Chapter 3

Single Attractor Cellular Automata

In this chapter, we provide a detailed analysis of the state transition behavior of a special class of non-group GF(2^p) CA. The special class of non-group GF(2^p) CA is referred to as single attractor cellular automata (SACA). SACA has a special characteristic in its state transition behavior which leads to a perfect hash function and that can be used in message authentication in the form of one-way hash function (next chapter details it).

3.1 Non-group CA and Attractor

The state transition diagram of a non-group CA consists of a set of cyclic as well as non-cyclic (referred to as transient) states. The non-cyclic states are represented by run of transient states forming an inverted tree rooted on a cyclic states.

The cycles in the state transition diagram of a non-group CA are referred to as attractors. Thus an attractor is a cycle of length i, (i ≥ 1). A state with a self-loop is referred to as a graveyard state. However, for sake of brevity, in this thesis the term attractor is used to denote graveyard state only.

The maximum run of the transient states is termed as depth (d) of the CA. Thus the depth d can be viewed as the number of clock cycles necessary for a CA to reach a cyclic state starting from a non-reachable state.

In the next section we discuss the special class of non-group CA referred to as single attractor cellular automata (SACA). SACA has been used to build a perfect hash function which will be discussed in subsequent section. A GF(2) SACA is also referred as two predecessor single attractor cellular automata (TPSA CA) and the details of TPSA CA can be found in [33].
3.2 Single Attractor Cellular Automata (SACA)

SACA, that is single attractor cellular automata is discussed in this section. The state transition graph of the SACA forms a single inverted tree rooted at a single attractor.

An $n$ cell SACA has maximum depth $n$. Here depth $n$ can be viewed as the number of clock cycles necessary for the SACA to reach its only attractor starting from a non-reachable state.

The state transition graph of 3 cell GF($2^2$) SACA is shown in figure 3.2. Its state transition graph has a single component of an inverted tree with its root as the state with self loop and referred to as ‘attractor’. Its depth is 3.

**Definition 3.1** A class of non-group CA at GF($2^p$) is called SACA (single attractor cellular automata) if it consists of a single attractor and the depth of the tree rooted at that attractor is $n$ where $n$ is the number of cells.

The following subsection extensively characterizes SACA.

3.2.1 Characterization of GF($2^p$) SACA

The CA belonging to the class of SACA and their complemented counterpart (dual SACA) possess some unique features that are explained in this section. One important theorem from [152] is reported below without the proof.

**Theorem regarding depth**:

**Theorem 3.1** If, for the largest value $d$, $x^d$ divides the minimal polynomial of the characteristic matrix $T$ of an $n$ cell GF($2^p$) CA, then the depth of the state-transition graph of the CA is $d$. 

![State transition diagram of 2 cell GF($2^2$) SACA](image-url)
Example 3.1 Consider the characteristic matrix $T$ of a 3 cell $GF(2^2) \ CA$ as
\[
\begin{pmatrix}
3 & 2 & 0 \\
3 & 1 & 2 \\
0 & 3 & 2
\end{pmatrix}
\]
then, $T + xI = \begin{pmatrix}
3 + x & 2 & 0 \\
3 & 1 + x & 2 \\
0 & 3 & 2 + x
\end{pmatrix}$. So, the characteristic polynomial as well as the minimal polynomial of this characteristic matrix is given by $det(T + xI)$, which is equal to $x^3$. Therefore the depth of the entire state transition graph will be 3. \hfill \Box

Hence minimal polynomial as well as characteristic polynomial $x^n$ must characterizes an $n$ cell $SACA$ at $GF(2^p)$.

**Theorem regarding rule number**: Following theorem on characterization of $SACA$ at $GF(2^p)$ is introduced here with proof.

**Theorem 3.2 The null boundary non-group CA where rule 170 is applied to all n cells always characterizes SACA at $GF(2^p)$.**

**Proof**: Rule 170 is already defined and referred in table 2.1 of section 2.1 at page 17. As per table 2.1 rule 170 : $q_i(t+1) = q_i(t)$. Therefore next state of a cell $q_i$ at $(t + 1)^{th}$ instant depends only on its right neighbor $q_{i+1}$ at $t^{th}$ instant for rule 170.

For example if we construct the characteristic matrix of a 4 cell $CA$ at $GF(2^2)$ such that all 4 cells follow rule 170, then the characteristic matrix of the $CA$ is,
\[
T_{4 \times 4} = \begin{pmatrix}
0 & a_{01} & 0 & 0 \\
0 & 0 & a_{12} & 0 \\
0 & 0 & 0 & a_{23} \\
0 & 0 & 0 & 0
\end{pmatrix},
\]
where $a_{ij}$ means the element at $i^{th}$ row and $j^{th}$ column of $T$ matrix and $a_{ij} \in GF(2^p)$; $a_{ij} \neq 0$ where $j = i + 1 \ \forall i = 0$ to 2. The characteristic polynomial as well as the minimal polynomial of this matrix becomes $x.x.x.x$ that is $x^4$.

To make it general if we form the characteristic matrix of $n$ cells $CA$ at $GF(2^p)$ where all the $n$ cells follow rule 170, then the matrix becomes
\[
T_{n \times n} = \begin{pmatrix}
0 & a_{01} & 0 & \cdots & \cdots & \cdots & 0 \\
0 & 0 & a_{12} & 0 & \cdots & \cdots & 0 \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
0 & \cdots & 0 & a_{(k-1)k} & 0 & \cdots & 0 \\
0 & \cdots & 0 & a_{k(k+1)} & 0 & \cdots & 0 \\
0 & \cdots & 0 & \cdots & \cdots & \cdots & 0 \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & a_{(n-2)(n-1)} \\
0 & \cdots & \cdots & \cdots & \cdots & 0 & 0
\end{pmatrix},
\]
and the characteristic polynomial as well as minimal polynomial of this matrix becomes $x^n$ and $\forall i = 0$ to $(n - 1)$, $a_{ij} \in GF(2^p)$ and $a_{ij} \neq 0$ where $j = i + 1$. Hence from this minimal polynomial and employing theorem 3.1 we obtain a $n$ cell $SACA$ at $GF(2^p)$ and hence the proof follows. \hfill \Box
Definition 3.2 The null boundary non-group CA where rule 170 is applied for all \( n \) cells is a \( SACA \) at \( GF(2^p) \) and henceforth named as \( SACA170 \).

Example 3.2 The state transition diagram and characteristic matrix of a 2 cell \( SACA170 \) at \( GF(2^2) \) is depicted through figure 3.1. \( \square \)

Theorem 3.3 The depth of a particular state in an \( n \) cell \( SACA170 \) at \( GF(2^p) \) can be stated specifically

Proof: If \( T \) be the characteristic matrix of an \( n \)-cell \( SACA170 \) at \( GF(2^p) \) then \( T^i \) always contains first \( i \) all zero columns and last \( i \) all zero rows. Hence any arbitrary state \( S = [a_0, a_1, \ldots, a_{n-1}] \) at depth \( i \) must have \( i \) zeros from its \( lsb \) (non-reachable states are at depth 0) like this \([a_0, a_1, \ldots, a_{n-i-1}, 0, \ldots, 0] \), where \( a_{n-i-1} \) must be non-zero for an \( n \) cell \( SACA170 \) at \( GF(2^p) \) and for rest of the bits there is no restriction for values. \( \square \)

Example 3.3 figure 3.1 displays a 2-cell \( SACA170 \) at \( GF(2^2) \) whose characteristic matrix, \( T_{2 \times 2} = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} \). If we want to get the states of this \( SACA170 \) at depth 1 then as \( T^1 \) contains first 1 all zero column and last 1 all zero row. Hence any arbitrary state \( S \) at depth 1 will be like this \([a_0, 0] \), where \( a_0 \) is strictly non-zero. Hence the states at depth 1 will be \([1,0], [2,0] \) and \([3,0] \) as depicted in figure 3.1 which satisfies the above theorem. \( \square \)

Theorem 3.4 Rank of an \( n \)-cell \( SACA170 \) is equal to \( n - 1 \)

Proof: The characteristic matrix of an \( n \)-cell \( SACA170 \) is like this-

\[
T_{n \times n} = \begin{pmatrix}
0 & a_{q1} & 0 & \cdots & \cdots & \cdots & 0 \\
0 & 0 & a_{12} & 0 & \cdots & \cdots & 0 \\
0 & \cdots & 0 & a_{k(k-1)k} & 0 & \cdots & 0 \\
0 & \cdots & 0 & 0 & a_{k(k+1)} & 0 & \cdots \\
0 & \cdots & 0 & \cdots & \cdots & \cdots & 0 \\
0 & \cdots & 0 & \cdots & \cdots & \cdots & 0 \\
0 & \cdots & 0 & \cdots & \cdots & \cdots & 0 \\
0 & \cdots & 0 & \cdots & a_{n-2(n-1)} & \cdots & 0 \\
0 & \cdots & 0 & \cdots & \cdots & a_{n-2(n-1)} & 0
\end{pmatrix}
\]

The rank of the matrix can be directly derived as \( n - 1 \) [57]. \( \square \)

Example 3.4 Considering the same \( T \) matrix as in figure 3.1 where we have a 2 cell \( SACA \) at \( GF(2^2) \) whose rank is \( 2 - 1 = 1 \). \( \square \)

Theorem 3.5 An \( n \)-cell non-group \( CA \) at \( GF(2^p) \) with \( T \) as characteristic matrix, has only one attractor if the depth of its state transition graph is equal to the number of cells that is \( n \).
Proof: Since at GF(2^p) an n cell non-group CA with characteristic matrix T, the number of attractors are \((2^p)^{(n-r)}\), where \(r\) is the rank of the \((T \oplus I)\) [from [152]]. Therefore as an n cell SACA at GF(2^p) the rank of \((T \oplus I)\) is \(n\) hence the number of attractor is \((2^p)^{(n-n)}=1\), that means it has a single attractor. \(\square\)

Example 3.5 From figure 3.1 this is clear that a 2 cell SACA at GF(2^2) whose characteristic matrix
\[
\begin{pmatrix}
0 & 2 \\
0 & 0 \\
\end{pmatrix}
\]
has 1 attractor that is [0 0], and the depth is 2 that is equal to the number of cells. \(\square\)

Theorem 3.6 Each reachable state of the SACA at GF(2^p) has \(2^p\) predecessors.

Proof: If \(\{x_1, x_2, \ldots, x_k\}\) are \(k\) linearly independent vectors of a \(k\)-dimensional vector space, then any vector in that space can be expressed as a linear combination of these \(k\) vectors as:
\[
\sum_{i=1}^{k} a_i x_i; \ a_i \in \text{that field.}
\]
Since the rank of an \(n\) cell SACA at GF(2^p) is always \(n-1\) (from previous theorem), the dimension of its null space is \(n - (n-1)=1\) ([152]). Therefore there exist only one linearly independent vector \(x_1\) (say) and hence any vector can be expressed as \(a_1 x_1; \ a_1 \in \text{GF}(2^p)\). Since there are \(2^p\) such linear combinations therefore there exist exactly \(2^p\) distinct predecessors for any reachable state. \(\square\)

From the figure 3.1 it is shown that the state transition diagram of a 2 cell SACA at GF(2^2) has \(2^2\) distinct predecessors for its all reachable state.

Theorem 3.7 Each combination of \((n - 1)\) non-zero variables at GF(2^p) in characteristic matrix of an \(n\) cell SACA170 leads to a unique state transition graph

Proof: Let, the characteristic matrix \(T\) for an \(n\) cell SACA170 at GF(2^p) be,
\[
T = \begin{pmatrix}
0 & a_1 & 0 & \ldots & \ldots & \ldots & 0 & 0 \\
0 & 0 & a_2 & \ldots & \ldots & \ldots & 0 & 0 \\
0 & 0 & 0 & \ldots & \ldots & \ldots & 0 & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & \ldots & \ldots & \ldots & \ldots & 0 & a_{n-1} \\
0 & 0 & \ldots & \ldots & \ldots & \ldots & 0 & 0 \\
\end{pmatrix}
\]
such that \(\forall i = 1 \text{ to } (n-1), \ a_i \in \text{GF}(2^p)\) and \(a_i \neq 0\). Each combination of these all \(n-1\) non-zero variables that is \(a_i, \forall i = 1 \text{ to } (n-1)\) leads to characteristic matrices for \(n\) cell SACA170 at GF(2^p).

We have to prove that all these SACA170s produce different state transition graphs that means each combination of \((n-1)\) non-zero variables at GF(2^p) leads to a unique state transition graph.
Let, $S_0$ and $S_1$ be two states of an $n$ cell $SACA_{170}$ at $GF(2^p)$ state transition graph such that $S_0$ is a present state and $S_1$ is its next state then $T.(S_0) = S_1$, where $T$ is constructed as above.

If $S_0$ is an all ‘1’ state then next state $S_1$ will be generated by T as

$$
\begin{pmatrix}
0 & a_1 & 0 & \ldots & \ldots & 0 & 0 \\
0 & 0 & a_2 & \ldots & \ldots & 0 & 0 \\
0 & 0 & 0 & \ldots & \ldots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & \ldots & a_{n-1} & 0 \\
0 & 0 & 0 & \ldots & \ldots & 0 & 0
\end{pmatrix}
\times
\begin{pmatrix}
1 \\
1 \\
\vdots \\
\vdots \\
1 \\
1
\end{pmatrix}
= 
\begin{pmatrix}
a_1 \\
a_2 \\
\vdots \\
\vdots \\
a_{n-1} \\
0
\end{pmatrix}.
$$

That is $S_1$ is $[a_1, a_2, a_3, a_4, \ldots, a_{n-2}, a_{n-1}, 0]$. Therefore if at least one of these $a_i$ is changed then $S_0$ goes to a different next state $S_1$. Hence each combination of these $a_i$ leads to a unique state. \hfill \Box

Following table summarizes different $SACA$ properties at a glance.

<table>
<thead>
<tr>
<th>Depth</th>
<th>$n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td>$n-1$</td>
</tr>
<tr>
<td>No. of attractor</td>
<td>1</td>
</tr>
<tr>
<td>No. of predecessors for each reachable state</td>
<td>$2^p$</td>
</tr>
</tbody>
</table>

### 3.3 Dual $SACA$

The complemented $SACA$ $C_k'$, resulting from the complementation of the next state functions of some cells in a $SACA$ $C_k$ such that all reachable states of $C_k$ becomes non-reachable states of $C_k'$ and $C_k$, $C_k'$ are isomorphic (for each state of $C_k$ there is a state at corresponding state diagram position of $C_k'$) - is referred to as dual $SACA$. The definition is reproduced from [33].

Figure 3.3 depicts a 3 cell dual $SACA$ at $GF(2^2)$ for the corresponding 3 cell $SACA$ at $GF(2^2)$ at figure 3.2. Here the complementation of the next state functions of all three cells has taken place. The inversion vector $F$ (referred to previous chapter) is here $[1 \ 1 \ 1 ]$.

The definition of dual $SACA$ (henceforth also termed as $\overline{SACA}$) is formally presented for ease of readability.

**Definition 3.3** Dual $SACA$: Given a $SACA$ with characteristic matrix $T$, then $SACA$ formed from $(T, F)$ is a dual $SACA$ or, $\overline{SACA}$, if that $SACA$ possess the following two properties
Clock $n = 3$, $p=2$, therefore elements are 0,1,2,3.

- $r =$ Rank = 2, Depth = 3
- Characteristic polynomial = $x^3$
- Minimul polynomial = $x^3$
- No. of predecessor = $\frac{r^p}{r} = 4$
- No. of non reachable states = 48
- Cyclic states = 000
- Attractor = 000

At $GF(2^p)$ field where $p = 2$,

\[
a^2 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \quad a^3 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \quad a^1 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \quad 0 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}
\]

\[
T = \begin{bmatrix} 3 & 2 & 0 \\ 3 & 1 & 2 \\ 0 & 3 & 2 \end{bmatrix}, \quad D = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad F = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}
\]

Figure 3.2: State transition diagram of 3 cell $GF(2^2)$ SACA
Attractor = 302    Depth = 3

Figure 3.3: State transition diagram of 3 cell GF(2²) dual SACA
• State transition graph of $\overline{SACA}$ is isomorphic to that of $SACA$.

• All reachable states in the $SACA$ are non-reachable states at its state transition graph of $\overline{SACA}$.

We also refer it as $\overline{SACA}(T, F)$ or simply $\overline{SACA}$.

The $\overline{SACA}$ in figure 3.3 is in fact a 3 cell dual $SACA$ corresponding to the 3 cell $SACA$ of figure 3.2. It exhibits the above two mentioned properties.

• State transition diagram of $\overline{SACA}$ at figure 3.3 is isomorphic to that of $SACA$ at figure 3.2.

• State $(1 \ 1 \ 0)$ is a reachable state at $SACA$ of figure 3.2 and this becomes a non-reachable state at $\overline{SACA}$ (figure 3.3) and so is for all other reachable states of $SACA$ at figure 3.2.

An $n$-cell $SACA$ at GF(2$^p$) is represented by a $T$ matrix while an $n$-cell dual $SACA$ at GF(2$^p$) is represented by $T$ matrix and $F$ vector.

The inversion vector $F$ of $\overline{SACA}$ exhibit special property which is stated next.

**Theorem 3.8 If the complement vector $F$ of an $n$ cell $SACA$ at GF(2$^p$) is such that $T^n.F = 0$, the all zero column vector, then this complemented $SACA$ is a dual $SACA$.**

**Proof :** Let, the state transition graphs of $SACA$ and its complemented part at GF(2$^p$) be $C_1$ and $C'_1$, where the complementation of $SACA$ is done with $F$ (as stated in this theorem). We have to prove that if $T^n.F = 0$ then this complemented $SACA$ is dual that means $C_1$ and $C'_1$ are isomorphic.

Let, $S$ be any arbitrary state of $C_1$ and define the state $S' = S \oplus F$ to be the dual state of $S$ in $C'_1$. Clearly for every state $S$ of $C_1$, there is a unique state $S'$ of $C'_1$. Also if there exist two directed edges $(S_1 \rightarrow S)$ and $(S_2 \rightarrow S)$ in $C_1$ such that $S_1$, $S_2$ are two non-reachable states in $C_1$ and $S$ is reached from $S_1$ after $(n + 1)$ clock cycles, where as $S$ is reached from $S_2$ after $(n)$ clock cycles. Then it essentially means that,

$$T^{n+1}S_1 = S \text{ and } T^nS_2 = S \Rightarrow T^{n+1}S_1 = T^nS_2 = T^n(TS_1) = T^nS_2 \quad (3.1)$$

Since all $n$ columns of $T^n$ are all zero,

$$\text{therefore } TS_1 = S_2 \oplus F \quad (3.2)$$

where $F$ is a vector whose $n$ bits (from msb) are not all zero. Now, if this $F$ constitutes dual $SACA$ $C'_1$ then there exists $S'_1$ and $S'_2$ in $C'_1$ such that

$$S'_1 = S_1 + F \text{ and } S'_2 = S_2 + F \quad (3.3)$$
From (3.2) and (3.3)

\[ TS_1 = S'_2 \quad (3.4) \]

Now, if this \( C'_1 \) is isomorphic with \( C_1 \) then there must be two directed edges \( (S'_1 \rightarrow S') \) and \( (S'_2 \rightarrow S') \) in \( C'_1 \) such that \( S'_1, S'_2 \) are two non-reachable states in \( C'_1 \) and \( S' \) is reachable from \( S'_1 \) after \( (n + 1) \) clock cycles, where as \( S' \) is reached from \( S'_2 \) after \( (n) \) clock cycles. That means

\[ T^{n+1}S'_1 + (T^n + T^{n-1} + ... + T + I)F = S' \quad \text{and} \quad T^nS'_2 + (T^{n-1} + T^{n-2} + ... + T + I)F = S' \]

Therefore \( C_1 \) and \( C'_1 \) are isomorphic if

\[ T^{n+1}S'_1 + (T^n + T^{n-1} + ... + T + I)F + T^nS'_2 + (T^{n-1} + T^{n-2} + ... + T + I)F = S' + S' = 0. \]

Therefore \( T^{n+1}S'_1 + (T^n + T^{n-1} + ... + T + I)F + T^nS'_2 + (T^{n-1} + T^{n-2} + ... + T + I)F = T^{n+1}(S_1 + F) + T^nTS_1 + T^nF \) [From (3.3) and (3.4)]

\[ = T^{n+1}S_1 + T^nS_1 + T^{n+1}F + T^nF \]

\[ = [T + I]T^nF \]

Now since \( T^nF = 0 \), therefore \( [T + I]T^nF = 0 \), hence the proof. \( \square \)

It is to be mentioned that not all the possible \( F \) vectors produce \( \overline{SACA} \).

**Corollary 3.1** The inversion vector \( F \) of an \( \overline{SACA} \) (\( T, F \)) displays the following feature \( T^n \cdot F = 0 \) while \( T^{n'} \cdot F \neq 0 \) where \( n' < n \) (from theorem 3.8).

**Corollary 3.2** There exist \( 2^{p(n-1)} \times (2^p - 1) \) duals for an \( n \)-cell \( SACA170 \) at \( GF(2^p) \) that means there is exactly \( 2^{p(n-1)} \times (2^p - 1) \) \( F \)-vectors for which \( C_1 \) and \( C'_1 \) are isomorphic.

**Proof:** From the above theorem \( T^nF = 0 \) but \( T^{n-1}F \neq 0 \). Now, for \( n \) cell \( SACA170 \) at \( GF(2^p) \), \( T^n \) has exactly \( n \) column(s) all zero vectors and \( T^{n-1} \) has exactly \( n - 1 \) column all zero vectors. Therefore each \( F \) vector can vary at most \( (n - 1) \) bits (from msb) but the \( n^{th} \) bit must be some non-zero element \( \in GF(2^p) \). Hence there exist \( 2^{p(n-1)} \times (2^p - 1) \) \( F \) vectors which produces isomorphic duals. \( \square \)

**Example 3.6** For a 2 cell \( SACA170 \) at \( GF(2) \) there will exist \( 2^{1(2-1)} \times (2^1 - 1)=2 \) duals as shown in figure 3.4. Here the \( F \) vectors for the duals are as shown in figure 3.4. Similarly for a 2 cell \( SACA170 \) at \( GF(2^2) \), there will exist \( 2^{2(2-1)} \times (2^2 - 1)=12 \) duals. Here the \( F \) vectors for the duals can be calculated as follows.

If \( a_0, a_1 \) are 2 cell positions (\( a_0 \) be the left most cell position) of the \( F \) vector then, \( a_1 \) is always non-zero. As \( a_0, a_1 \in GF(2^2) \) hence \( a_1 \) can vary from 1 to \( 2^2 - 1 = 4 \) but \( a_0 \) can vary from 0 to \( 2^2 - 1 = 3 \). Hence the 12 dual \( F \) vectors are \[ [1 0], [2 0], [3 0], [1 1], [2 1], [3 1], [1 2], [2 2], [3 2], [1 3], [2 3], [3 3]. \] \( \square \)
Dual \( SACA \) also possesses all the properties of \( SACA \) as described in table 3.1. figure 3.3 depicts the example.

A \( SACA \) and its dual (\( SACA \)) can act as an efficient unique address generator. This is discussed next.

3.3.1 \( SACA \) as a Unique Address Generator

A very important class of functions are the perfect hashing functions. A perfect hash function for a given set of keys maps each key to a unique address and thus acts as a unique address generator. One major advantage is derived from using a perfect hashing scheme, it needs no collision, deletion, or overflow and thus generates unique address. However, perfect hashing functions are rare. A detailed survey on existing perfect hashing functions along with their problems are found in chapter 8 [33].

In chapter 8 [33] it has been proved that how a GF(2) \( SACA \) can generate perfect hash functions. It has been depicted over there that when such a \( CA \) is loaded with the key (to be perfectly hashed) as the initial seed, the address bits for the key can next be extracted from the successive states of the \( CA \) as it runs in autonomous mode in successive clock cycles. The theoretical analysis of \( CA \) state transition diagram has enabled us to identify precisely the address bits to be extracted for perfect hashing [33].

We present the overview of \( SACA \) based unique address generator from [150]. An (\( SACA, SACA \)) pair is also referred to as \( SS \). The \( SS \) constitutes a unique address mapping function; this function is termed as \( Unique\_Map\_SS \). Given a key \( k \), the address generated through \( Unique\_Map\_SS(k)=h \), where \( h \) is unique for \( k \). The steps for mapping of a given key \( k \) which produces a unique address \( h \) is noted in algorithm 3.1.

An \( n \)-symbol key produces a unique address if it is a non-reachable state in \( SACA \). If a state is reachable in \( SACA \), then it is non-reachable in its dual \( SACA \). With this information, the algorithm for unique address generator is reported from chapter 8 [33] and each step of the algorithm is supplemented here with an example.

Algorithm 3.1 \( Unique\_Map\_SS \) (\( k \))

Input: Key \( k \) of \( n \times p \) bits; and \( n \) cell GF\((2^n)\) \( SACA, SACA \)

Output: Address \( h \) of \( n \times p \) bits

Step 1: If \((k \in \text{non-reachable state in SACA})\)

Load \( k \) in \( SACA \) else load \( k \) in \( SACA \).

Step 2: Run \( k \) in \( SACA \) \( (SACA) \) in autonomous mode till it reaches the attractor.

Step 3: Extract least significant symbol (LSS) from each of the states reached during transition and form the unique address.
\[
T = \begin{bmatrix}
0 & 1 \\
0 & 0
\end{bmatrix}
\quad F = \begin{bmatrix}
a_0 \\
a_1
\end{bmatrix}
\]

Minimal Polynomial \( x^2 \)

Depth = 2 and Cycle Structure \([ 1(1) ]\)

Since \( T^2 F = 0 \) and \( TF \neq 0 \)

Therefore,
\[
\begin{bmatrix}
0 & 0 \\
0 & 0
\end{bmatrix} \ast \begin{bmatrix}
a_0 \\
a_1
\end{bmatrix} = \begin{bmatrix}
0 \\
0
\end{bmatrix}
\]

and
\[
\begin{bmatrix}
0 & 1 \\
0 & 0
\end{bmatrix} \ast \begin{bmatrix}
a_0 \\
a_1
\end{bmatrix} = \begin{bmatrix}
a_1 \\
0
\end{bmatrix} \neq \begin{bmatrix}
0 \\
0
\end{bmatrix}
\]

Hence \( a_1 \) must be 1 and \( a_0 \) can be any element from GF(2) field

that means either 0 or, 1

Figure 3.4: State transition graphs of a 2 cell SACA at GF(2) and its all duals
Example 3.7 Let key $k$ be of $3 \times 2 = 6$ bits in a 3 cell $GF(2^2)$ SACA, $\overline{SACA}$, if key $k$ is a non-reachable state in SACA and is equal to 6 bits (01 11 11) that is 3 symbols (1 3 3) then as shown in figure 3.5, $k$ (1 3 3) gets the transition during its run in autonomous mode as follows: (1 3 3) $\rightarrow$ (2 1 3) $\rightarrow$ (3 1 2) $\rightarrow$ (0 0 0), where (0 0 0) is the attractor.

Therefore least significant symbol (LSS) from each of the states reached during transition are 3, 3 and 2. Consequently, it produces the hash address $h = [3 3 2]$ for (1 3 3) as shown in figure 3.5.

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{example_3.7_diagram.png}
\caption{Unique hash addressing using 3 cell $GF(2^2)$ SACA}
\end{figure}

3.4 Conclusion

The SACA and its dual $\overline{SACA}$ display some unique features that have been exploited in this chapter and based on that designing of the one-way hash function emerged which is detailed at next chapter. SACA, $\overline{SACA}$ based unique address generator is used iteratively to import one-way-ness to the hash function. A SACA
and its dual $\overline{SACA}$ together can act as an excellent one-way hash function which is a prerequisite for designing a good authentication scheme. We elaborate the methodology of building one-way hash function through message authentication scheme in the next chapter.