Chapter 1

Introduction

A cellular automaton is a decentralized computing model providing an excellent platform for performing complex computation with the help of only local information. Researchers, scientists and practitioners from different fields have exploited the cellular automaton paradigm of local information, decentralized control and universal computation for modeling different applications. This modeling tool can be regarded as parallel processing computer simulating logical universe with its own local physics and emergent structures [202]. The researchers have explored the possibility of building cellular automaton model having the capacity for self-reproduction and other essential functions of biomolecules leading to the possibility of life-like behavior [46]. In this background, cellular automaton has been projected as an essential tool for the study of physical systems [237].

Cellular automaton (CA) model is sufficiently complex to develop an entire universe as sophisticated as the one in which we live. CA allows a programmer to specify rules for local interaction between ‘cells’ on a lattice-like grid and to study the emergent consequences of those rules. Von Neumann [142, 201] first envisioned the fact that proper specification of rules can empower CA to build models simulating bacterial growth, the growth of patterns on seashells, fluid dynamics, and the voting patterns of individuals who take decisions based on their local neighbors.

One of the most important milestones in the history of development of the simple homogeneous structure of CA is due to Wolfram [226]. The simplification leads to an one/two dimensional structure of simple cells, each having two states with uniform three-neighborhood dependence. It further motivated a number of researchers, as reported in the book [33], to undertake the study of CA behavior for next state function amenable to matrix algebraic analysis. This new group of researchers explored innovative applications of this simple, regular, modular, and cascaddable structure of CA having local neighborhood.

The last decades of twentieth century have witnessed a colossal stride in the power
of computation and communication leading to the development of Internet Technology. While pushing civilization to new heights, such technological advancement has opened up new challenges to the human society of cyber age.

The issue of ‘cyber crime’ has become a major challenge for law-makers, government officials, social workers and technologists around the globe. In this context, research in the fields of authentication for message as well as image has got renewed emphasis. Several approaches have been proposed [56, 67, 89, 169, 241] to solve this problem out of which one-way hash function based solution is the most popular. However, to make message and image authentication available anywhere like on the mobile set etc., a high speed, low cost hardwired implementation of the one-way hash function used is the necessity. The sparse network of cellular automata (CA) can provide efficient, cost effective hardwired solution for one-way hash function.

As the thesis is based upon two important subjects (a) cellular automata and (b) authentication and watermarking, a brief review of each of the subject is presented next. More relevant reviews are presented in the chapters where each of the topic is elaborately discussed.

1.1 A Survey On Cellular Automata

Cellular Automata (CA) is a simple model of a spatially extended decentralized system, made up of a number of individual components (cells). The communication between constituent cells is limited to local interaction. Each individual cell is in a specific state which changes over time depending on the states of its neighbors and as a whole may be regarded as a parallel processing computer. The concept of the homogeneous structure of CA was initiated in early 1950s by J. Von Neumann [143]. It was conceived as a general framework for modeling complex structures, capable of self-reproduction and self-repair. Subsequent developments [106, 127, 227, 235] have taken place in several phases. Current intensive interest in this field can be attributed to the phenomenal growth of VLSI technology that permits cost-effective realization of the simple structure of local-neighborhood CA. Research work reported in the field of CA till mid 1990 has been compiled in [33, 72, 173]. The next few sub-sections outline a concise up-to-date review of the theory and applications of this computing model as it has evolved in last few decades. We assemble the historical development of cellular automata under three distinct modules.

- Development of Cellular Automata as a computing model.
- Theory and applications of Cellular Automata.
- Recent developments.
1.1.1 CA Based Computing Model

The concept of CA as a model for biological self-reproduction was introduced by J. Von Neumann in 1950s. His primary interest was to derive a computationally universal cellular space with self-reproducing configurations [143]. The set of transition rules he proposed involves a five neighborhood CA with 29 states per cell that constitutes a universal computer. Subsequently, CA theory received closer attention from a large number of researchers. The researchers explored CA as a powerful computing model in diverse field of applications - it ranges from modeling of biological self-reproduction to the analysis of crystal structure. They established CA as sufficiently simple to allow detailed mathematical analysis, yet sufficiently complex to exhibit a wide variety of complicated phenomena. Its self organizing behavior attracted the people from diverse fields. The survey on evolution of CA machine as a computing model has been organized under following two headings.

- Initial phase of development.
- CA as a Modeling Tool.

**Initial Phase of Development**

The initial phase of development started with the investigation of CA as a class of mathematical computing model. The computational universality of CA was established in the early phase of development. The extensive studies on its computational capabilities have been reported in [5, 15, 43, 102, 130, 203].

The automata was originally described as a two dimensional infinite array of uniform cells referred to as cellular space with each cell interconnected to its four orthogonal neighbors. The popular structure of present day’s CA was introduced by Von Neumann in 1966 as a formal model of self-reproducing biological systems. The main purpose of Neumann was to bring the rigor of axiomatic and deductive treatment to the study of complicated natural system. The notion of self-production introduced by Neumann is asexual, in the sense that the offspring is derived from a single parent. A self-reproducing machine has the capability of universal computation.

Turing machines have been known to be computationally universal. One such universal Turing machine has 7 internal states and allows 4 symbols to be used. It has been shown that, an 18 state 1 dimensional CA with 3-neighborhood can simulate this 7 state 4 symbol Turing machine [188]. The work reported in [61] has experienced the simulation of Turing machine with cellular automata called reversible CA. The notable contributors in developing the theory of universality in Von Neumann CA model are Thatcher [201] and Burks [130]. The proof of computation universality of cellular automata has also been provided in [48, 120]. Simplifications in the theory were introduced by Codd, Banks, and Smith [15, 43, 187] and they established CA as the information processor. In [90, 189, 191] the researchers have further extended the analytical study of the CA machine and proposed it as a language recognizer.
It can be observed that during the early days, the theory has evolved in a fragmented way. A systematic and detailed study of CA was initiated by Yamada and Amoroso. Their contributions have been reported in [10, 245, 246]. Consequently, the CA based computing model attracted interest of a larger group of research community from different fields. Their collective endeavor established CA on a platform of sound mathematical tools like abstract algebra, topology, measure theory, and so on.

Amoroso and Cooper have studied one and two dimensional CA which after a finite number of steps reproduce its initial pattern [9]. The original CA described by Von Neumann used 29-states per cell. Since its inception, the CA research community proposed different structural variations of this machine to achieve higher computational power, simultaneously with ease of design and behavioral analysis. Codd [43] introduced the machine with 8-state per cell. Arbib provided a simple description of self-reproducing CA in [11]. Whereas, Banks [15] worked with the CA having 4-state cells. All these 2-d (two dimensional) CA are assumed to have 5-cell neighborhood (self and four orthogonal neighbors). The 9-cell neighborhood CA, with 2 states per cell, has been shown to be computation-universal [185] that implements a set of local rules to create the Game of Life [75]. The trade off in respect of neighborhood size versus number of states per cell, of 1-d CA capable of self reproduction, is reported in [188].

The properties of CA with varying (non-uniform) neighborhoods for the CA cells have been studied in [93]. On the other hand, the totalistic CA employ a variant of local interconnection (rules) for different cells. The computation power of this class of CA machine have been evaluated in [48]. A number of authors [31, 103, 175] have studied iterative cellular automata - the CA model where only a particular cell is given an input. Iterative CA is used as language recognizer and also for one-way communication. A special class of CA machine consists of reachable and non-reachable states in its state space distributed as inverted trees (Garden of Eden). Investigation of such a CA has started in 1970's [10, 138]; further developments in this direction are noted in [98, 97].

In mid 80's, Kinzel [101], Grassberger et. al. [77], Kaneko et. al. [96], and Domany et. al. [60] have started characterizing the statistical and mechanical properties of probabilistic CA. The reversibility conditions of probabilistic CA have been reported in [20, 78, 97, 207]. Sutner [195] has investigated the global reversibility of cellular automata and characterized its linear counterpart from the standpoint of algebra [196, 197]. In his work, Walker [218] has examined a family of sparsely connected Boolean nets to characterize the CA machines. On the other hand, Li et. al. [108], and Gutowitz [80] have defined several qualitative class of CA behavior based on statistical measures and described how the state space of CA is organized. Wootters et. al. [242], Barbe [16], Voorhees [216], and Jen [92] have also contributed in
characterizing CA with different set of tools. Characterization of CA with linear and non-linear rules has been extensively studied during 1980-1990. The development of linear and non-linear CA theory provided the platform for characterization of comparatively complex non-linear rules by mapping its behavior to that of linear rules [92].

Characterizing the growth rate and fractional dimensions in cellular automata is an interesting research direction initiated through the work of Willson [222]. The apparently chaotic behavior of certain class of cellular automata have been studied in [224]. It has been shown that for CA with additive rules, the growth rate dimension, the Kolmogorov dimensions, and the Hausdorff dimensions coincide. Analytical tools for computing fractional dimensions of cellular automata have been reported in [223]. It has been established in [200] that there are correlations between dimensions of the space pattern of linear CA and fractals.

In the background of the initial phase of development reported earlier, a brief review on the applications of cellular automata as a modeling tool is next presented. CA as a Modeling Tool

CA has been used to model biological systems from the level of cell activity to the levels of clusters of cells and population of organisms. It has been used to model the kinetics of molecular systems and crystal growth in chemistry. In the discipline of physics, the applications cover the study of dynamical systems as diverse as the interaction of particles and the clustering of galaxies. While in computer science, the CA methods has been employed to model the Von Neumann (self-reproducing) machines [236] and as well as the parallel processing architecture.

The dynamical CA structure, where the cells may appear or disappear with time, is employed to model the growth for filamentary organism by Lindenmayer [111]. Many people in the field of artificial life have explored the CA to establish the fact that it preserves the essential function of biomolecules leading to the possibility of life-like behavior and consequently it has the capacity of self-reproduction. The first attempt in this direction was Von Neumann’s self-reproducing automata. An implementation of this construction was done in [4, 159]. Detailed study of artificial life with cellular automata has been explored by Langton in [107]. Langton [106] argued that computation universality is not a fundamental requirement for a self-reproducing automata.

Waterman [221] has identified some basic properties of entropy in CA behavior which encourage the applications of CA in information theory. Conway and his colleagues [21] have illustrated how extremely simple CA rules can be used to characterize very complex system behaviors such as ‘Game of Life’. The game was originally proposed by Conway and made popular through Martin Gardner [75, 76]. The motivation was to design a simple set of rules to study the macroscopic behavior of a population.
In machine design, the application of CA was proposed for building parallel multipliers [12, 44], prime number sieves [64], parallel processing computers [119, 165], and also for sorting machine [145]. The CA as a fault-tolerant computing machine has been projected in [142, 146]. The 2-dimensional CA has been used extensively for image processing and pattern recognition [172, 193]. Subsequently in 1983, MPP (Massively Parallel Processor) was completed by Goodyear Aerospace Corporation [62], which was one of the fastest computers of that time. CA based machines termed as CAMs (CA Machines) have been developed by Toffoli and others [204]. These CAMs operate in autonomous mode. The structure of such machines having high degree of parallelism (with local and uniform interconnection) is ideally suited for simulation of complex systems [206]. A CAM can achieve simulation performance at least several order of magnitude higher than that can be achieved with a conventional computer at comparable cost. CAM was developed over a decade of machine and modeling research by the Information Mechanics Group at MIT [79].

The CA structure with its state space distributed as a set of inverted trees (‘Garden of Eden’) has been established as a powerful modeling tool. Properties of the state space generated by such machines have been studied in a number of research works. Notable among these is the work of Kaneko [94] that introduced an information theoretic approach for a system referred to as multi-attractor system. This helps to characterize the complexity of ‘Garden of Eden’ states in terms of its volumes, stability against noise, information storage capacity, etc. To impose the accuracy in modeling of dynamical systems, a number of metrics have been proposed. One of these metrics is Lyapunov Exponents defined for dynamical system lattices in [95]. In continuation of this trend, Culik II et. al. [63] have studied CA to model complexity within a system. CA based language recognition was initiated by Kim [100]. Carter [27] investigated the effective use of CA based structure for molecular level computing.

A number of CA applications have been reported in the fields of DNA sequences, stripe, solution of differential equations etc. [25, 148, 186, 248]. It has been shown that CA could be used as general purpose computers performing complex computations. The trend continued further with the effort of researchers from all disciplines. The cellular automata has been proposed as an alternative to differential equations in modeling laws of physics [205]. CA models for physical systems with an emphasis on spin systems [47, 112, 161, 214], models for various forms of regular, dendritic and random growth based on two-dimensional CA [151], models for pattern formation in reaction-diffusion systems [115, 149, 225], modeling of hydrodynamical systems [69], etc. are some of the major applications investigated. The successful application of cellular automata in modeling the immune system have been also explored by Celada, Seiden, and De Boer et. al. [24, 29].

Since the publication of Von Neumann’s seminal work in late 1950s, the study of artificial self-replicating structures has produced plethora of results [184]. The
studies have raised the possibility of using such self-replicating machine to perform computations [183]. In [34], it is shown that self-replicating structures can be used to solve the NP-complete problem known as satisfiability. Recently researchers have begun to explore the cellular automata as typical computing devices - it has been presented as a manometer-scale classical computer in [19].

The works reported in [91, 131] have proposed cellular automata based associative memory model to successfully replace the dense neural net based models. A number of researchers [91, 131, 167] have also studied the pattern recognition capacity of CA-based associative memory. Efficient design of pattern recognizable CA that display encouraging results has been reported in [73, 74, 116, 117].

In this subsection we have reviewed the evolution of CA theory and its applications as a modeling tool. In general, the cell of such a CA is a complex one with reasonable computing power. CA with simplified cell structure is reviewed next.

1.1.2 Additive Cellular Automata

A breakthrough in the study of cellular automata (CA) was initiated by Wolfram [227, 228, 229] with the introduction of a simplified cell structure. He identified several characteristic features [230, 231, 232, 233, 234] of self organization in 3-neighborhood (left, right and self) CA with 2-state per cell. This class of cellular automata is referred to as $GF(2)$ CA. Based on the dynamical behavior, Wolfram [229] broadly classified the 3-neighborhood CA into 4 categories - (i) Class 1: CA which evolve to a homogeneous state; (ii) Class 2: those which evolve to simple separated periodic structures; (iii) Class 3: which exhibit chaotic or pseudo-random behavior [232]; and (iv) Class 4: yield complex patterns of localized structures and are capable of universal computation.

With advancement in VLSI technology, cost effective realization of $GF(2)$ CA having simple, regular and modular structure is highlighted by a number of researchers [33, 85, 178]. It has been projected as an alternative to LFSR (Linear Feedback Shift Register) having irregular interconnection structure. Further, the potential of CA has been exploited in many applications - such as Built-In-Self Test (BIST) for VLSI circuits, error correcting codes, data encryption etc. In this background, a large number of researchers started investigating the characterization and applications of local neighborhood CA. Notable among the researchers are Hortensius [85], Serra [176, 178] and Pal Chaudhuri [33].

The above scenario of mid 80s motivated the researchers at the Indian Institute of Technology (IIT), Kharagpur, to investigate the applications of the simple structure of CA. The research group concentrated on building an analytical framework to study the state transition behavior of CA employing only XOR/XNOR next state logic of a CA cell. A wide variety of applications have been proposed with this class of CA. Such a CA is referred to as Additive CA while the cellular automata employing
only XOR logic is referred to as linear CA. All the results of this study have been compiled in the book [33].

Applications
A significant progress has been made for characterization of additive CA behavior and its application in VLSI domain, specially in VLSI design and test, error correcting codes, cryptography, etc. The matrix algebraic tools are developed for complete analysis of the state transition behavior of additive CA [52, 54]. The study characterizes the state transition behavior of cellular automata as group and non-group properties. In a group CA all the states are reachable from some other states of the machine. Analysis of 1-d linear CA is reported in [137, 176]. In [28], the authors proposed the synthesis of 1-d linear hybrid CA having different rules for different CA cells. While the researchers concentrate on developing the theory of 1-d additive cellular automata, Chowdhury et al. [35, 40] have proposed the two dimensional structure of additive cellular automata and studied its efficiency in different field of applications. The applications of additive cellular automata in VLSI domain are summarized in the following discussions.

- VLSI Design and Test
Based on Wolfram classification CA are found to be most suitable for pseudo random pattern generation (PRPG) [229] and Hortensius [84] proposed it for built-in self-test in VLSI circuits. The major contributions in this direction are reported in [35, 50, 176, 177, 178, 209, 210]. Chowdhury [35], Das [50, 53] and Tsalide et al. [209, 210] also proposed the CA as a framework for built in self test (BIST) structures. Applications of CA are also investigated by Albicki et al. [6, 7, 8] and Das et al. [50, 51] and subsequently, Nandi [139] has established CA as a universal test pattern generator. In this regard other contribution in VLSI are found in [30, 37, 86, 122, 125, 126, 128, 171, 178].

- Error correcting codes
Chowdhury et. al. [36] introduced the CA-Based Error Correcting Codes (CAECC). The encoder/decoder circuit complexity for CAECC has been shown to be lesser than that of well known Hsiao code [87]. The CA based single byte error correcting and double byte error detecting code proposed in [41] was found to be superior than other schemes in terms of throughput and silicon area.

- Design of CA based Cipher system
Nandi et. al. [140] presented an elegant low cost scheme for CA based cipher system design. Both block ciphering and stream ciphering strategies designed with programmable cellular automata (PCA) have been reported.
• Pattern Classification

A novel approach for implementation of hashing scheme in hardware has been presented in [38, 39]. The method uses CA as its central controlling hardware. Essentially, the scheme provides a cheaper alternative to content addressable memories (CAM). CA based associative memory is employed for pattern classification. Tzionas et. al. [212] also proposed two dimensional additive cellular automata (2 - d CA) as a pattern classifier. The hamming distance and entropy variations induced on the patterns by the evolution of the 2 - d CA establish the fact that it is possible to implement the pattern classifier with variable discrimination sensitivity. Chattopadhyay et. al. [32] has recently observed that a special class of CA, referred to as MACA, behaves as a natural classifier. Such results are also covered in the book [33].

• Compression

Bhattacharya et al. [22] proposed methods to use CA to perform text compression. Olu Lafe reported a novel technique of deriving CA transform functions for compression and encryption [105]. CA based transform have been investigated by Paul [155, 156] and Shaw [179] for developing efficient schemes for image compression.

Next, we explore an upcoming and highly promising application area of cellular automata. It deals with message authentication and image authentication.

• Design of CA based Authentication Scheme

Dasgupta et al. [55] proposed an ASIC design for message authentication. The scheme has been refined by the current author by using GF(2^n) CA [135] and has been further extended for inserting invisible watermark in images [134]. The watermark can be either fragile where the watermark serves the purpose of authentication or it can be semi-fragile where the watermark serves the purpose of copyright protection. Fragile watermarking is particularly important in the domain of medical images while semi-fragile watermarking plays important role for transfer of video/audio over the Internet. This thesis along with other published work of the current author [134, 135, 136] make a significant contribution in addressing this specific area.

Dasgupta et al. further [150] has observed that a special class of CA, referred to as SACA, behaves as a natural unique hash addresser. Such results are also covered in the book [33]. This thesis further characterizes the reachable and non-reachable states of SACA and develops the applications of authentication for messages as well as images. Some of these results have been published in [134, 135, 136, 181].
A brief survey of authentication and watermarking follows. The detailed survey of each of the topic is presented in the chapter where we present our schemes.

1.2 A Survey On Authentication and Watermarking

Authentication is the study of verifying the integrity and authenticity of information which is a prime necessity in computer and network systems. In particular two parties communicating over an insecure channel require a method by which information sent by one party can be validated as authentic (or unmodified) by the other [18]. A number of surveys on authentication are published at regular intervals [162, 163, 238] that enables one to have a focused look into the recent trends in this field.

An authentication protocol is a sequence of message exchanges between principals (parties) that either distributes secrets to some of those principals or allows the use of some secret to be recognized [26, 194]. At the end of the protocol the principals involved may deduce certain properties about the system; for example, that only certain principals have access to particular secret information (typically cryptographic keys) or that a particular principal is operational. They may then use this information to verify claims about subsequent communication, for example, a received message encrypted with a newly distributed key must have been created after distribution of that key and so is timely [42]. See M. Burrows et. al [26] to get an overview of the different authentication protocols specified and implemented.

Conventionally authentication of message or image is based on cryptographic hash functions designed for SHA by a research group [147] and MD5 by Rivest [169] where the key is incorporated within the message. However, the conventional MD5 based message authentication, as reported in [174], cannot withstand advanced cryptanalytic attacks. The weakness of MD5 has also been established by Bakhtiar et. al [13, 14] and by Dobbertin [59]. Preneel has criticized SHA as well as MD5 [163]. In this light CA based authentication scheme is introduced in this thesis to ensure higher security.

Watermarking is the act of embedding another signal (the watermark) into an image, the embedding of which protects owners rights [166]. The process of embedding the watermark requires modifying the original image and in essence the watermarking process inserts a controlled amount of “distortion” in the image [110]. This “distortion” may be a small image called watermark image. The recovery of this distortion allows the one to identify the owner of the image. Thus image authentication as well as copyright protection of image can be achieved through watermarking.

Watermarks may be visible or invisible, where a visible mark is easily detected by observation while an invisible mark is designed to be transparent to the observer and detector [123, 166]. In the class of transparent watermarks one may further categorize techniques to be fragile or robust [110].
• A fragile mark is designed to detect slight changes to the watermarked image with high probability. The main application of fragile watermarking is in content authentication [110, 250].

• A robust mark is designed to resist attacks that attempt to remove or destroy the mark. Such attacks include lossy compression, filtering, and geometric scaling [110].

• Semi-fragile watermarking is robust to some perceptual quality preserving manipulations (lossy compression) but fragile to others [250].

A number of surveys on fragile watermarking [65, 67, 132, 144] and on semi-fragile/robust watermarking [109, 114, 158, 220] are published at regular intervals that enabled us to take a focused look into the recent trends in this field. In this thesis we have developed one fragile and two semi-fragile watermarking schemes. For fragile watermarking state of the art scheme is the scheme developed by Wong and Menon in [241] where as the methods developed by Hsu and Liu in [88] and by Wang, Doherty and Dyck in [220] are state of the art schemes for semi-fragile watermarking schemes. Our algorithm performs better than the schemes considered as state of the art.

In the above background, we report the focus of the research undertaken in this thesis.

1.3 Aim of the Dissertation

The thesis undertakes study of cellular automata which employ only xor & xnor logic in the next state function of a cell. This class of CA is referred to as GF(2^p) CA [33]. The major focus of this research is to explore the applications of this class of simple modeling tool in the important area of message/image authentication. In order to effectively use such tool, an in-depth characterization of GF(2^p) CA is considered as an essential prerequisite.

The basic framework is extended to study a special class of GF(2^p) CA termed as single attractor cellular automata (SACA). This class of CA can effectively model a unique addressing hash function. The framework is employed to synthesize a SACA that generates keyed one-way hash function. The function is then used in the proposed authentication and watermarking methods.

1.4 Organization of the Dissertation

We have reported a comprehensive survey of the relevant research publications in chapter 1 and chapter 2. The survey covers the following aspects:

• A general study of the methods employed to characterize cellular automata.
A brief outline of the concepts and major results of GF(2) CA and GF(2^n) CA is provided along with a brief review of extension field theory. ¹

- Applications of cellular automata with special emphasis on modeling authentication problem.

Chapter 3 describes characterization of a special class of GF(2^n) CA referred to as single attractor CA (SACA). SACA characterization leads to building of an one-way hash function discussed in next chapter.

In chapter 4 we report a SACA based message authenticator. The SACA-based one-way hash function has been modeled using both single and multiple SACA. The one-way hash function based on SACA and its application in message authentication are the major focus of this chapter. Subsequent study and experimental results establish SACA based one-way hash function as an efficient tool for modeling a message authenticator.

The application of SACA based one-way hash function is extended for watermarking schemes in chapter 5 and 6. Watermarking schemes are employed in many applications such as image authentication, copyright protection etc. Some of these applications demand secured one-way hash function, so the SACA based one-way hash function has its direct relevance for designing different watermarking schemes for image copyright protection.

Chapter 5 covers image authentication through fragile watermarking. In fragile watermarking no intentional or unintentional image processing which can cause data loss of the host image is allowed. Special applications of fragile watermarking are image authentication for medical, defense images where we need to have the exact unaltered image.

However in practice we need watermarking which accomodates image processing like lossy compression. Such type of watermarking serves the purpose of copyright protection etc. Watermarking which are robust to lossy compression is reported in chapter 6. Depending on the type of lossy compression such as JPEG or JPEG2000 lossy compression the watermarking schemes have been designed accordingly. One discrete cosine transform (DCT) based watermarking scheme and another discrete wavelet transform (DWT) based watermarking scheme have been developed to resist data alteration due to JPEG and JPEG2000 lossy compression respectively in chapter 6.

The last chapter concludes the thesis and provides direction for future research.

¹In this thesis, since we only deal with GF(2^n) CA, unless otherwise mentioned a GF(2^n) cellular automata is referred to as simple cellular automata.