturbance to the dynamical system. It is clear that as the time step chosen approaches the period of one single complete orbit around the strange attractor, the amount of disturbance increases and the likelihood of retained chaotic behaviour decreases. Also, before going into the discussion of the effects of Lorenz dynamical system parameters and initial conditions, one has to first clearly define a fixed and optimal time step h value since it is a component that does not change in the Lorenz chaotic system implementation. From my knowledge, no one has concretely shown this threshold where the noise from truncation error introduced by the fourth order Runge Kutta approximations becomes unacceptable and chaotic behaviour vanishes. With the bulk of research of discrete chaotic cryptosystems focusing mainly on piecewise linear chaotic maps, the majority of research focus has been on dynamical degradation of piecewise linear chaotic maps for discrete systems [47].

Another factor that the selection of time step h has on the behaviour of the discrete Lorenz chaotic system is the rate of divergence of two arbitrary trajectories. Given two discrete Lorenz chaotic systems A and B, the number of fourth order Runge Kutta approximation steps required for the two systems to significantly diverge is:

$$\Delta x_{nAB} = x_{nA} - x_{nB} \tag{3.10}$$

where n is each progression in the fourth order Runge Kutta approximations. From the very definition of chaos, sensitivity to initial conditions is one of the main characteristic in chaotic systems. Hence, it is obvious that the trajectory undertaken by system B will diverge from the path of system A given $(x_{a0}, y_{a0}, z_{a0}) \neq (x_{b0}, y_{b0}, z_{b0})$. Given the selection of a large value of h, the trajectory diversion time will be significantly less. However, the number of possible different values of x_0, y_0, z_0 and ρ will also be smaller. On the other, a smaller value of h will yield a longer system diversion time but will provide a larger pool of possible secret key values. For this reason, we need to find a citical h value that will provide maximum key space given a system diversion time that is acceptable for RFID use.

In order to determine what the change of time step h has on the overall behaviour of the Lorenz dynamical system, we begin by modifying only one state initial value (the y initial state value) by 0.001 and setting discrete time step to 0.001.

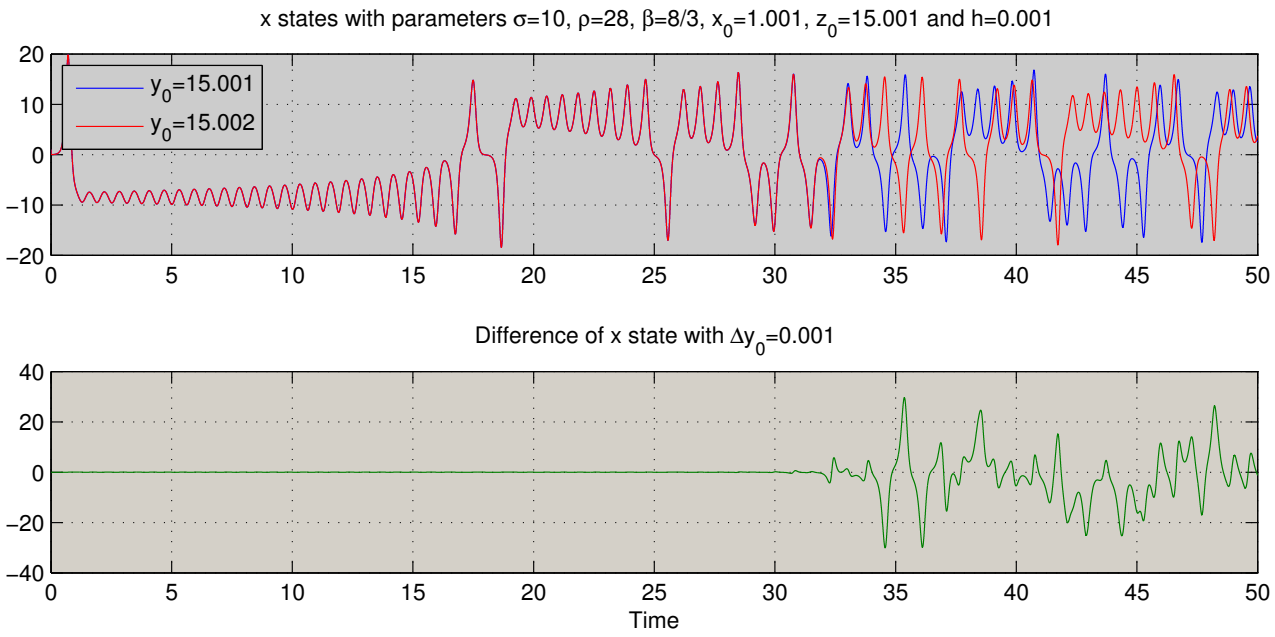


Figure 3.10: Plot of x states with parameters $\sigma = 10$, $\rho = 28$, $\beta = 8/3$, $x_0 = 1.001$, $z_0 = 15.001$ and $h = 0.001$

In figure 3.10, the top graph represents the x states of both systems. In the bottom graph, the difference between x_{ai} and x_{bi} where i is the time step, is displayed. Since the difference in initial conditions between the two system is very small, both systems behaves very closely with respect to each other. When $t > 35$, x states begin to diverge significantly between the two systems. In any type of chaotic cipher employing this type of discrete Lorenz chaotic system, the number of time steps required for divergence is an important parameter to take note of because we want to let the two system progress for some time in the event that an attacker was able to guess very closely to the actual initial conditions used.

Figure 3.11 shows the result of a finer time step h. As one would suspect, the outcome from going towards $h = 0.01$ shows a more rapid divergence in x states, which is closer to $t \approx 29$ compared with $t \approx 35$ previously.

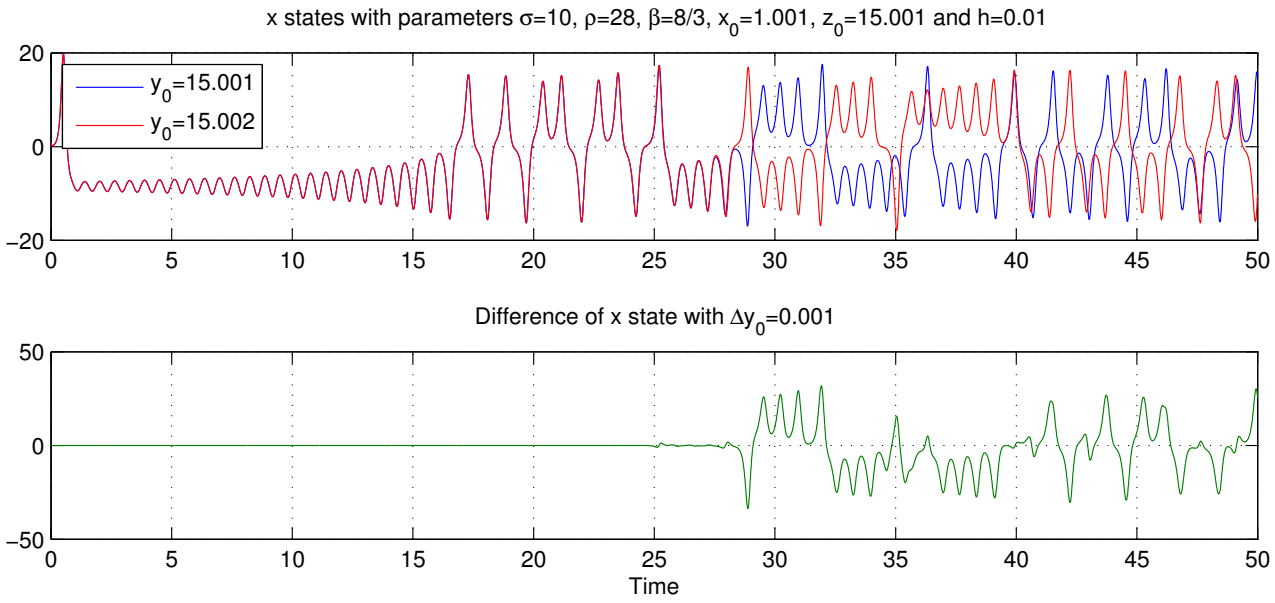


Figure 3.11: Plot of x states with parameters $\sigma = 10$, $\rho = 28$, $\beta = 8/3$, $x_0 = 1.001$, $z_0 = 15.001$ and $h = 0.01$

An important fact about the rate of divergence is the time that it takes for the calculation of all those intermediate states before divergence actually occurs. In resource constrained applications, this delay could render an authentication scheme to be too slow for practical use and also decrease the effective data rate in data obfuscation. The further apart we set this "resolution" of initial conditions, the faster divergence will occur. However, on the same token, the maximum number of possible x_0, y_0 and z_0 values will also decrease. In other words, the theoretical limit can be made as fine as one would like but the practical limit has to be much larger so that it is proportional to current hardware technological limits. The ultimate goal in selecting the optimal value for time step h therefore means the quickest divergence rate possible without the lost of chaotic behaviour.

By using the method of calculating the maximum Lyapunov exponent discussed earlier in this section, equation 3.9 is used in the determination of $S(\Delta n)$. For each different time step selection, a subsequent change of divergence of two arbitrary points can be seen in the plot of $S(\Delta n)$ vs $n \times h$ as shown in Figure 3.12. Applying linear approximation to find the best fitting slope in Figure 3.12, it can provide a good approximation of the sign of the Lyapunov exponent, which in turn will reveal whether the system is chaotic, peri-

odic or tends to a fixed point. Hence, from the positive slope of this plot, for $\Delta h = 0.001$, the x states of the discretized Lorenz dynamic system still behave chaotically.

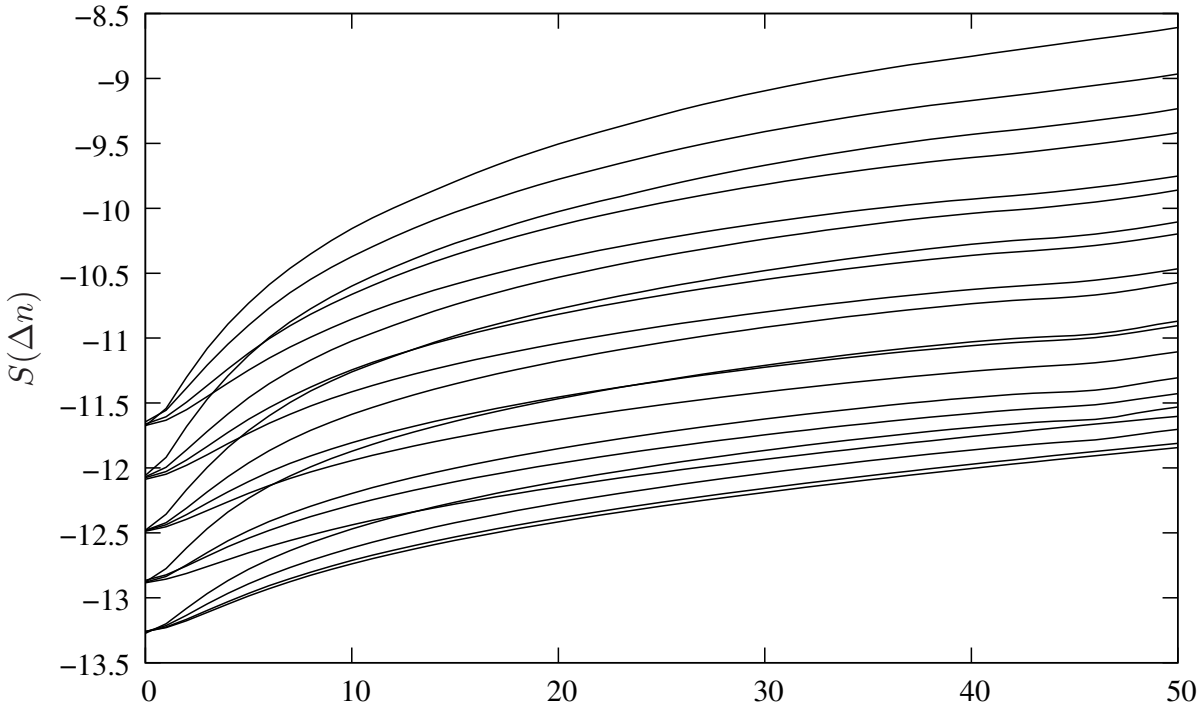


Figure 3.12: Plot of $S(\Delta n)$ with different values of ϵ having dimensions of 3, 4, 5, 6 and $\Delta h = 0.001$

In order to make the efficiency of the hardware implemented Lorenz chaotic engine as high as possible, the aim is evaluate the Lyapunov exponent from these numerical results and continually increase the fourth order Runge Kutta approximation time step until the point that chaotic behaviour is no longer present. By doing so, we effectively maximize the diffusion factor per time step of each calculated Lorenz state and increases the efficiency level of the cipher. Let us now reduce the accuracy of the forth order Runge Kutta approximation from $\Delta h = 0.001$ to $\Delta h = 0.1$ as shown in Figure 3.13.

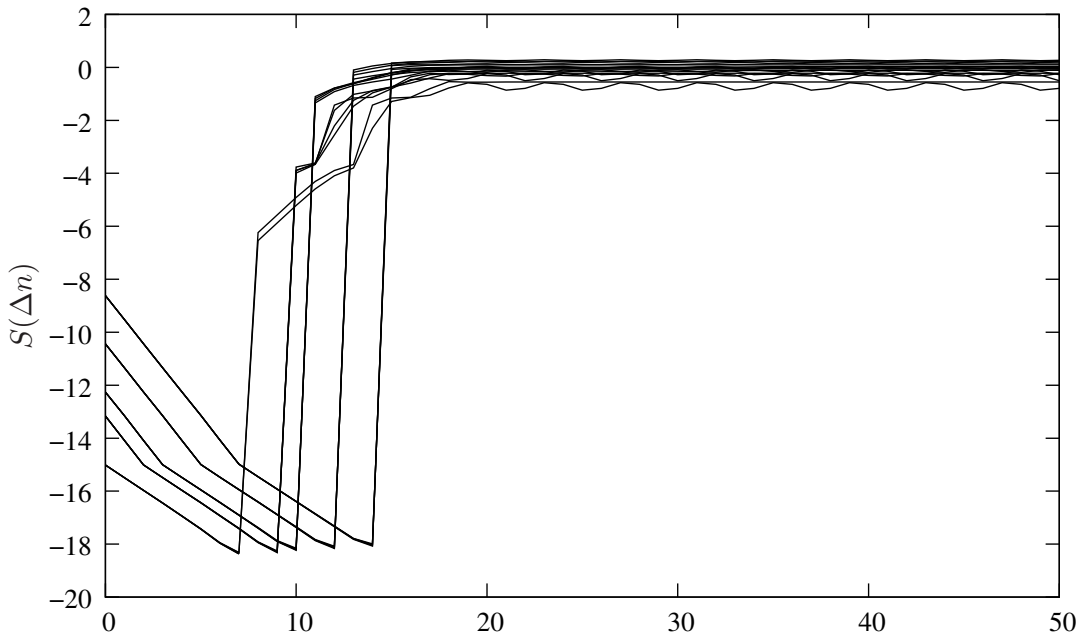
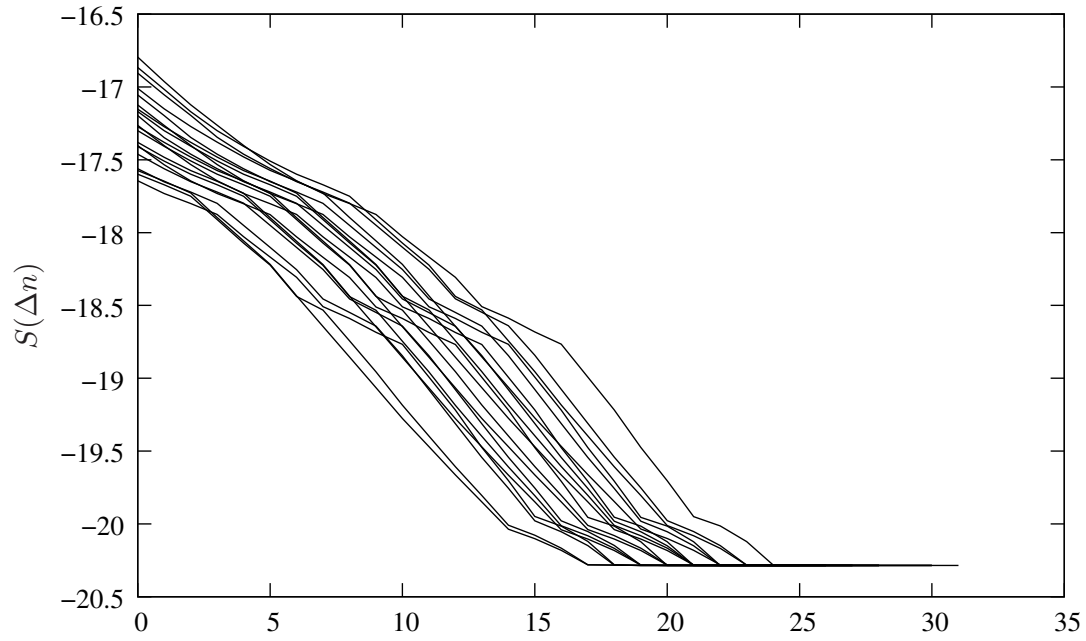
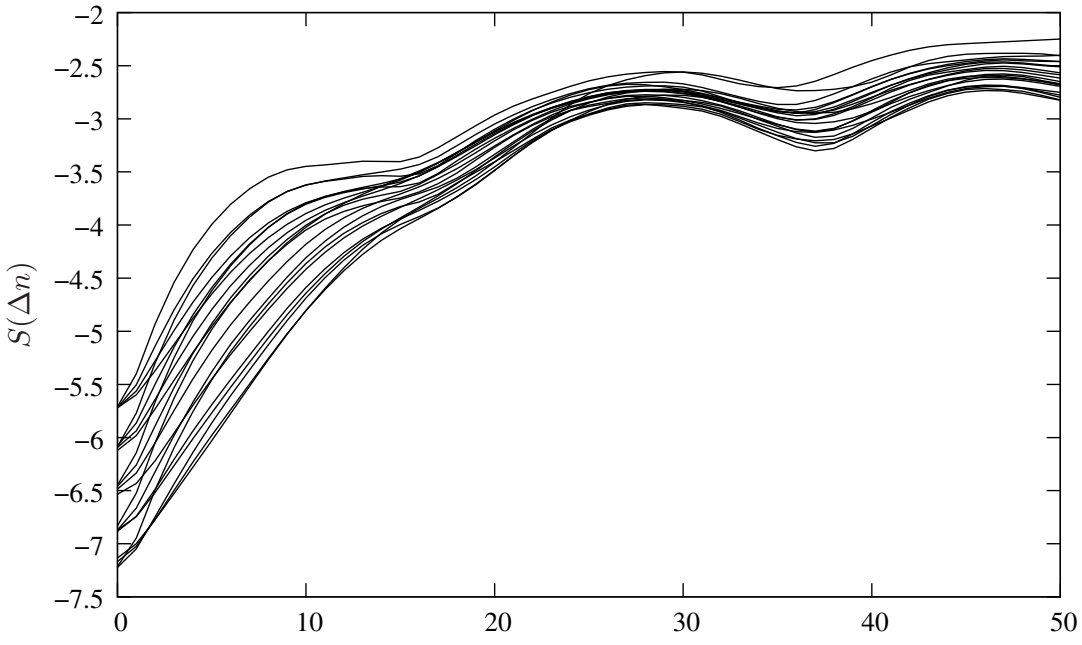


Figure 3.13: Plot of $S(\Delta n)$ with $\Delta h = 0.1$ having dimensions of 3, 4, 5 and 6

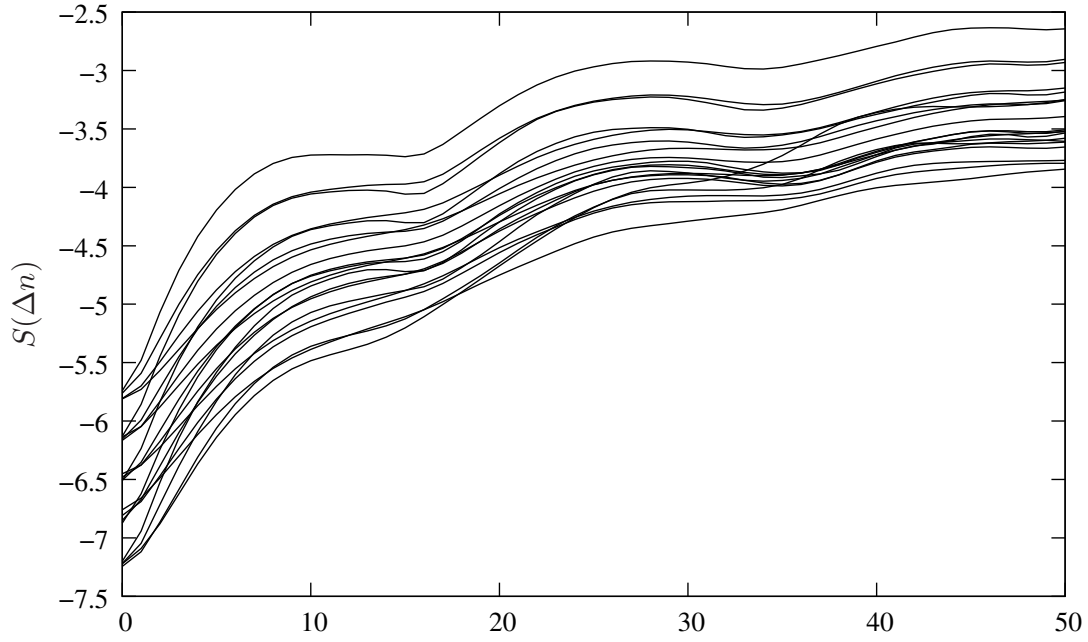
From looking at Figure 3.13, the x states first tend to a fixed point because of the negative slope between $0 < t < 10$. Then the slope becomes sharply positive indicating that the divergence of two arbitrary points increases exponentially for a short burst between $10 < t < 15$. Finally, when $15 < t < \infty$, the slope of the $S(\Delta n)$ vs t curve changes into a flat line, indicating that the trajectory of the x states has settled into a periodic region. Comparing Figure 3.12 and Figure 3.13, one can suspect that the threshold value of Δh, which changes the x states from chaotic to periodic, must be larger than 0.001 and less than 0.1. By undergoing a gradual increase in the forth order Runge Kutta accuracy, the resulting plots of $S(\Delta n)$ vs t are shown in figure 3.13.



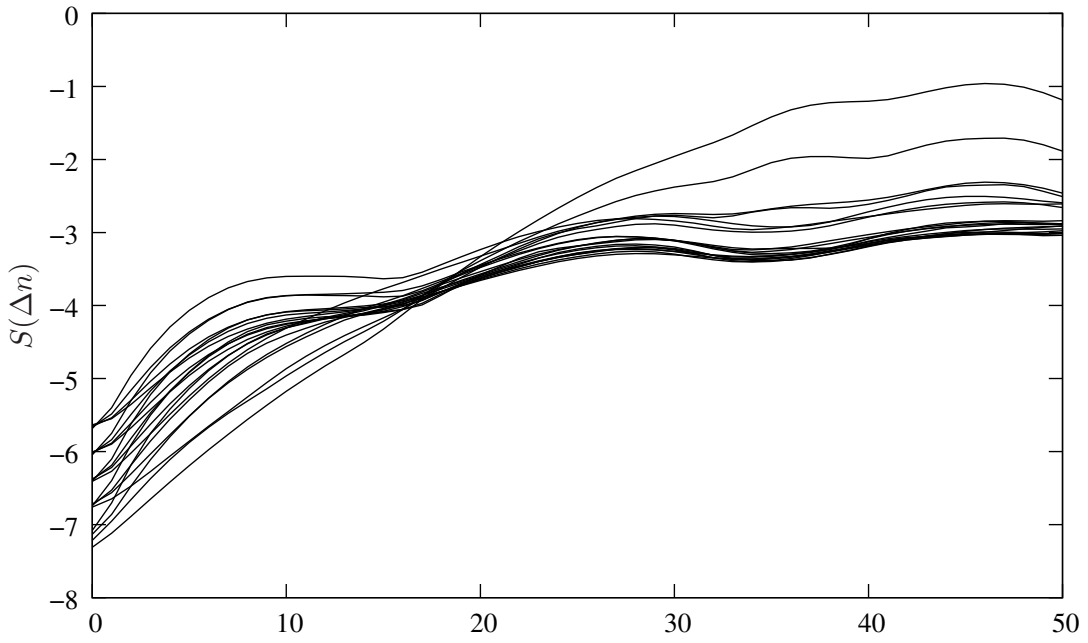
(a) $\Delta h = 0.029$



(b) $\Delta h = 0.0204$



(c) $\Delta h = 0.0202$



(d) $\Delta h = 0.0201$

Figure 3.13: Plots showing different Δh values as the x states of the system approache chaotic range

The following is an explanation of different values of Δh as it approaches the critical

value of maximum diffusion with retained chaotic behaviour:

- Figure 3.13A has $\Delta h = 0.029$. Between the values of $0 < t < 20$, the Lorenz dynamic system has a negative slope, which means that the system approaches a fixed point. Then, it changes into a periodic orbit as indicated by the flat horizontal line at around $S(\Delta n) = 20.25$.

- Figure 3.13B has $\Delta h = 0.0204$ and shows an improved response as indicated by the overall positive slope of $S(\Delta n)$, which means that it exhibits some type of chaotic behaviour. However, one can also observe the oscillating expansion and contraction cycles as the dynamical system progresses in time.

- Figure 3.13C has $\Delta h = 0.0202$. It has a similar curve as figure 3.13B; however, the expansion and contraction cycles have been smoothed out and more of a general positive slope can be observed.

- Figure 3.13D has $\Delta h = 0.0201$ and the distance between the reference point S_{n0} and other points within diameter ϵ truly starts to diverge exponentially as indicated by the almost straight line with a positive slope.

The above results regarding the selection of Δh shows that despite using a discretized Lorenz dynamic system, chaotic behaviour could still be preserved given a careful selection of time step h. This addition of quantization error suggests that as the Lorenz chaotic dynamic system is perturbed by a certain amount of quantization error, or simply put, a small signal quantization noise, the chaotic behaviour of the dynamical system could be suppressed and periodic behaviour will emerge. Therefore, any time step values Δh in a discrete Lorenz chaotic dynamical system employing IEEE-754 single precision has to have $\Delta h < 0.0201$ in order to maintain chaotic behaviour.

To find out the approximate value of the maximum Lyapunov exponent for this particular dynamic system with $\Delta h < 0.0201$, a numeric approach is taken with the help of the $S(\Delta n)$ vs t plot. The equation defining $S(\Delta n) = S(\epsilon, m, t)$ is given by:

$$S(\epsilon, m, t) = \left\langle ln\left(\frac{1}{|U_n|}\sum_{s_{n\prime}\in U_n}|s_{n+t} - s_{n\prime+t}|_n\right)\right\rangle_n \tag{3.11}$$

where ϵ is the radius limiting the selection of points $s_{n\prime}$, m is the dimension and t is the RK-4 time steps.

By applying linear approximation to the straight line as shown in Figure 3.14, the actual slope represents the approximate maximum Lyapunov value.

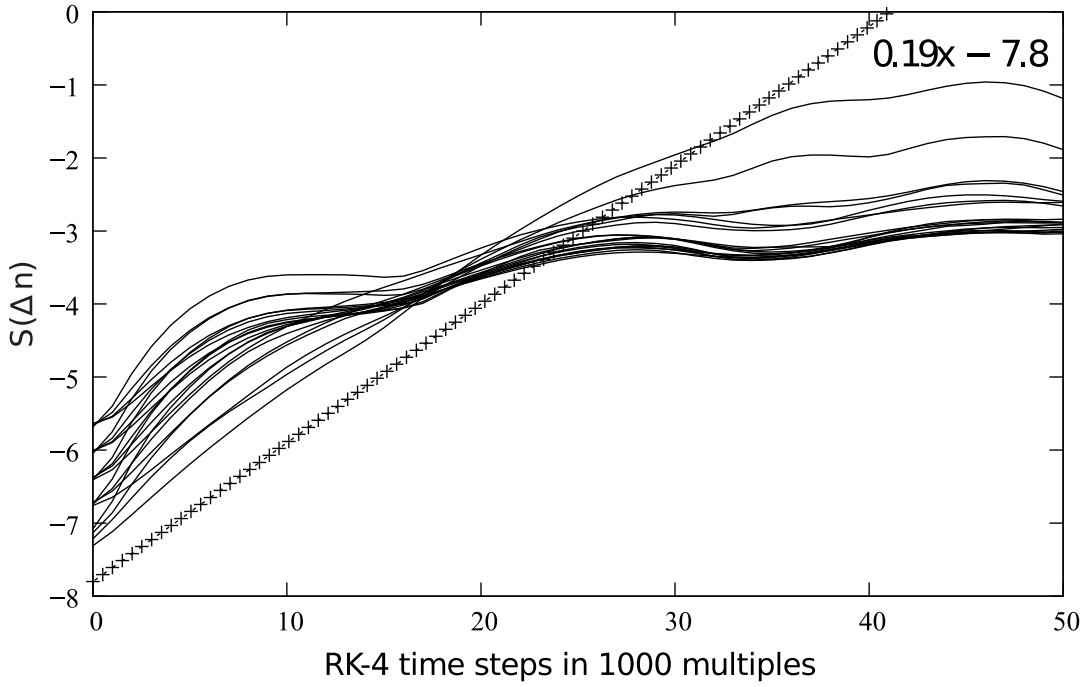


Figure 3.14: Plot of $S(\Delta n)$ showing $\lambda \approx 0.19$

Given the above results, this fourth order Runge Kutta time step threshold value $h_{threshold} = 0.0201$ is selected as the optimal h value.

3.6.3 ρ boundary conditions

The three parametric study of the Lorenz dynamical system has not received as much focus as the study of single parametric study involving ρ. Since the Lorenz based RFID authentication protocol builds on the work that has been done over continuous Lorenz dynamical systems, the focus on utilizing Lorenz dynamical system parameters as part of the secret key is restricted to using only the ρ parameter. To demonstrate why the range of $24.06 < \rho < 99.5$ was chosen. An evaluation of Lorenz system behaviour is performed given different operating ranges of ρ selection.

The behaviour of the Lorenz attractor is detailed in [71] for varying values of ρ. For $\rho < 1$, the trajectory of the system tends to 0 as shown in figure 3.15.

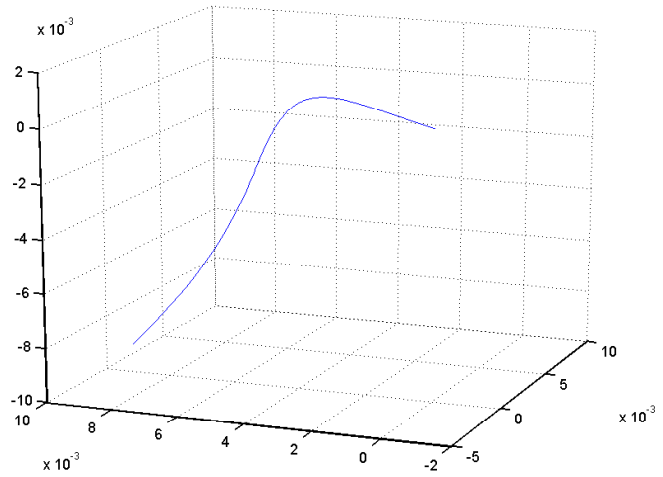


Figure 3.15: Lorenz dynamical system orbit when $\rho = 0.5$

The value of $\rho = 1$ denotes a point of transition where for $\rho > 1$, there is one point of attraction as shown in figure 3.16.

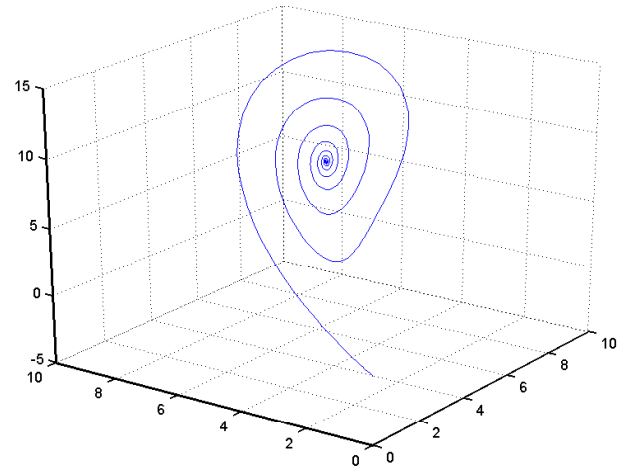


Figure 3.16: Lorenz dynamical system orbit when $\rho = 10$

Then, the next value of transition is when $\rho \approx 13.926$ and the trajectory first gets into a short limit cycle before stabilizing at a rest point (figure 3.17).

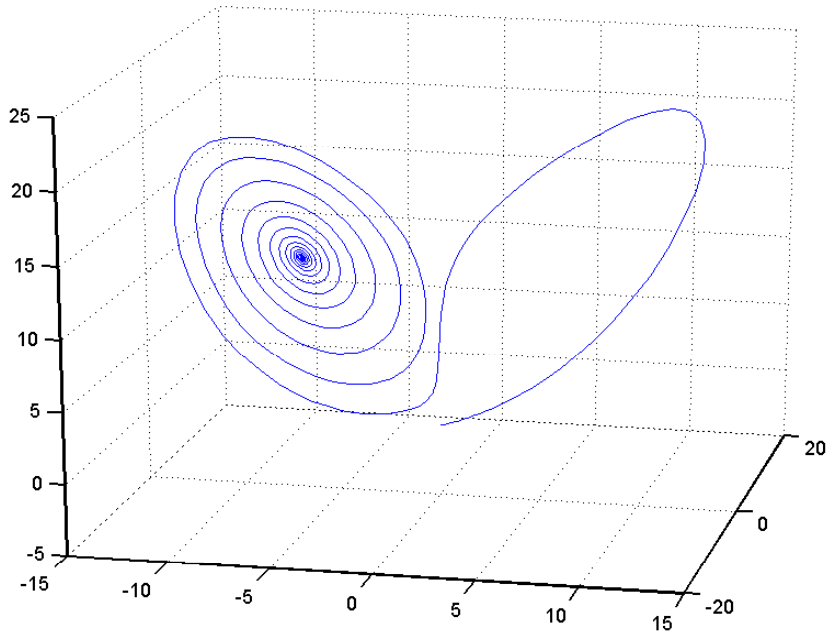


Figure 3.17: Lorenz dynamical system orbit when $\rho = 14$

Subsequently, for $13.926 < \rho < r_a$ where $r_a = 24.06$, the system behaves chaotically, but for only a finite amount of time. This period, called "metastable chaos" can be seen more easily when the observation of the system is isolated to only x states as in figure 3.18.

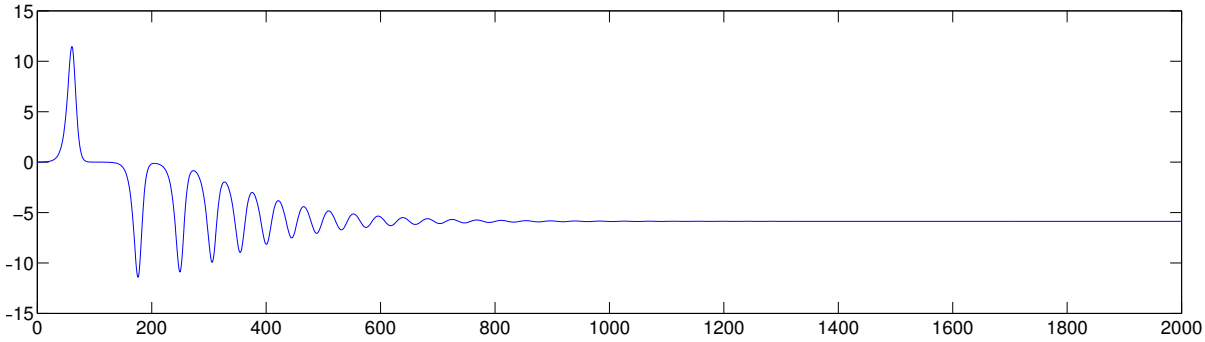


Figure 3.18: Plot of x state variables with $\rho = 14$

As the value of ρ approaches r_a, the length of time that the system remains chaotic increases. When $\rho = r_a = 24.06$, the system behaves chaotically indefinitely as shown in figure 3.19 [34].

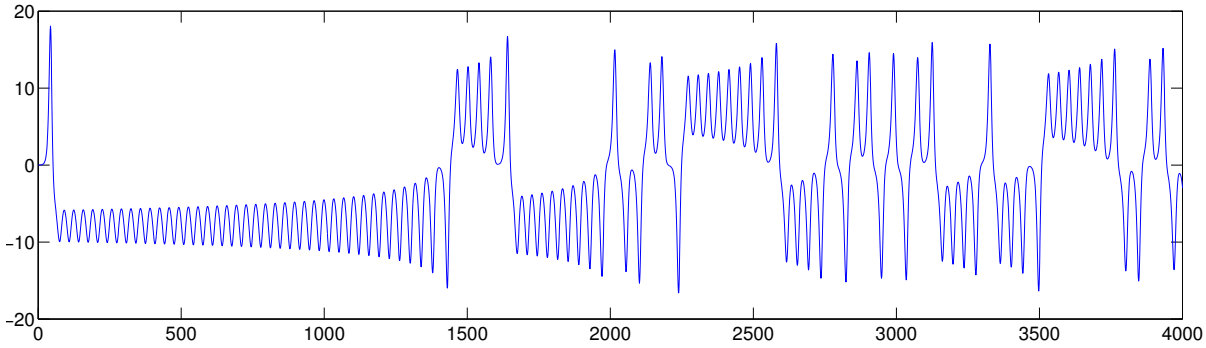


Figure 3.19: Plot of x state variables with $\rho = 24.06$

This type of chaotic behaviour, however, does not persist for all values of $\rho > 24.06$. When $\rho > 99.5$, the dynamical system's orbit transforms from a symmetrical orbit to an asymmetrical $x^2 - y$ orbit. Figure 3.20 shows what began as a chaotic attractor type of trajectory turned into a periodic orbit around two rest points.

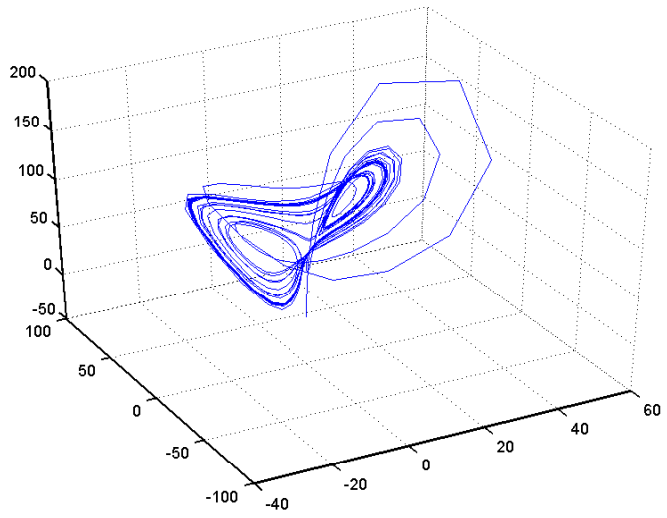


Figure 3.20: Lorenz dynamical system orbit when $\rho = 100.5$

This phenomenon can be more clearly observed in figure 3.21 with a x states only plot versus time.

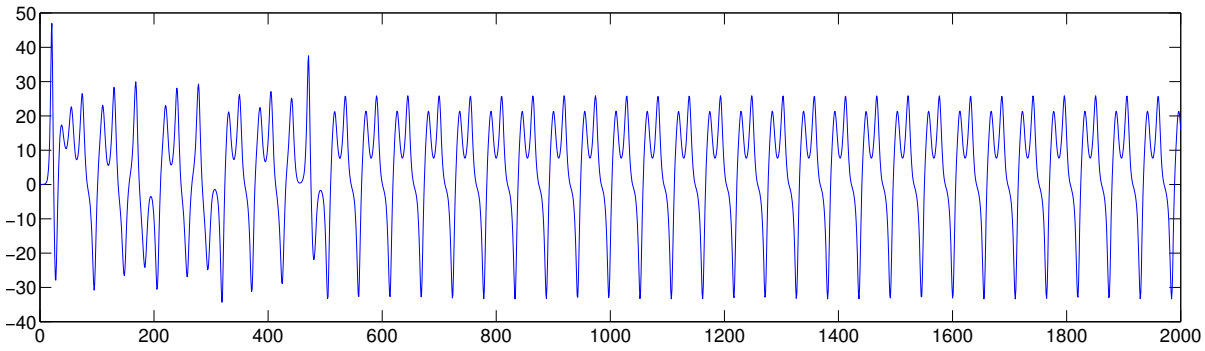


Figure 3.21: Plot of x state variables with $\rho = 100.5$

Once the value of ρ surpasses 99.5, there exists many more stable orbits during certain intervals of ρ. From a cryptographic application standpoint, care must be taken in the selection of ρ because an unexpected transition from chaotic to periodic behaviour could completely negate all desirable properties of chaotic dynamical system. It is important to note that from [34][5][71] and many other reference works that the behaviour of Lorenz dynamical system given set values of σ and β with $24.06 < \rho < 99.5$ is well known. For

that reason demonstrated above, the range of $24.06 < \rho < 99.5$ is selected for ensured chaotic behaviour.

3.6.4 System divergence from ρ

Given the almost infinite spectrum of possible ρ values to chose from between boundary conditions $24.06 < \rho < 99$, the question now becomes how much resolution can the Lorenz dynamical system operating in its chaotic region offer to allow the smallest difference in the selection of two different keys. In other words, if an attacker were to guess the value of ρ, how successful would he/she be if the guess were 0.1 off the actual chosen ρ value in the secret key? From figure 3.22, x states begin to diverge significantly at

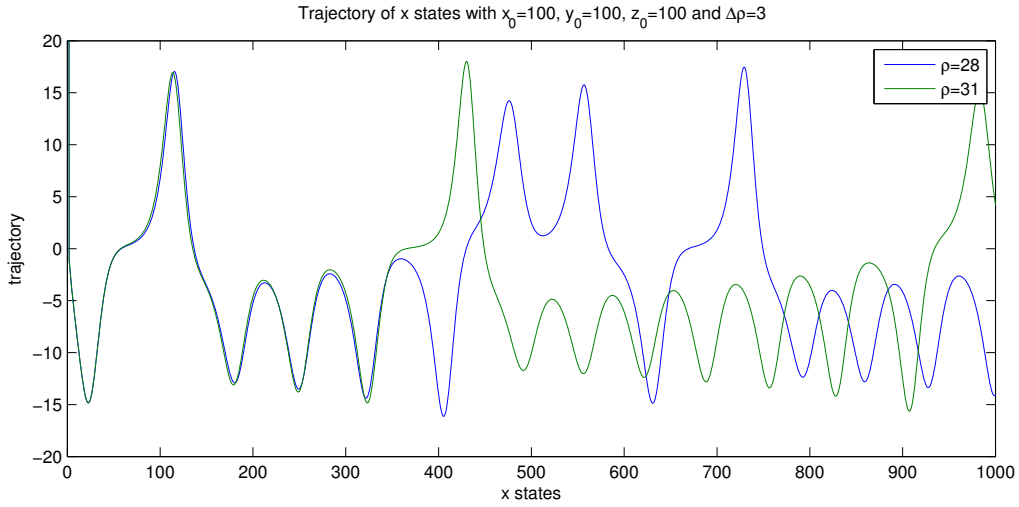


Figure 3.22: Plot of x states with $x_0 = 100$, $y_0 = 100$, $z_0 = 100$ and $\Delta\rho = 0.1$

around $t = h \times 350$. In the design of a chaotic cipher using the discrete Lorenz dynamic system proposed in my research, the transmitter has the freedom to decide how far apart should ρ be in the subset of possible ρ selection.

Let ρ_a be the value of ρ for system A and ρ_b be the value of ρ for system B. It can be concluded by deduction that as the difference between the value of ρ_a and ρ_b increases, the time required for x states to diverge will correspondingly decrease. To confirm this hypothesis, let us increase $\Delta\rho$ in figure 3.23. This shows that when $\Delta\rho = 3$, the x state trajectory begins to diverge significantly at $t = h \times 180$, which solidifies our deduction. During actual application of discrete Lorenz dynamic system, the selection of ρ in the

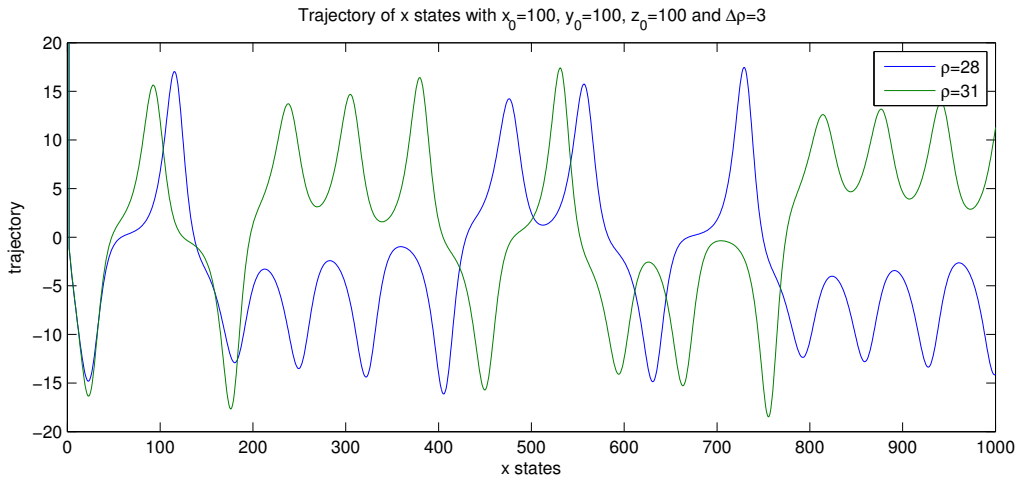


Figure 3.23: Plot of x states with $x_0 = 100$, $y_0 = 100$, $z_0 = 100$ and $\Delta\rho = 3$

secret key will depend on how fast trajectory divergence is needed. The further apart is $\Delta\rho$, the quicker exponential divergence of the trajectories of two distinct system will occur. On the other hand, this increase of $\Delta\rho$ would in turn decrease the number of bits that the secret key has because ρ is bounded by $24.06 < \rho < 99$ and there are fewer distinct values of ρ to choose from.

The significance of this $\Delta\rho = 3$ result will be discussed in the last section of this chapter. When this finding is combined with the maximum number of distinct initial conditions x_0, y_0 and z_0, it will be possible to calculate the effective key size of the Lorenz chaos based RFID authentication protocol.

3.6.5 x_0, y_0 and z_0 boundary conditions

Having discussed the significance of ρ, we now turn our attention to the initial conditions of the Lorenz dynamical system. In figures 3.243.253.263.27, a graphical representation of the effects of an increasing x_0 is shown:

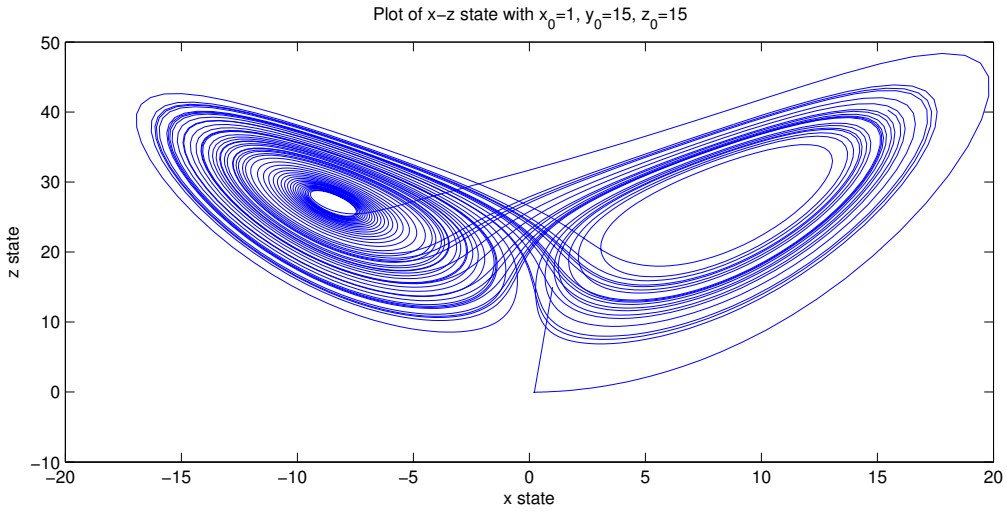


Figure 3.24: Plot of $x - z$ state with $x_0 = 1$, $y_0 = 15$, $z_0 = 15$

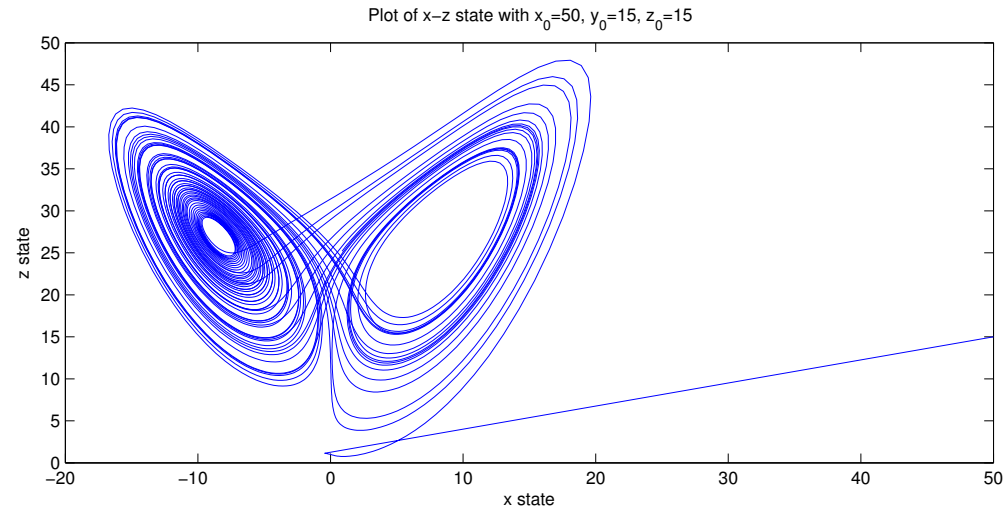


Figure 3.25: Plot of $x - z$ state with $x_0 = 50$, $y_0 = 15$, $z_0 = 15$

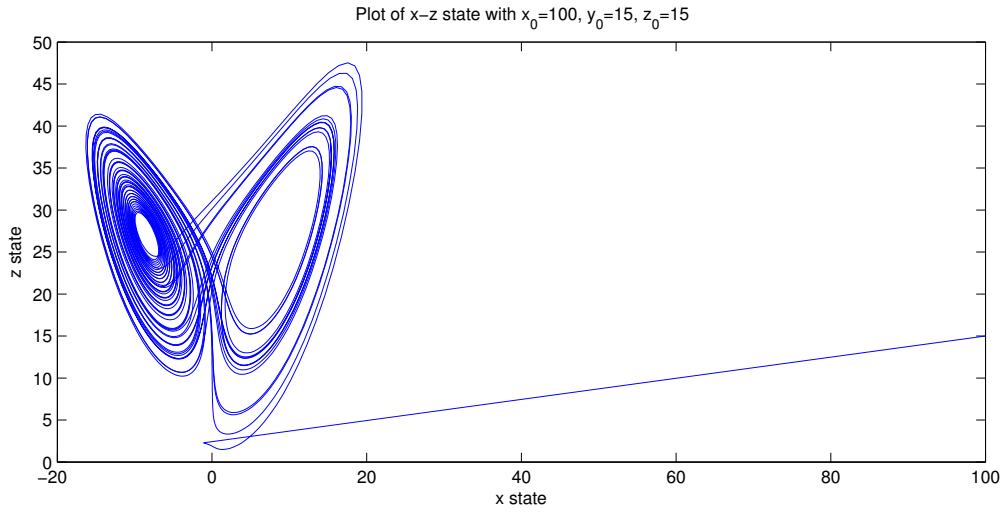


Figure 3.26: Plot of $x - z$ state with $x_0 = 100$, $y_0 = 15$, $z_0 = 15$

As the value of the initial state is increased, the signature Lorenz strange attractor rapidly returns toward the $x_0 = 0$ point while maintaining the signature Lorenz strange attractor trajectory. This signifies that chaotic behaviour is still present with initial conditions that are not close to zero, as other studies in Lorenz dynamic system have primarily been focused on. However, as the initial conditions get further away from the point $(0, 0, 0)$, the integrity of the chaotic behaviour deteriorates. Figure 3.27 below shows the deterioration of the tightness of trajectories along the chaotic attractor.

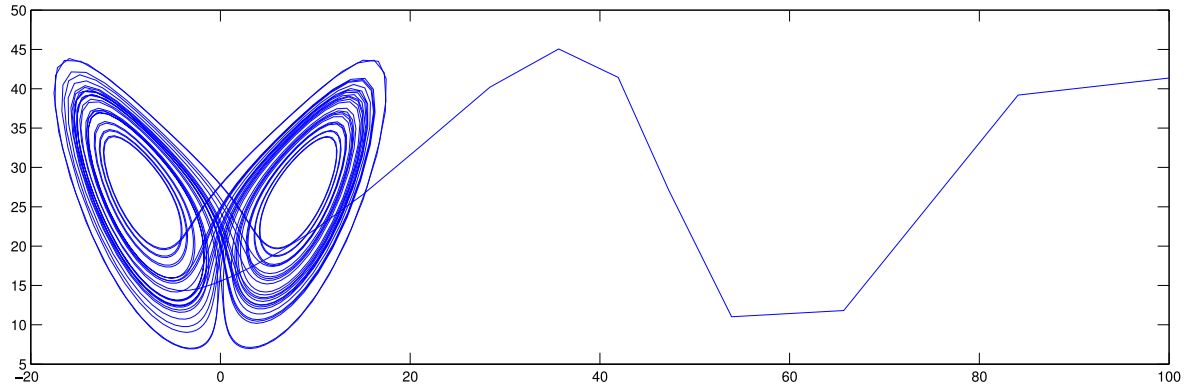


Figure 3.27: Plot of $x - z$ state with $x_0 = 500$, $y_0 = 15$, $z_0 = 15$

For this reason, it is important to note that during actual implementation in hardware, depending on the level of precision of the number system chosen, initial conditions x_0, y_0 and z_0 have to be bounded. From the x state vs time step plot of $(x_0, y_0, z_0) > (0, 0, 0)$, a spike occurs during the beginning stages of the Lorenz x states. Figure 3.28 shows a close up of this extremely rapid change of x states from an exponential downward trend to an exponential upward slope.

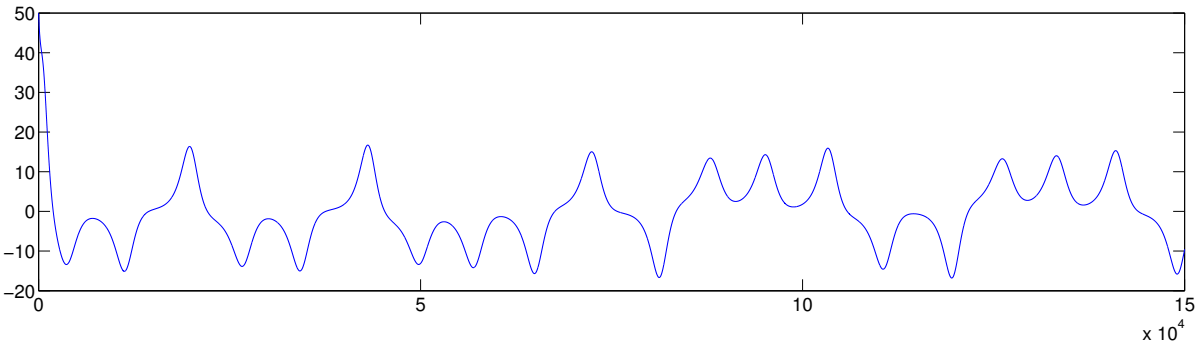


Figure 3.28: Plot of x states with $x_0 = 50$, $y_0 = 1$, $z_0 = 1$ and $h = 0.0001$

Because the Lorenz chaotic state progressions are approximated by the fourth order Runge Kutta method, in the event that the speed of the state transitions are changing more rapidly than the maximum allowed per each time step h, the fourth order Runge Kutta approximation will not be able to catch up and instability will occur. This effect can be observed in figure 3.29, where the set of Lorenz system parameters, initial conditions x_0, y_0 and z_0 were all unchanged. This, in theory, should reveal an almost exact same Lorenz trajectory.

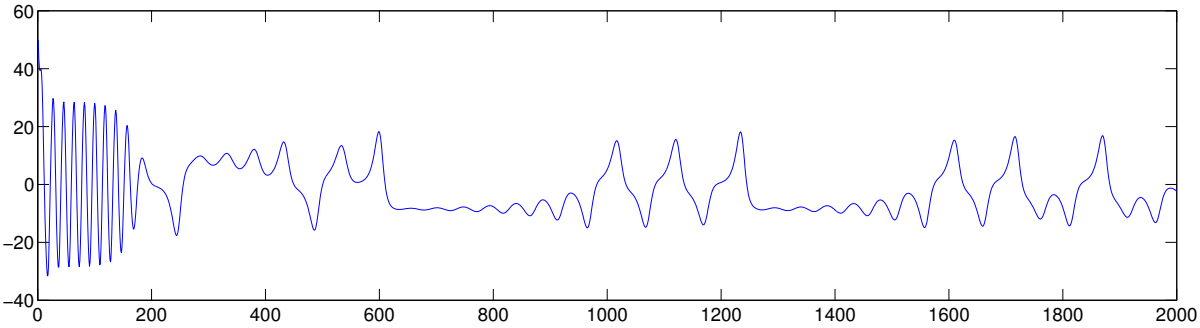


Figure 3.29: Plot of x states with $x_0 = 50$, $y_0 = 1$, $z_0 = 1$ and $h = 0.013462$

When compared with $h = 0.0001$, it can be clearly observed that x states oscillate during the beginning stages of the discrete lorenz chaotic system. In this case, for initial conditions $x_0 = 50$, $y_0 = 1$, $z_0 = 1$, the limit of h is approximately 0.013462. Beyond this time step value, the change in x states occur too quickly for the fourth order Runge Kutta approximation to capture and hence, the system will approach either positive or negative infinity. Therefore, it is paramount that given a certain selection of h, the initial conditions for the discrete Lorenz chaotic system cannot go beyond the limit of the fourth order Runge Kutta approximation range.

Now, to determine the range of initial conditions for a given step size h, one can observe the total change in x states over time for each set of initial conditions. With the aid of Matlab, this can be accomplished numerically and shown graphically. Let $y_0 = 1$, $z_0 = 1$ and:

$$x_0 = [x_1, x_2, ..., x_n] \quad \text{where} \quad n = 250 \tag{3.12}$$

and the total number of time steps in the fourth order Runge Kutta approximation is set at 5000. For $x_0 = 1$, $y_0 = 1$, $z_0 = 1$, the total absolute change is given by:

$$\sum_{i=1}^{5000} |\Delta x_i| \quad \text{where} \quad |\Delta x_i| = |x_{i+1} - x_i| \tag{3.13}$$

By plotting $|\Delta x_i|$ vs x_n, it is possible to determine the critical point where the initial conditions are changing too rapidly for the time step h chosen. Figure 3.30 shows an example of this plot.

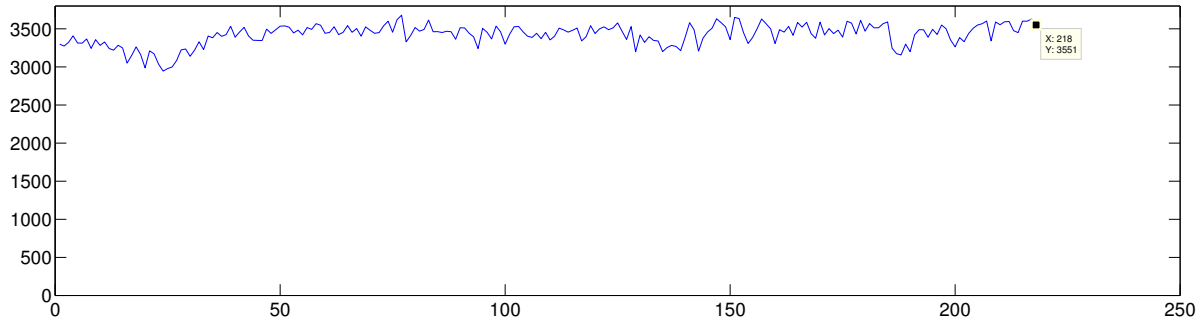


Figure 3.30: Plot of $|\Delta x_i|$ for initial conditions $y_0 = 1$, $z_0 = 1$, $x_0 = [1, ..., 250]$ and $h = 0.0201$

One can observe that $|\Delta x_i|$ hovers between 3000 and 3500 for $1 < x_n < 218$. Then, for $x_n \leq 219$, changes in x states reach that critical point where the fourth order Runge Kutta approximation with $h = 0.0201$ could not keep up and the resulting x states derail into either positive or negative infinity. It is important to note that all three initial states of the discrete Lorenz chaotic system have a cumulative effect on the range of x_0, y_0 and z_0. For instance, figure 3.31 shows the range of valid x_0 is decreased with an increase in y_0 and z_0. Given the above observations, when selecting a valid range of initial conditions,

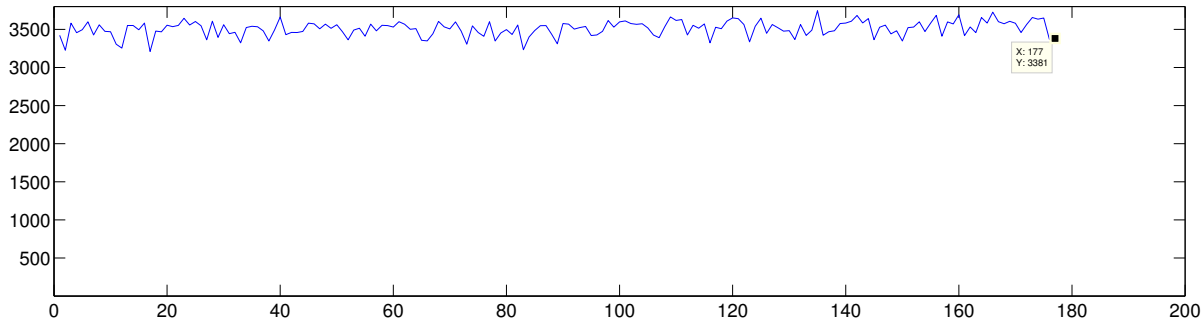


Figure 3.31: Plot of $|\Delta x_i|$ for initial conditions $y_0 = 180$, $z_0 = 180$, $x_0 = [1, ..., 200]$ and $h = 0.0201$

the goal is to maximize x_0, y_0 and z_0 without going over the fourth order Runge Kutta approximation limit. In the case of $h = h_{threshold} = 0.0201$, from figure 3.31, a good choice for the range of initial conditions is $x_0 = 170$, $y_0 = 170$ and $z_0 = 170$. This would give an equal number of x_0, y_0 and z_0 sets for the key size evaluation that will be performed later in this chapter.

3.6.6 System divergence from initial conditions

From the original paper published by Lorenz and other works done by researchers in the field of chaos, initial conditions that are very close to zero have predominantly been employed. For example, in [49], Lorenz used the initial conditions $x_0 = 0$, $y_0 = 1$ and $z_0 = 0$ for his initial study of his convection flow model. Similar to other cryptographic schemes, the goal for the selection of the secret key is to try and have as large a key as possible. In the Lorenz based RFID authentication scheme, the resolution of initial conditions influences directly the outcome of the Lorenz trajectory. In order to maximize the size and the level of confusion of the secret key, initial conditions of $x_0 = 170$, $y_0 = 170$

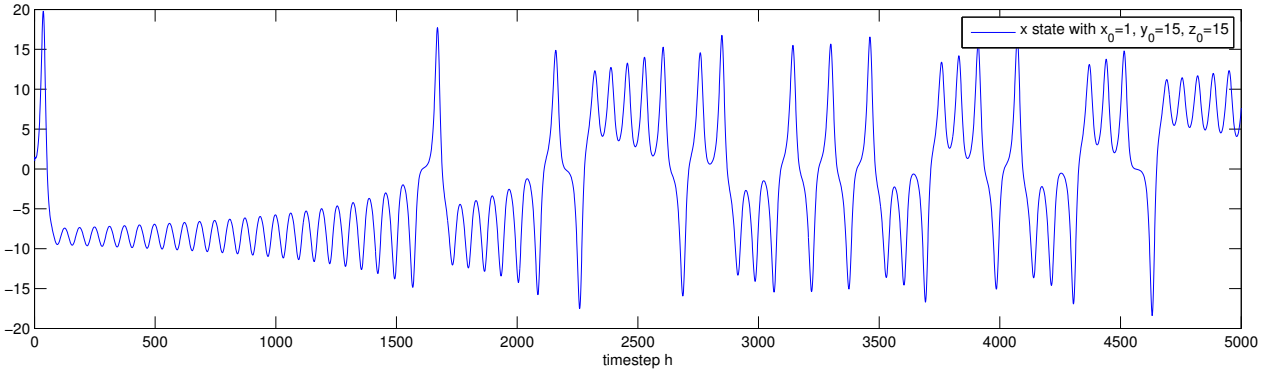
and $z_0 = 170$ were chosen. Knowing that initial conditions not close to the zero also displays a strange attractor form from the previous section, one has to now evaluate the total number of distinct x_0, y_0 and z_0 that yield a unique point along the Lorenz chaotic trajectory. To illustrate this more simply, let x_{a0}, y_{a0} and z_{a0} be the initial conditions that communication system "A" uses. Then, in another separate system "B", x_{b0}, y_{b0} and z_{b0} are the initial conditions chosen. The trajectory of system A after t second is x'_{a0} and the corresponding time in system B after t seconds is x'_{b0}. Given:

$$\Delta x_0 = x_{a0} - x_{b0} \tag{3.14}$$

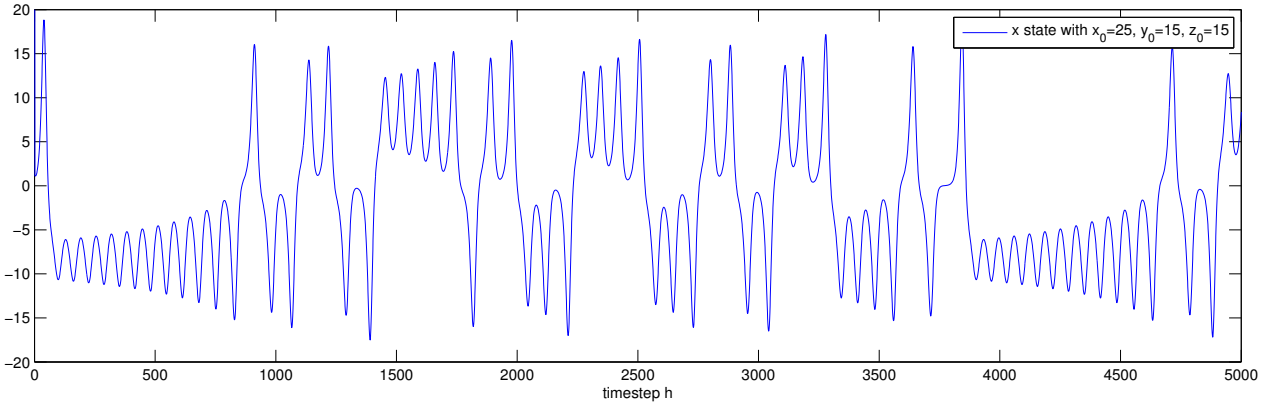
The set of valid x_{b0} depends on Δx_0 where,

$$x'_{a0} - x'_{b0} > 0 \tag{3.15}$$

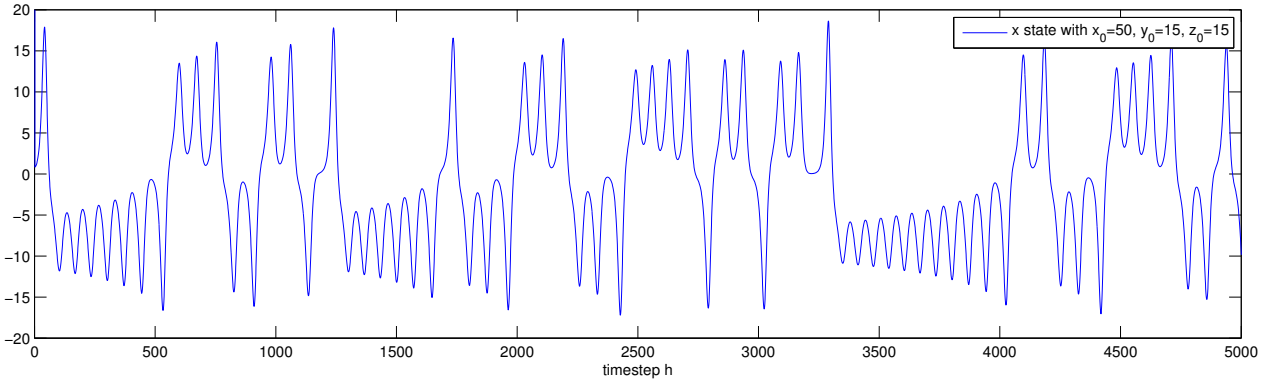
Therefore, if Δx_0 is made too small, it could potentially take too long for two separate dynamical systems to exponentially diverge, which would be a major flaw in the cipher. Figure 3.31 shows x states as a function of time for different x_0 values.



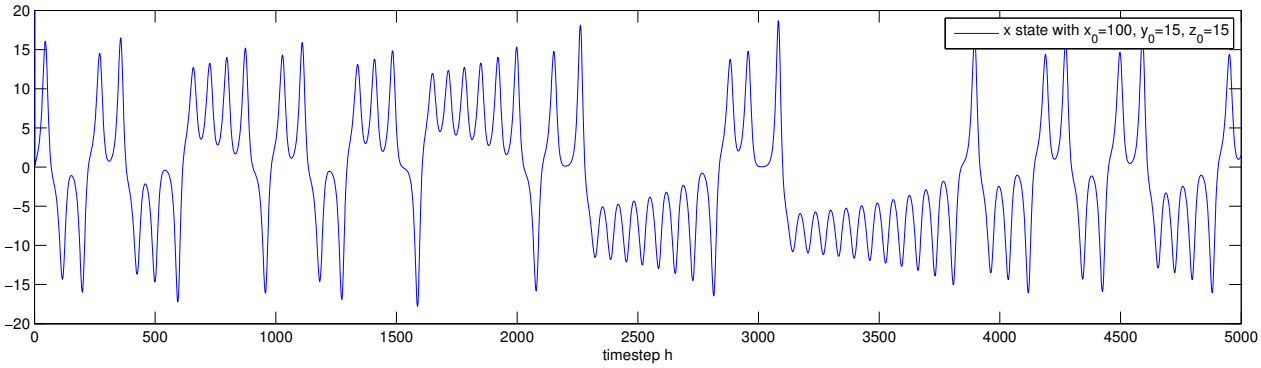
(a) x states with $x_0 = 1$



(b) x states with $x_0 = 25$



(c) x states with $x_0 = 50$



(d) x states with $x_0 = 100$

Figure 3.31: x states with different initial conditions of x

As the value of the initial x state is increased, the transient oscillation period before x state becomes chaotic decreases. Over the set of all three Lorenz initial conditions, the larger the initial conditions, the faster the Lorenz dynamic system approaches the zero point. This is a beneficial property for the Lorenz chaos based RFID authentication protocol because the transmitter and the receiver will be able to enter a chaotic state as well as negotiate and authenticate within a shorter time span given the decrease in time in the Lorenz chaotic trajectory. There is, however, a limit as to how far the initial conditions x_0, y_0 and z_0 can be from the point $(0, 0, 0)$. The initial spike of x in figure 3.31 was omitted because accent was put on showing the chaotic behaviour of the x states. Figure 3.32 below shows the initial x state right before what is shown in figure 3.31.

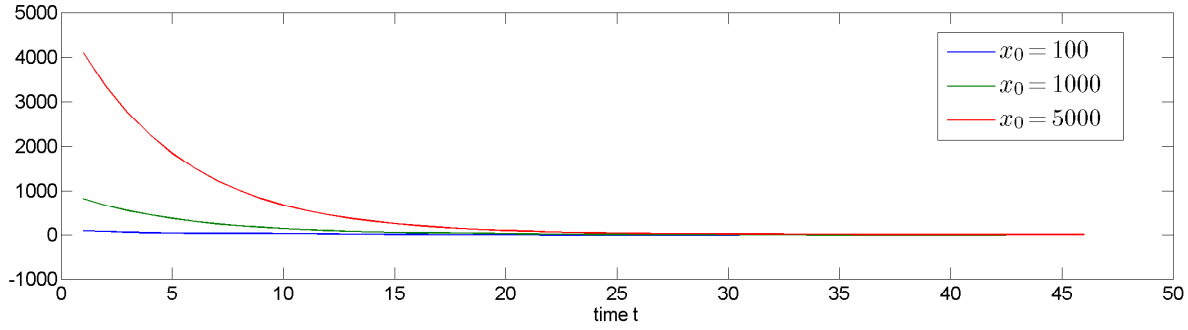


Figure 3.32: Plot of x states for time shortly after start of Lorenz dynamic system

This clearly shows the strong tendency for the x states to converge back to zero. Setting the y axis of figure 3.31 to logarithmic scale provides a more clear look at the exponential convergence to zero:

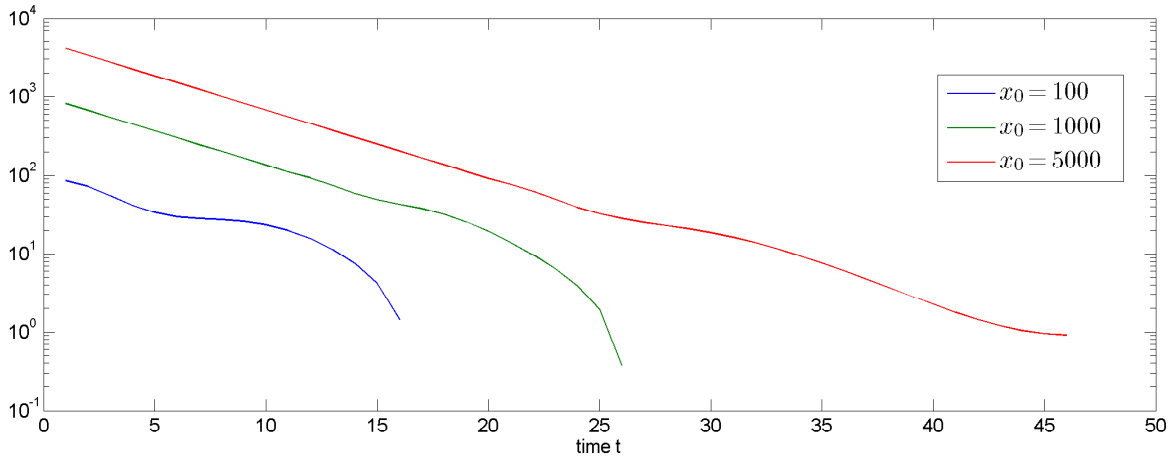


Figure 3.33: Logarithmic Plot of x states for time shortly after start of Lorenz dynamic system

From this exponential convergence, a pitfall in the selection of x_0 is present. The confusion property of the secret key could potentially be lost since an attacker could easily approximate the x state values shortly after the start of the Lorenz dynamic system knowing that it approaches exponentially quickly $x = 0$.

From the definition of chaos, one should expect an increasing divergence of two arbitrary trajectories as the initial conditions of two systems increase. Figure 3.34 show the plot of x states with a difference in x of 0.1.

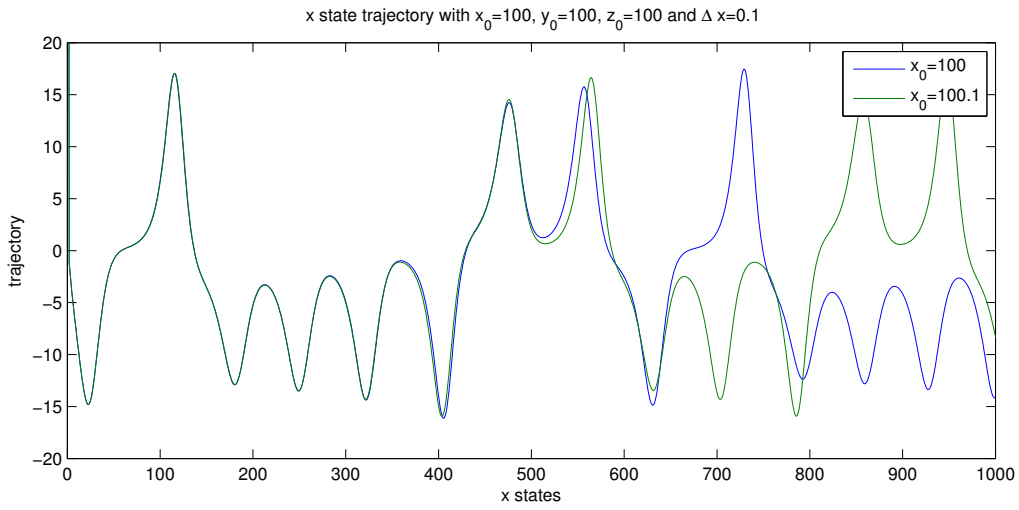


Figure 3.34: Plot of x states with $x_0 = 100$, $y_0 = 100$, $z_0 = 100$ and $\Delta x = 0.1$

With $\Delta x = 0.1$, x states begin to diverge at $t = h \times 650$. In an attempt to decrease the state progressions needed such that chaotic behaviour will occur sooner in time, let us increase the value of Δx.

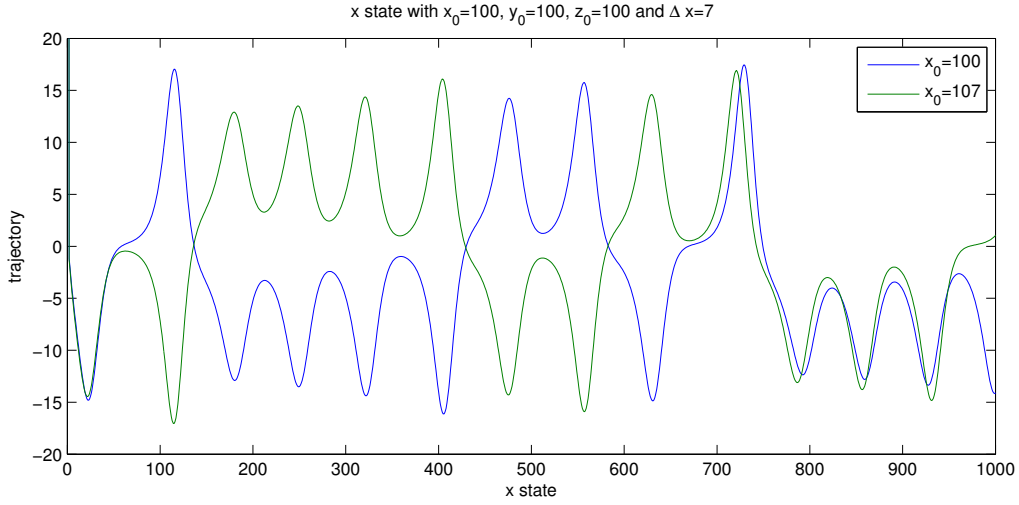


Figure 3.35: Plot of x states with $x_0 = 100$, $y_0 = 100$, $z_0 = 100$ and $\Delta x = 7$

Figure 3.35 clearly shows a decrease in the amount of time required for x states to significantly diverge. This behaviour is expected and confirms that as the initial conditions are further apart, the time that it takes before the Lorenz chaotic system diverges

is decreased.

In the next section, the results that were demonstrated about the characteristics of ρ and the Lorenz initial conditions x_0, y_0 and z_0 will be put together to determine the effective key size of the Lorenz chaos based RFID authentication protocol.

3.6.7 Key size

Parameters of the discrete Lorenz chaotic engine make up the content of the secret key used during encryption and decryption. These parameters are what differentiate one discrete Lorenz chaotic trajectory from another. They include:

- Initial condition x_0
- Initial condition y_0
- Initial condition z_0
- Lorenz system parameter ρ

As seen in previous sections, there exists factors that the initial conditions have to abide by during its selection in order to ensure that chaotic behaviour is maintained. Also, the fourth order Runge Kutta time step h plays an important role that directly influences the outcome and behaviour of the discrete Lorenz chaotic system. For the sake of explaining the actual key size of the Lorenz chaos based RFID authentication protocol, focus is on the optimal time step h, system parameters and initial conditions chosen of $h = 0.0201$, $24.06 < \rho 99.5$ and $x_0 <= 170$, $y_0 <= 170$, $z_0 <= 170$ respectively. From my hardware implementation of the Lorenz chaotic engine, each Lorenz state requires 57 clock cycles of calculation time. Recalling figure 3.31 showing the optimal maximum initial conditions $x_0 = 170$, $y_0 = 170$ and $z_0 = 170$. Given a resolution of 0.0201 for the selection of initial conditions, figure 3.36 shows the difference in x, y and z states for discrete Lorenz chaotic systems A and B having initial conditions $x_{A0} = 10$, $y_{A0} = 50$, $z_{A0} = 50$ and $x_{B0} = 10.0201$, $y_{B0} = 50$, $z_{B0} = 50$ respectively.

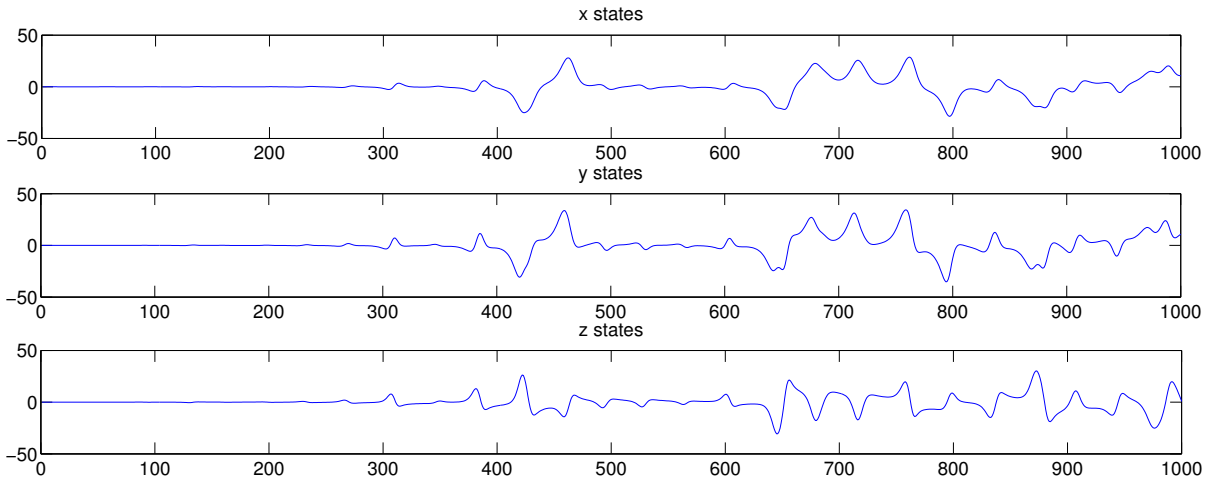


Figure 3.36: Plot of x, y and z states with a $\Delta x = 0.0201$ and $h = 0.0201$

In order for two arbitrary discrete Lorenz chaotic systems to diverge, from looking at figure 3.36, it is necessary to progress chaotic states past 400 steps in the fourth order Runge Kutta approximation. The total time $t_{divergence}$ required before the trajectory of a reader having a carrier frequency of $13.56Mhz$ and a non authorized tag starts to diverge is given by:

$$\begin{aligned} t_{divergence} &= (1/13.56 \times 10^6) \times 57 \times 400 \\ &= 1.68ms \end{aligned}$$

This delay is within the practical range of a typical RFID authentication session, which is in the millisecond range. To determine the total number of possibilities for x_0, y_0 and z_0 selections, we refer to the optimal range of valid initial conditions:

$$\begin{aligned} x_0 &= [0.0201, ..., 170] \\ y_0 &= [0.0201, ..., 170] \\ z_0 &= [0.0201, ..., 170] \end{aligned}$$

Given a resolution of 0.0201 for x_0, y_0 and z_0, the total number of possible choices for initial conditions are:

$$\begin{aligned} \text{total number of possible } x_0,\, y_0,\, z_0 &= \frac{170 - 0.0201}{0.0201} \\ &\approx 8456 \end{aligned}$$

Hence, the total number of possible initial condition choices is $8456^3 = 604,637,282,816$. Now, for the Lorenz dynamic system parameter ρ, the same process is followed. Referring back to the optimal and valid range of ρ, chaotic behaviour is maintain when $24.06 < \rho < 99.5$. Recalling figure 3.22, a difference of 0.1 in ρ has the effect of diverging two arbitrary paths after approximately 350 fourth order Runge Kutta time step calculations. To determine the total number of possibilities of ρ:

$$\begin{aligned}\text{total number of possible } \rho &= \frac{99.5 - 24.06}{0.1} \\ &\approx 754\end{aligned}$$

Therefore, the total number of possible combinations of x_0, y_0, z_0 and ρ is:

$$\begin{aligned}\text{total number of unique combinations of } x_0,\, y_0,\, z_0,\, \rho &= 8456 \times 8456 \times 8456 \times 754 \\ &= 4.558965112 \times 10^{14}\end{aligned}$$

In terms of number of bits of security, this scheme has an equivalent of roughly 49 effective bits of security, which is very efficient for a one round cipher that only requires a small amount of resources to implement.

3.7 Encryption and decryption rate

After both the reader and the tag have proven their identity via the authentication scheme, both communicating parties have now secured their authenticity. For the encryption and decryption of a plaintext bit stream, the ultimate goal is to maximize the bit transfer rate of the encryption implementation without compromising the level of entropy offered by chaos. The Lorenz chaos based scheme offers several different implementation methods. For the Lorenz chaos based RFID authentication protocol, a modified permutation method utilizing x state peaks was chosen for encryption and decryption a plaintext binary bit stream. In this section, we will explain the reasons behind this implementation method selection.

3.7.1 Direct x state utilization

Perhaps the most straight forward approach is the use of a simple exclusive OR operator. In a single precision IEEE-754 number, there is a total of 32 bits. Given an input binary stream S, it can be divided into 32 bit blocks.

$$S = [S_0, S_1, ..., S_n] \tag{3.16}$$

where n is equal to the length of the plaintext bit stream segment and each element of S is 32 bit long. In order to obfuscate this input bit stream, it is exclusive OR'ed with each x discrete Lorenz chaotic state. So that:

$$T = [S_0 \oplus x_0, S_1 \oplus x_1, ..., S_n \oplus x_n] \tag{3.17}$$

where x_n are the 32 bit IEEE-754 single precision x states generated from the discrete Lorenz chaotic engine. With this approach, one can easily see that the decimal representation of x Lorenz chaotic states are truly chaotic but when it is converted into a binary representation, in this case the IEEE-754 single precision format, the statistical distribution would not be uniform. If an attacker were to guess x_n, they can easily eliminate a high number of possibilities because there is a limit in the range of possible x state values. Recalling that in a truly secure cryptosystem, the only secret is the content of the secret key and one should not rely on hiding the elements and algorithms of a cryptosystem in order to try and make it more secure.

3.7.2 x state permutation

In an effort to make the distribution of each bit more uniform, another method that can be used is by permuting the binary mantissa of the Lorenz dynamical system's x states. Recalling that the IEEE-754 single precision number has 24 mantissa bits. Since the first bit of the mantissa is always a binary one, the last bit of the exponent is used to represent this first bit of the mantissa in order to maintain its chaotic nature and will be referred to as M_1 subsequently. Let M be the x Lorenz state mantissa. By separating M in two parts, we have:

$$M = [M_l, M_r] \tag{3.18}$$

where $M = [M_1, M_2, ..., M_{24}]$ and $M_l = [M_1, ..., M_{12}]$ and $M_r = [M_{13}, ..., M_{24}]$
To create a $24 \times 12 = 288$ bit mask K for use in the encryption and decryption of a plaintext bit stream, where $K = [K_1, K_2, ..., K_{288}]$, M is the first 24 bits used.

For the second set of 24 bits, M is permuted and bits are XOR'ed according to figure 3.37 such that $M_1 = M_{12} \oplus M_1$ and $M_2 = M_{11} \oplus M_2$ and so on. Then, a right side rotating shift is performed to yield the next set of M used in the encryption and decryption mask K.

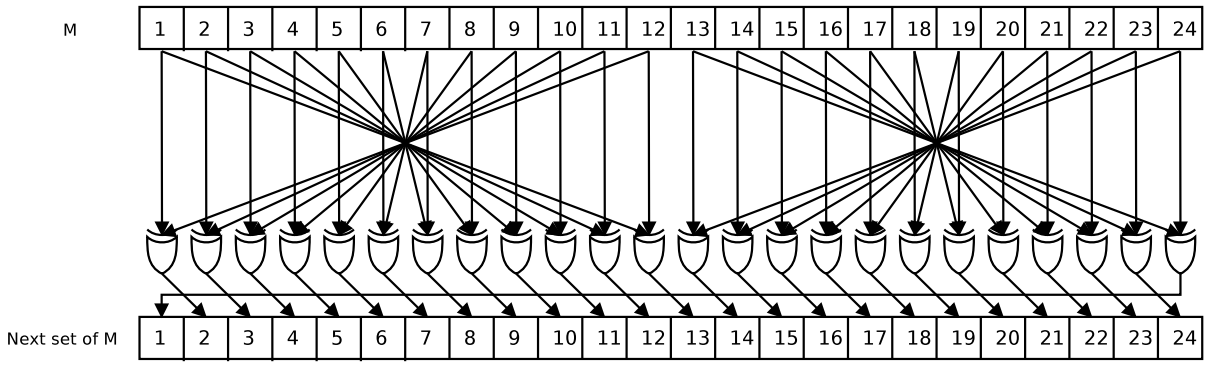


Figure 3.37: Permutation and XOR operations between sets of M

The result of this method gives a stronger bit masking of the single precision x states and increases its length to 288 bits. In terms of the security of this permutation technique, it is important to note the following:

1. This method differs from traditional applications of permutation techniques in cryptography because this permutation is done on the Lorenz x state and not on the actual authentication key itself. This is a unique masking technique benefiting from the unique application of chaos in cryptography, which is different from a traditional symmetric key cipher design.

2. This bit stream of Lorenz x state that is used to encrypt the plaintext data has no direct correlation with the real authentication key. In other words, if an attacker were to know one of the 288 bit Lorenz x state, it would not reveal any additional information on the trajectory of the Lorenz dynamical system; hence, other x states.

3. The strength of this Lorenz x state bit stream builds on the complexity of solving for the Lorenz chaotic system. This means that for an attacker to know even part of this 288 bit Lorenz x state, they would have to first solve for the actual Lorenz x state itself.

Based on the above, this method of extending the length of Lorenz x state is considered as strong as the chaotic behaviour in predicting the actual x state itself.

3.7.3 x state selection

With the coding of x states defined, the next step in completing the data encryption scheme is to determine which x states are chosen to perform the exclusive OR operations. Obviously, the most straight forward approach would be to utilize each and every x state generated by the discrete Lorenz chaotic engine. By doing so, the maximum bit rate in this obfuscation scheme can be achieved. However, there is a downside to this method. Given a plaintext bit stream S. As shown above, the obfuscated ciphertext is given by:

$$T = [S_0 \oplus X_0, S_1 \oplus X_1, ..., S_n \oplus X_n] \tag{3.19}$$

where the x state is at an arbitrary point in its chaotic trajectory. In the event that a particular point of this arbitrary trajectory is compromised, the chaotic nature of x states that have been approximated by the fourth order Runge Kutta method shortly before and after this point will also be compromised.

Recalling the signature Lorenz chaotic state plot below:

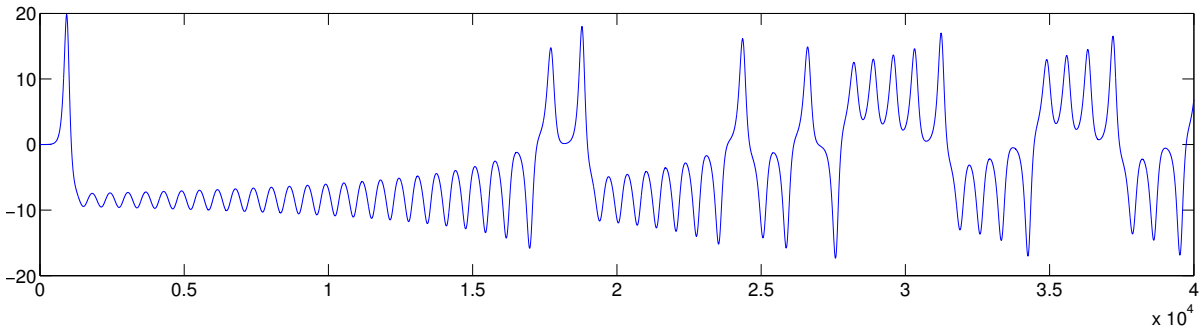


Figure 3.38: Plot of Lorenz x states in its chaotic region

Given the fine fourth order Runge Kutta time step h relative to the rate of change in Lorenz chaotic x state values, it can be observed that any arbitrary x state x_n where $t = h \times n$ is relatively close to x_{n-1} and will also be relatively close to x_{n+1}. Therefore, if an attacker has the value of x_n, the security of the binary plaintext bit stream that has been encrypted shortly before and after this point n will be weak and likely be compromised.

A solution to this problem of correlation between x states is to not use each and every state but rather select states that will not be relatively close to each other. As the

x states reach either a positive or negative peak, those points will be selected for use in encryption. This way, even if a given x state value is compromised, it will not be possible for an attack to guess with high success the next x states that will be used.

By using the techniques mentioned above, an estimation of the mean encryption bit-rate can be performed. Given the following discrete Lorenz chaotic system parameters:

$$\begin{aligned} \rho &= 28 & x_0 &= 10 \\ \sigma &= 10 & y_0 &= 10 \\ \beta &= 8/3 & z_0 &= 15 \\ h &= 0.0201 \end{aligned} \tag{3.20}$$

The corresponding x states are given in figure 3.39. From this plot, the peak to peak delay in fourth order Runge Kutta approximation time steps are roughly:

$$\Delta h_{\text{peak to peak}} = 389 - 358 \tag{3.21}$$

$$= 31 \tag{3.22}$$

As demonstrated in the implementation of the discrete Lorenz chaotic engine in FPGA, each fourth order Runge Kutta approximation takes $1.68msec$. This means that the actual time t required between x state peaks are:

$$\begin{aligned} t_{\text{peak to peak}} &= 1.68ms \times 31 \\ &= 52msec \end{aligned}$$

For the modified permutation scheme, the effective bit rate will be:

$$\begin{aligned} \text{effective bit rate} &= \frac{288}{52 \times 10^{-3}} \\ &= 5.538Kb/sec \end{aligned}$$

In a resource constrained system such as the implementation demonstrated in the Lorenz chaos based RFID protocol, a bit rate of $\approx 5.538Kb/sec$ is very good given such low resource usage and the speed that each Lorenz chaotic state can be generated.

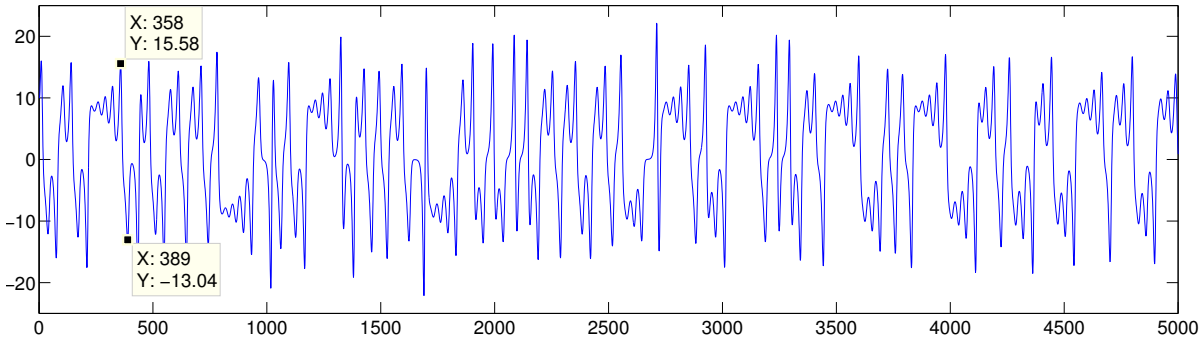


Figure 3.39: Plot showing x states peak to peak Δh

In this upcoming chapter, a numerical security evaluation is given in order to provide proof that my proposed Lorenz chaos based RFID authentication scheme offers the same level of security as the continuous Lorenz chaotic system itself.

Chapter 4

Security Evaluation of Proposed Scheme

An observation in the field of chaos based cryptography shows that although there has been a number of suggested implementations, few of them actually proceeded in any type of security evaluation. The consequence is the lack of any proof that their suggested system is resilient against different types of attacks and that there are no weaknesses in their implementation of chaos. In this chapter, the discretized implementation of chaos employed in the Lorenz chaos based RFID authentication protocol will undergo security evaluations from several different angles. A statistical analysis of a very large pool of compiled x states is examine to determine whether short cycle periodic behaviour exists. Then, the Lorenz chaos based RFID authentication scheme is evaluated against the rules of security requirements in chaos-based cryptosystems detailed in [25] to ensure that my proposed implementation is as secure as currently possible.

4.1 Statistical analysis

A factor that affects the level of security of the discretized Lorenz dynamic system is the distribution of states. From numerous works that were done in the field of analog chaotic dynamic systems, a strong emphasis has been put on the sensitivity to initial conditions property. For chaos to be a real contender in the field of cryptography, one has to know exactly what are the chances of a particular chaotic cipher being broken when faced with specific attacks. It is nice to have the sensitive to initial conditions property but how good will it do to a cipher if the range of possible outputs are always repeating or has

only a relatively small pool of possible values? This section takes a concrete look at two possible weaknesses of any chaotic cipher: short cycle periodic patterns and non-symmetrical statistical state distribution.

Before proceeding into detail with the statistical evaluations of this section, an explanation of the test setup is in order. For the results obtain to be significant behaviours of the discretized Lorenz dynamic system and not just short transient behaviours, the x state generation process underwent a long period of time. A total of $50,000$ fourth order Runge Kutta steps were generated with the hardware implemented Lorenz chaotic state generator. Given the time required for a typical authentication session to be much less than a second, and that each authentication session required 31 time steps, this would provide a total of $50,000/31 \approx 1,612$ authentication attempts.

4.1.1 Short cycle periodic pattern verification

To make sure that the authentication scheme proposed in my research can withstand a man-in-the-middle attack, where communication between the reader and the tag is compromised and intercepted, one has to ensure that this advantage will not grant the attacker any advantage regardless of the number of authentication communication interceptions. Since there has not been any concrete work performed in the subject of verifying whether chaotic dynamic systems exhibit short periodic cycles, this subsection will explain the method performed and provide actual results in order to support the security of the RFID authentication scheme proposed.

In the previous section, the $S(\Delta n)$ vs t plot provided a mean to quantitatively identify periodic and chaotic behaviour and as well as the Lorenz trajectory approaching a single point. For the evaluation of short periodic cycles, although this method could be used, it does not effectively displays repeated periodic cycles. The reason is because the $S(\Delta n)$ vs t plot can have an overall positive slope while having very small repeating staircase type of periodic mini-stages. Those stages in itself might not show severe periodic cycles but when combined together, can be a clue to flaws in the system. To combat such shortcoming, another method should be used in the evaluation of short periodic cycles. By taking the Fast Fourier Transform of the x states generated by the hardware implemented Lorenz chaotic engine, one can then clearly see any significant repeated periods accumulated during the entire time span of the x states. As a way to confirm

this method, Fast Fourier Transform is applied to a system with $\Delta h = 0.029$. From the Lyapunov exponent calculations performed in previously, this evaluation should give some type of repeating periods.

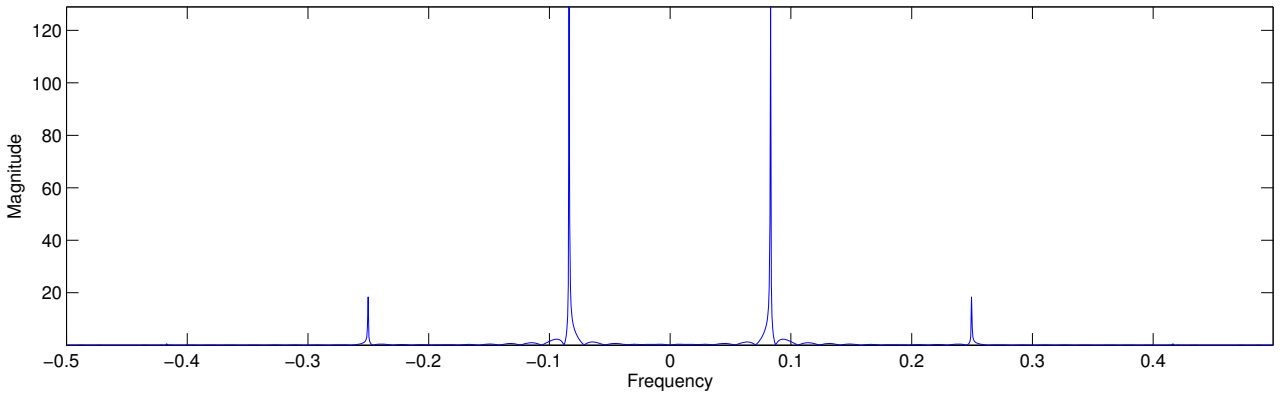


Figure 4.1: FFT of Lorenz dynamical system with $\Delta h = 0.029$

It is clearly shown in Figure 4.1 that there are two distinct periods that emerge from the dynamical system having $\Delta h = 0.029$. Once again, this reinforces the notion mentioned in the previous section that improper selection of time step h will degrade chaotic behaviour into periodic behaviour. Now, the exact same test performed with time step $h_{threshold}$ should not have this shortcoming. Figure 4.2 shows the result of the Fast Fourier Transform of the discretized Lorenz dynamic system with the threshold time step.

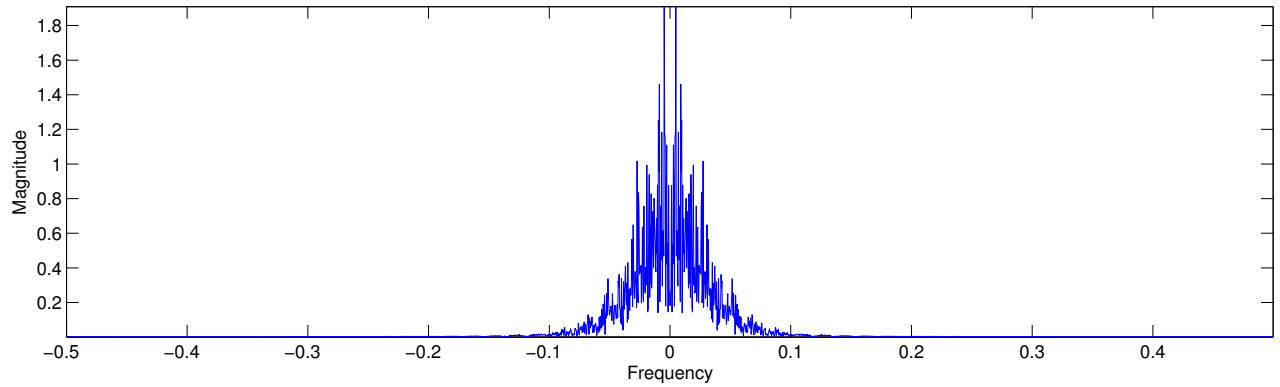


Figure 4.2: FFT of Lorenz dynamical system with $\Delta h = 0.0201$

Figure 4.2 shows a dramatic improvement in terms of frequency spectrum compared to $h = 0.029$. The resulting Fast Fourier Transform has a strong DC like component, which is a favourable property in terms of minimizing the periodic determinism of the discretized Lorenz dynamical system.

4.1.2 Statistical distribution verification

In this subsection, the distribution of x Lorenz chaotic states over time is examined in order to determine whether the probability of states are equally distributed. To begin, a series of x states are generated from the discrete Lorenz chaotic engine such that the total duration of state generation is much larger than the length of time of a typical authentication session in order to ensure that small cycle periodic behaviour is not present. Again, with $\Delta h = 0.0201$ and 50000 RK-4 steps, we have a total of approximately $1,612$ authentication attempts. Figure 4.3 shows the distribution of states of this dynamical system.

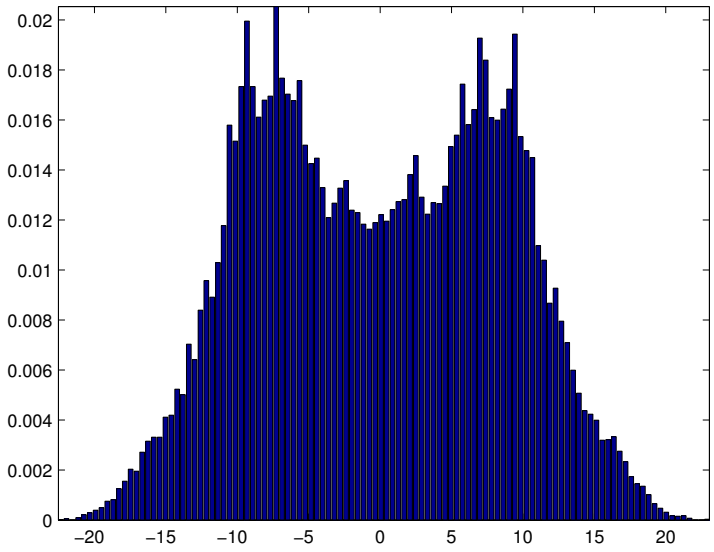


Figure 4.3: x state distribution over 1000 seconds from my proposed Lorenz chaotic engine

From the results obtained in Figure 4.3, one is able to see that the Lorenz chaotic x states distribution is symmetrical. In other words, there is an even distribution of x

states in the positive as well as the negative range. Given the symmetry of this x state distribution, if we assign positive states to have a binary value of 1 and negative states to have a binary value of 0, the probability for an attacker to correctly guess a binary 1 would be 1/2 and the same is true for the probability of guessing correctly a binary 0. This fact solidifies the noise-like uniform distribution of the discrete Lorenz chaotic x states.

For discrete Lorenz chaotic engine applications that are not resource constrained, an additional encryption scheme is possible. If the probability proportions are adjusted accordingly, it is possible to have four equal ranges of x states in Figure 4.3 such that the probability for each range to appear would be 1/4. Then, one can continuously divide state ranges in order to increase coding effectiveness as long as the range division is not made too small to maintain proper probability distribution. This method could be used as a perfect chaotic pseudo random number generator that has an even probability distribution and is none periodic.

Ultimately, knowing that the discrete Lorenz chaotic engine has even probability distribution, an implementation of the Lorenz chaos based RFID authentication protocol can become the ideal method for integrating chaos into existing RFID systems. To my knowledge, this is the first practical use of chaos in resource constrained digital hardware based systems that has undergone in depth security scrutiny by means of time-series analysis.

4.1.3 Rules and guidelines to follow to ensure the security of chaos based cryptosystems

According to the paper [25], there are 17 rules that any designer of chaos based cryptosystem should follow to ensure that their system is not easily broken. From testing those rules against the Lorenz chaos based RFID authentication protocol, it can be shown that my proposed scheme already satisfies those rules. The following is a list of those nine rules that are relevant for a digital chaotic cryptosystem and explain how they are being met. A list of the other rules can be found in Appendix A.

Rule #1: A thorough description of the implementation of the chaotic systems involved should be provided

This rule applies to works that are theoretical in nature and no concrete implementations are given or not enough details are given to suggest possible implementation direction. Unfortunately, many suggested cryptosystem employing chaos has a narrow focus that makes it impractical for implementation in actual hardware. My proposed chaos based RFID authentication protocol has been discussed in great detail in previous chapters of this thesis.

Dynamical system used:
The dynamical system used for my proposed authentication scheme is a discretized version of Lorenz dynamical system. In order to calculate each x, y and z states, the fourth order Runge Kutta approximation method is used with time step set at $h = 0.0201$, which is the optimal time step value for chaotic behaviour to still be present.

Dynamical system paramters
The Lorenz dynamical system has governing parameters ρ, σ and β that model heat convection in the atmosphere. It was shown in chapter three that Lorenz dynamical system parameters play an important role in it's overall behaviour. While most research in Lorenz dynamical system has been done on single parametric systems, it makes sense to build on the work that has been done previously in this field instead of branching out into a three parametric Lorenz dynamical system. For that reason, σ and β are set at 10 and 8/3 respectively. The value of ρ is the one that is changing and it can only take on values between 24.06 to 99.5. This is because values outside of this range exhibits short periodic cycles that are degrading to the chaotic nature of the Lorenz system.

Rule #2: For chaotic systems implemented in digital form, the negative effects of dynamical degradation should be taken into consideration with careful evaluation

For dynamical chaotic systems to be in the discrete domain, it has to be in a finite space employing number representations in digital form such as fixed point or floating point and methods of truncation such as ceiling, floor or round. It has been demonstrated in [46] that piece-wise linear chaotic maps are very susceptible to linear degradation, which has a detrimental effect on the sustained chaotic behaviour of the finite chaotic

system. This phenomenon can be viewed as a constant variable small disturbance on a continuous dynamical system which are caused by the quantization error of digital computer systems. According to [10], the orbits traced by a continuous chaotic system are obviously different from their discrete counterpart. For this reason, chaotic behaviour in a continuous system given a certain initial state and parameters cannot be guaranteed in a corresponding digitized system.

In my proposed chaotic scheme, care was taken to make sure that long iterations of the chaotic system in finite space does not converge to a single point or follow a periodic orbit. To theoretically take into consideration all the quantization error chaos is a difficult task because of the difficulty in performing analytical modelling. Many of the current research in the field of discrete chaotic systems make use of numerical methods for this purpose. My proposed approach for the evaluation of dynamical degradation in this chaotic scheme is to utilize the TISEAN toolset to perform numerical evaluation on time series data obtained from the hardware implemented Lorenz dynamical system. A positive Lyapunov exponent indicates that exponential diverge is presence and chaotic behaviour is maintained.

Rule #3: Without loss of security, the cryptosystem should be easy to implement with acceptable cost and speed

In comparing the Lorenz chaos based RFID authentication protocol with widely used symmetric key cryptosystems in terms of speed and level of security, a typical software implementation of AES [6] shows that performance is in the range of 20-150 cycles per byte. As shown in my RFID authentication scheme detailed in chapter two, the level of resource utilization is extremely low and I have proven its actual design complexity by implementing this chaotic cryptosystem fully on an FPGA. This low level of hardware resource utilization also has the beneficial side effect of making the cost of manufacturing such a device low. The throughput of this chaotic cryptosystem, which is at approximately $5.538Kb/sec$, is very respectable for systems having limited resources such as in RFID applications.

Rule #4: The key should be precisely defined

In chapters three, a detailed explanation of the makeup of the secret key is given. It is composed by a combination of:

- The selection of the value of ρ
- The selection of the initial values of x_0 , y_0 and z_0

The binary format representation used is the IEEE 754 single precision format. Therefore, each secret key is 128 bits long (32-bit single precision x_0, y_0, z_0 states plus 32-bit single precision system parameter ρ). Most of the proposed chaotic cryptosystems fall short of defining the exact key layout and leaves it totally up to the reader to perform this task. The uniqueness of my approach is the proposal of a new chaotic RFID authentication scheme with concrete implementation details and with a numerical study of its security from multiple attack angles.

Rule #5: The key space K, from which valid keys are to be chosen, should be precisely specified and avoid nonchaotic regions

From the evaluation of initial conditions x_0, y_0 and z_0 and the Lorenz chaotic system parameters ρ, σ and β in chapter three, it was shown that the values of the initial conditions and system parameters indeed yield chaotic behaviour. Since the key originates from those system parameters and initial conditions, we know which regions to avoid in order to ensure chaotic behaviour. For example, when the Lorenz strange attractor is formed, the only state that exhibits chaotic behaviour is the x state. Another example is the range of possible ρ values. It was shown in chapter three that chaotic and non-periodic behaviour is observed when $24.06 < \rho < 99.5$. From reading other proposed chaotic cryptosystems and the successful attacks on those systems, very often, those attacks do not focus on the chaotic system itself but rather in the other components surrounding the chaotic algorithm. By ensuring that there are no weak secret keys, it renders an attacker's job that much harder and denies their attempt in a workaround circumventing chaos itself.

Rule #6: The useful chaotic region, i.e. the key space K, should be discretized in such a way that the avalanche effect is guaranteed: two ciphertexts encrypted by two slightly different keys $k1$, $k2 \in K$ should be completely different

Referring back to chapter three, the minimum change in the chosen secret key is demonstrated numerically in order for two closely related keys to provide two completely different outcomes. For the calculation of the effective secret key bit length, this minimum

distance between initial conditions and ρ selection has been taken into account so that the level of security of this chaotic cryptosystem is not over inflated.

Rule #7: Partial knowledge of the key should never reveal partial information about the plaintext nor the unknown part of the key

Originating from one of the most basic rule in cryptography, the Kerckhoffs principle tells us that the security of the cryptosystem must rely entirely on the key. In other words, the only secret that an attacker does not know is the key and everything surrounding the implementation of such cryptosystem cannot be used as a mean to increase security. Often times, proposed chaotic cryptosystems tend to hide or be unclear about certain aspect of their method. In my proposed chaos based RFID authentication protocol, the partial knowledge of the key does not mean part of the plaintext or other parts of the key is revealed because valid key values are carefully chosen so that they are all within chaotic regions of the dynamical system. For example, if an implementation blindly uses all values of ρ in a Lorenz dynamical system and if such value were to be revealed to the attacker, the weak periodic behaviour of the dynamical system will be revealed. That has serious consequences in the revelation of the plaintext and is totally unacceptable in a secured cryptosystem.

Rule #8: The algorithm or process of generating valid keys from the key space K should be precisely specified

This rule is partially answered from the explanation given in the previous rule. Since the range of values of ρ, x_0, y_0 and z_0 is known, the process of selecting valid key is simply the selection from this range of values.

Rule #9: For two keys (or two plaintexts) with the slightest difference, no distinguishable difference between the corresponding ciphertexts can be found by any known statistical analysis and rule #10: The ciphertext should be statistically indistinguishable from the output of a truly random function, and should be statistically the same for all keys

These two rules are similar to rule #6 except that not only two slightly different keys should yield a completely different ciphertext, but two slightly different plaintexts should yield a set of completely different ciphertexts as well. To demonstrate this, statistical analysis of my proposed system is used. If we were to plot out the location of the

chaotic trajectory X_n, Y_n and Z_n where n is the time step h multiplied by the number of iterations, the distribution of X_n, Y_n and Z_n across the span of different initial conditions X_0, Y_0 and Z_0 should appear noise like or has a symmetrical distribution. This is covered in this chapter previously with the evaluation of possible periodic behaviour and x state distribution utilizing a very large pool of x states.

Chapter 5

Conclusions and Future Work

Ever since Edward Lorenz published his famous paper, "Deterministic non-periodic flow", in 1963, he has opened the doors to a new type of dynamical system that exhibits complex behaviour but yet, is modelled by only three simple ordinary differential equations. What was originally used to model heat convection in the atmosphere has found itself in everyday phenomenons ranging from the human heartbeat to trends in the publicly traded financial markets. Even though the Lorenz attractor has been around for quite some time, it has been the subject of active research and many works have probed into different aspects of the Lorenz's dynamic system. In particular, there has been a substantial number of research papers suggesting the use of chaos in communication security and cryptosystems for the past two decades. A look around cryptographic methods being used today in digital communication security reveals the story of a complete absence of real world use of chaos in actual implementations. The reason is because most suggested cryptosystems based on chaos have major shortcomings including:

1. Most implementations require broadband communication medium which, in this digital age, limits its usefulness.

2. Chaotic cryptosystems based on piecewise-linear systems had serious security issues because of dynamic degradation.

3. Lack of clarity in the actual methods of implementation.

4. Lack of proof in the level of security provided by their implementations.

With all the knowledge that we have gained in the past few decades on the subject of Lorenz's dynamic system, its overall behaviour and regions of chaotic states have been

carefully examined. In my research, I proposed a new method in harnessing beneficial chaotic behaviour and utilized it in a RFID authentication protocol. Details that previously suggested cryptosystems based on chaos failed to address, such as boundaries of the dynamic system, security evaluation and key composition, were delivered in this thesis and verified numerically for correctness and well rounded security. By examining the Lyapunov exponent of time series of a spectrum of Lorenz x states, I discovered that the discretized Lorenz dynamic system, subjected to quantization noise, still retains its chaotic behaviour given careful selection of system parameters, initial conditions and fourth order Runge Kutta time-step h. In fact, a critical time-step value $h_{threshold}$ was found that maximizes state entropy while still maintaining chaotic behaviour.

I have also shown that this new Lorenz chaos based RFID authentication protocol has a low resource utilization level that made it suitable for low-resource devices. Unlike other chaos based cryptographic schemes, my proposed system can be implemented via baseband signals such as radio frequency communications and digital communications. Also, this characteristic makes my proposed scheme easily implementable by using current technologies and standards. For example, it can be implemented over existing ISO-15693 RFID systems because the radio communication frequencies, tag power requirements and hardware resource utilization levels all adhere to its limits.

The above discoveries concretely shows the unique characteristics of chaotic cryptosystems by harnessing the proven chaotic behaviour of Lorenz dynamic system in a discrete state and numerically demonstrating its effective level of security. This is a brand new way of implementing continuous time chaotic systems in digital communications and this thesis has only uncovered partially the spectrum of possible usage of chaos in resource constrained devices. From this point on, one can embark on many avenues of improvement and innovation:

1. Fourth order Runge Kutta approximation was used to calculate x, y and z state progressions. From a resource usage standpoint, the use of other ordinary differential equation approximation methods can potentially improve the efficiency and decrease hardware resource usage. One key point to be examined, if one chooses to go towards this route and use Euler's approximation method, is the behaviour of Lorenz's dynamic system and the effect it has on initial condition boundaries. The $h_{threshold}$ value found in this thesis will most likely be changed as a consequence.

2. Since research performed in a three-parametric study of the Lorenz dynamic system is still quite preliminary, my proposed RFID authentication scheme only included ρ in the secret key. However, with more work concentrated on the behaviour of the Lorenz system in a three-parametric system, this could potentially open another door to the increase in the effective security bit length of the secret key and make this new approach even more secure. In addition, this has the possibility of speeding up the x state divergence rate, which will make it the bit rate of the obfuscation scheme increase significantly.

3. With the use of development hardware such as the Proxmark, the FPGA design of my proposed chaos based RFID authentication protocol can be fully implemented in a full scale RFID reader and tag system for in circuit evaluation of power usage and an evaluation of potential error correction methods that can be employed.

Finally, this work is the first to propose the use of Lorenz chaotic system in RFID authentication. It effectively solves the primary problem of degradation in piecewise-linear chaotic maps and the implementation problems of methods based on chaos synchronization. In addition, it makes use of the well researched chaotic behaviour of the continuous time Lorenz attractor to deliver a numerically proven secure chaotic cryptosystem that is ready to be implemented in current resource constrained RFID systems.

Appendix A

Additional rules and guidelines

The rules and guidelines discussed in chapter four in relations to the security of chaos based cryptosystem are highlighted because of their relevant nature with respect to the implementation of my proposed RFID authentication scheme. Because of the limited hardware resource nature of RFID applications and the inability to analytically solving chaotic dynamical systems, some rules and guidelines are irrelevant and were not discussed in chapter four of my thesis. They are hereby listed as a reference:

1. The ciphertext should be statistically undistinguishable from the output of a truly random function, and should be statistically the same for all keys.

2. It should be checked whether the designed cryptosystem can be broken by the relatively simple known-plaintext and chosen-plaintext attacks, and even chosen-ciphertext attacks.

3. Resistance to differential and linear cryptanalysis should be proved or checked very carefully in digital block ciphers.

4. It should be checked whether the cryptosystem can be broken by all known chaos-specific attacks.

5. It should be checked whether the cryptosystem can be broken by all known application-specific attacks.

6. To provide a sufficient security against brute-force attacks, the key space size should be $K > 2^{100}$.

7. When a keystream cipher is used, the security study should include the statistical test results conducted on the pseudo-random number generator.

8. A designed secure communication system should work in a real channel environment with $\approx -40dB$ signal/noise ratio, with a certain limited bandwidth, and with attenuation between $0dB$ and $16dB$.

Bibliography

[1] Electronic pickpocketing. `http://www.wreg.com/wreg-electronic-pickpocketing-story,0,6289527.story`. Accessed online on April 28, 2013.

[2] Fixed-point arithmetic modules. `https://opencores.org/project,fixed_point_arithmetic_parameterized`. Accessed online on April 28, 2013.

[3] Gildas Avoine, Cédric Lauradoux, and Tania Martin. When compromised readers meet RFID. In *Information Security Applications*, pages 36–50. 2009.

[4] Gildas Avoine and Aslan Tchamkerten. An asymptotically optimal RFID authentication protocol against relay attacks. *Computing Research Repository*, abs/0809.4183, 2008.

[5] Roberto Barrio and Sergio Serrano. A three-parametric study of the Lorenz model. *Physica D: Nonlinear Phenomena*, 229(1):43–51, 2007.

[6] Guido Bertoni, Luca Breveglieri, Pasqualina Fragneto, Marco Macchetti, and Stefano Marchesin. Efficient software implementation of AES on 32-bit platforms. In *Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '02, pages 159–171, 2003.

[7] Stefan Brands and David Chaum. Distance-bounding protocols. In *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, EUROCRYPT '93, pages 344–359, 1994.

[8] J. Y. Chen, K. W. Wong, L. M. Cheng, and J. W. Shuai. A secure communication scheme based on the phase synchronization of chaotic systems. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 13(2):508–514, 2003.

[9] J. Y. Chen, K. W. Wong, H. Y. Zheng, and J. W. Shuai. Phase signal coupling induced $n : m$ phase synchronization in drive-response oscillators. *Physical Review E*, 63:036214, February 2001.

[10] B. V. Chirikov and F. Vivaldi. An algorithmic view of pseudochaos. *Physica D*, 129(3-4):223–235, May 1999.

[11] Pawel Chodowiec and Kris Gaj. Very compact FPGA implementation of the AES algorithm. In *Proceedings of the 2003 Cryptographic Hardware and Embedded Systems*, volume 2779 of *Lecture Notes in Computer Science*, pages 319–333. Springer, 2003.

[12] Chol-Ung Choe, Klaus Hohne, Hartmut Benner, and Yuri Kivshar. Chaos suppression in the parametrically driven Lorenz system. *Physical Review E*, 72:036206, September 2005.

[13] David J. Christini and James J. Collins. Using noise and chaos control to control nonchaotic systems. *Physical Review E*, 52:5806–5809, December 1995.

[14] Leon O. Chua, Ljupco Kocarev, Kevin Eckert, and Makoto Itoh. Experimental chaos synchronization in Chua's circuit. *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, 2(3):705–708, 1992.

[15] Kevin Cuomo and Alan Oppenheim. Circuit implementation of synchronized chaos with applications to communications. *Physical Review Letters*, 71:65–68, July 1993.

[16] Andreas Dandalis, Viktor K. Prasanna, and José D. P. Rolim. A comparative study of performance of AES final candidates using FPGAs. In *Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems*, CHES 2000, pages 125–140, London, UK, UK, 2000. Springer-Verlag.

[17] Saar Drimer and Steven J. Murdoch. Keep your enemies close: distance bounding against smartcard relay attacks. In *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium*, SS'07, pages 7:1–7:16, 2007.

[18] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In *Cryptographic Hardware and Embedded Systems*, pages 357–370, August 2004.

[19] Ute Feldmann, Martin Hasler, and Wolfgang Schwarz. Communication by chaotic signals: the inverse system approach. *International Journal of Circuit Theory and Applications*, 24(5):551–579, 1996.

[20] Klaus Finkenzeller. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. John Wiley & Sons, Inc., New York, NY, USA, 2nd edition, 2003.

[21] Aurelien Francillon, Boris Danev, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. Cryptology ePrint Archive, Report 2010/332, 2010.

[22] D.R. Frey. Chaotic digital encoding: an approach to secure communication. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, 40(10):660–666, October 1993.

[23] Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. Wirelessly pickpocketing a MIFARE classic card. In *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, SP '09, pages 3–15, Washington, DC, USA, 2009. IEEE Computer Society.

[24] H. Gilbert, M. Robshaw, and H. Sibert. Active attack against HB+: a provably secure lightweight authentication protocol. *Electronics Letters*, 41(21):1169–1170, 2005.

[25] Alvarez Gonzalo and Shujun Li. Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation & Chaos in Applied Sciences & Engineering*, 16(8):2129–2151, 2006.

[26] Sean Halle, Chai Wah Wu, Makoto Itoh, and Leon Chua. Spread spectrum communication through modulation of chaos. *International Journal of Bifurcation and Chaos*, 3:469–477, 1993.

[27] Gerhard P. Hancke. Practical attacks on proximity identification systems (short paper). In *Proceedings of the 2006 IEEE Symposium on Security and Privacy*, SP '06, pages 328–333, 2006.

[28] Gerhard P. Hancke. Modulating a noisy carrier signal for eavesdropping-resistant HF RFID. *Elektrotechnik und Informationstechnik*, 124(11):404–408, 2007.

[29] Gerhard P. Hancke, Keith Mayes, and Konstantinos Markantonakis. Confidence in smart token proximity: Relay attacks revisited. *Computers Security*, 28(7):615–627, 2009.

[30] Rainer Hegger, Holger Kantz, and Thomas Schreiber. Practical implementation of nonlinear time series methods: The TISEAN package. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 9(2):413–435, 1999.

[31] Martin Hlavac and Tomas Rosa. A note on the relay attacks on e-passports: The case of Czech e-passports. Cryptology ePrint Archive, Report 2007/244, 2007.

[32] ISO/IEC. *14443-2 proximity cards - part 2: Radio frequency power and signal interface*, 2001.

[33] Tomasz Kapitaniak. *Controlling chaos: theoretical and practical methods in nonlinear dynamics*. Harcourt Brace, 1996.

[34] James L. Kaplan and James A. Yorke. Preturbulence: A regime observed in a fluid flow model of lorenz. *Communications in Mathematical Physics*, 67(2):93–108, 1979.

[35] Jonathan Katz and Ji Sun Shin. Parallel and concurrent security of the HB and HB+ protocols. In *Proceedings of the 24th annual international conference on The Theory and Applications of Cryptographic Techniques*, EUROCRYPT'06, pages 73–87, 2006.

[36] M.P. Kennedy. Three steps to chaos. I: Evolution. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 40(10):640–656, October 1993.

[37] Ziv Kfir and Avishai Wool. Picking virtual pockets using relay attacks on contactless smartcard. In *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, SECURECOMM '05, pages 47–58, 2005.

[38] Chong Hee Kim, Gildas Avoine, François Koeune, François-Xavier Standaert, and Olivier Pereira. The Swiss-Knife RFID distance bounding protocol. In *Information Security and Cryptology — ICISC 2008*, pages 98–115. 2009.

[39] L. Kocarev, G. Jakimoski, T. Stojanovski, and U. Parlitz. From chaotic maps to encryption schemes. In *Proceedings of the 1998 IEEE International Symposium on Circuits and Systems*, volume 4, pages 514–517, 1998.

[40] Ljupco Kocarev and Shiguo Lian. *Chaos-based Cryptography: Theory, Algorithms and Applications*. Springer, 2011.

[41] G. Kolumban, M.P. Kennedy, and L.O. Chua. The role of synchronization in digital communications using chaos. I: Fundamentals of digital communications. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 44(10):927–936, October 1997.

[42] G. Kolumban, M.P. Kennedy, and L.O. Chua. The role of synchronization in digital communications using chaos. II: Chaotic modulation and chaotic synchronization. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 45(11):1129–1140, November 1998.

[43] Gerhard Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia. A practical attack on the MIFARE classic. In *Proceedings of the 8th IFIP WG 8.8/11.2 international conference on Smart Card Research and Advanced Applications*, CARDIS '08, pages 267–282, 2008.

[44] Po-han Lee, Soo-chang Pei, and Yih-yuh Chen. Generating chaotic stream ciphers using chaotic systems. *Chinese Journal of Physics*, 41:559–581, 2003.

[45] Shujun Li. When chaos meets computers. arXiv:nlin.CD/0405038, also available at http://www.hooklee.com/pub.html, 2004.

[46] Shujun Li, Guanrong Chen, and Xuanqin Mou. On the dynamical degradation of digital piecewise linear chaotic maps. *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, 15(10):3119–3151, 2005.

[47] Shujun Li, Xuanqin Mou, Yuanlong Cai, Zhen Ji, and Jihong Zhang. On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision. *Computer Physics Communications*, 153(1):52–58, 2003.

[48] Mingsheng Liu and Yan Wang. RFID system information security based on chaotic encryption. In *2011 Third International Conference on Multimedia Information Networking and Security (MINES)*, pages 499–502, November 2011.

[49] Edward N. Lorenz. Deterministic nonperiodic flow. *Journal of the Atmospheric Sciences*, 20(2):130–141, March 1963.

[50] Huaping Lu, Shihong Wang, Xiaowen Li, Guoning Tang, Jinyu Kuang, Weiping Ye, and Gang Hu. A new spatiotemporally chaotic cryptosystem and its security and performance analyses. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 14(3):617–629, 2004.

[51] Behzad Malek and Ali Miri. Chaotic masking for securing RFID systems against relay attacks. *Security and Communication Networks*, June 2012.

[52] Qurban A. Memon. Synchronized choas for network security. *Computer Communications*, 26(6):498–505, April 2003.

[53] Aikaterini Mitrokotsa, Melanie Rieback, and Andrew Tanenbaum. Classifying RFID attacks and defenses. *Information Systems Frontiers*, 12:491–505, 2010.

[54] Jorge Munilla and Alberto Peinado. Enhanced low-cost RFID protocol to detect relay attacks. *Wireless Communications and Mobile Computing*, 10(3):361–371, March 2010.

[55] A.V. Oppenheim, G.W. Wornell, S.H. Isabelle, and K.M. Cuomo. Signal processing in the context of chaotic signals. In *1992 IEEE International Conference on Acoustics, Speech, and Signal Processing*, volume 4, pages 117–120, March 1992.

[56] Edward Ott, Celso Grebogi, and James A. Yorke. Controlling chaos. *Physical Review Letters*, 64:1196–1199, March 1990.

[57] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and A. Shang. Transmission of digital signals by chaotic synchronization. *International Journal of Bifurcation and Chaos*, (2):973–977, 1992.

[58] Louis M. Pecora and Thomas L. Carroll. Synchronization in chaotic systems. *Physical Review Letters*, 64:821–824, February 1990.

[59] Tuan Anh Pham, M.S. Hasan, and Hongnian Yu. A RFID mutual authentication protocol based on AES algorithm. In *2012 UKACC International Conference on Control*, pages 997–1002, 2012.

[60] Jason Reid, Juan M. Gonzalez Nieto, Tee Tang, and Bouchra Senadji. Detecting relay attacks with timing-based protocols. In *Proceedings of the 2nd ACM symposium on information, computer and communications security*, ASIACCS 2007, pages 204–213, 2007.

[61] Barrio Roberto and Serrano Sergio. Bounds for the chaotic region in the Lorenz model. *Physica D: Nonlinear Phenomena*, 238(16):1615–1624, 2009.

[62] Michael G. Rosenblum, Arkady S. Pikovsky, and Jürgen Kurths. Phase synchronization of chaotic oscillators. *Physical Review Letters*, 76:1804–1807, March 1996.

[63] Michael T. Rosenstein, James J. Collins, and Carlo J. De Luca. A practical method for calculating largest Lyapunov exponents from small data sets. *Physica D: Nonlinear Phenomena*, 65(1–2):117–134, 1993.

[64] Nikolai F. Rulkov, Mikhail M. Sushchik, Lev S. Tsimring, and Henry D. I. Abarbanel. Generalized synchronization of chaos in directionally coupled chaotic systems. *Physical Review E*, 51:980–994, February 1995.

[65] Said Sadoudi, Mohamed Salah Azzaz, Mustapha Djeddou, and Mustapha Benssalah. An FPGA real-time implementation of the Chen's chaotic system for securing chaotic communications. *International Journal of Nonlinear Science*, 7(4):467–474, 2009.

[66] Barry Saltzman. Finite Amplitude Free Convection as an Initial Value Problem–I. *Journal of the Atmospheric Sciences*, 19(4):329–341, July 1962.

[67] Shinichi Sato, Masaki Sano, and Yasuji Sawada. Practical methods of measuring the generalized dimension and the largest Lyapunov exponent in high dimensional chaotic systems. *Progress of Theoretical Physics*, 77(1):1–5, 1987.

[68] O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert, and J. Reverdy. RFID noisy reader how to prevent from eavesdropping on the communication? In *Proceedings of the 9th international workshop on Cryptographic Hardware and Embedded Systems*, CHES '07, pages 334–345, 2007.

[69] Wang Shaohui. Security flaws in two RFID lightweight authentication protocols. In *Communication Systems and Information Technology*, volume 100 of *Lecture Notes in Electrical Engineering*, pages 149–156. Springer Berlin Heidelberg, 2011.

[70] Kevin M. Short. Signal extraction from chaotic communications. *International Journal of Bifurcation and Chaos*, 07(07):1579–1597, 1997.

[71] Colin Sparrow. *The Lorenz Equations Bifurcations Chaos and Strange Attractors*. Springer-Verlag, 1982.

[72] J.A.K. Suykens and J. Vandewalle. *Nonlinear Modeling: Advanced Black-box Techniques*. Kluwer Academic Publishers, 1998.

[73] Guoping Tang, Xiaofeng Liao, and Yong Chen. A novel method for designing S-boxes based on chaotic maps. *Chaos, Solitons and Fractals*, 23(2):413–419, 2005.

[74] Michael Weiss. Performing relay attacks on ISO 14443 contactless smart cards using NFC mobile equipment. Master's thesis, Technische Universität München, May 2010.

[75] Alan Wolf, Jack B. Swift, Harry L. Swinney, and John A. Vastano. Determining Lyapunov exponents from a time series. *Physica D: Nonlinear Phenomena*, 16(3):285–317, 1985.

[76] Xilinx. *Xilinx LogiCORE IP floating-point operator v5.0*, March 2011.

[77] Hong Zhou and Xie-Ting Ling. Problems with the chaotic inverse system encryption approach. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 44(3):268–271, March 1997.

[78] Li-Hai Zhou and Zheng-Jin Feng. A new idea of using one-dimensional PWL map in digital secure communications-dual-resolution approach. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, 47(10):1107–1111, 2000.