A secret sharing scheme based on cellular automata

A. Martín del Rey a,*, J. Pereira Mateus b, G. Rodríguez Sánchez c

a Department of Applied Mathematics, University of Salamanca C/Santo Tomás s/n 05003 Ávila, Spain
b Department of Mathematics, Technical Institute of Guarda, 6300 Guarda, Portugal
c Department of Applied Mathematics, University of Salamanca Avda. Requejo 33, 49022 Zamora, Spain

Abstract

A new secret sharing scheme based on a particular type of discrete delay dynamical systems: memory cellular automata, is proposed. Specifically, such scheme consists of a \((k, n)\)-threshold scheme where the text to be shared is considered as one of the \(k\) initial conditions of the memory cellular automata and the \(n\) shares to be distributed are \(n\) consecutive configurations of the evolution of such cellular automata. It is also proved to be perfect and ideal.

© 2005 Elsevier Inc. All rights reserved.

Keywords: Cellular automata; Cryptography; Discrete dynamical systems; Secret sharing; Threshold scheme
1. Introduction

Secret sharing schemes are cryptographic procedures to share a secret among a set of participants in such a way that only some qualified subsets of these participants can recover the secret (see [1]).

Such schemes were independently introduced by Shamir (see [2]) and Blakley (see [3]) and their original motivation was to safeguard cryptographic keys from loss. Currently, they have many applications in different areas such as access control, opening a safety deposit box, etc.

The basic example of secret sharing scheme is the \((k, n)\)-threshold scheme, where \(k\) and \(n\) are integers numbers such that \(1 \leq k \leq n\). The structure of this scheme is as follows: there exists a mutually trusted party (or a dealer) which computes \(n\) secret shares from an initial secret and securely distributes them into \(n\) participants in such a way that any \(k\) or more of these participants who pool their shares may easily recover the original secret, but any group knowing only \(k - 1\) or fewer shares are unable to recover the secret. Shamir’s scheme, which is based on polynomial interpolation, and Blakley’s scheme, based on the intersection of affine hyperplanes, are examples of \((k, n)\)-threshold schemes.

A secret sharing scheme is perfect if the size of every share is greater or equal than the size of the shared secret. Moreover, when these two sizes are equal, the secret sharing scheme is called ideal. For a more detailed description of these schemes we refer the reader to [4–6].

In this work we use a particular type of delay discrete dynamical systems called memory cellular automata in order to share a secret text. Basically, memory cellular automata are discrete dynamical systems formed by a finite number of identical objects called cells. These cells are endowed with a state which changes at every discrete step of time according to a deterministic rule whose variables are the states of a set of cells at previous time steps (see [7,8]).

The use of cellular automata to design cryptosystems goes back to middle eighties when Wolfram proposed the cellular automaton with rule number 30 as a pseudorandom bit generator (see [9]) for cryptographic purposes. Since then, many CA-based cryptosystems have been proposed not only for text (see, for example, [10–18]) but also for images (see [19,20]).

The rest of the paper is organized as follows: In Section 2, the basic definitions about memory cellular automata are introduced; in Section 3 the secret sharing scheme based on memory cellular automata is presented with its security analysis. Finally, the conclusions are shown in Section 4.

2. One-dimensional memory cellular automata

One-dimensional finite Boolean cellular automata (CA for short) are discrete dynamical systems formed by a finite one-dimensional array of \(n\) identical
objects called cells, in such a way that each one of them can assume a state: 0 or 1. The \( i \)-th cell is denoted by \( h_i \), and the state of this cell at time \( t \) is \( a(t) \). The CA evolves deterministically in discrete time steps, changing the states of all cells according to a local transition function. The updated state of each cell depends on the variables of the local transition function, which are the previous states of a set of cells, including the cell itself, and constitutes its neighbourhood. In this work, symmetric neighbourhoods of radius \( r \) are considered; for every cell \( h_i \) it is defined as follows: \( V_i = \{ h_{i-r}, \ldots, h_i, \ldots, h_{i+r} \} \). As a consequence, the local transition function is of the following form:

\[
a^{(t+1)}_i = f \left( a^{(t)}_{i-r}, \ldots, a^{(t)}_i, \ldots, a^{(t)}_{i+r} \right), \quad 0 \leq i \leq n - 1,
\]

or equivalently, \( a^{(t+1)}_i = f(V^{(t)}_i) \), where \( V^{(t)}_i \) stands for the states of the neighbour cells of \( h_i \) at time \( t \). The vector \( C(t) = (a^{(t)}_0, \ldots, a^{(t)}_{n-1}) \) is called the configuration at time \( t \) of the CA, and \( C(0) \) is the initial configuration of the CA. Moreover, the sequence \( \{C(t)\}_{0 \leq t \leq k} \) is called the evolution of order \( k \) of the CA, and \( \mathcal{C} \) is the set of all possible configurations of the CA; consequently \( |\mathcal{C}| = 2^n \). As the number of cells of the CA is finite, boundary conditions must be considered in order to assure the well-defined dynamics of the CA. In this work, periodic boundary conditions are taken: if \( i \equiv j \pmod{n} \), then \( a^{(t)}_i = a^{(t)}_j \).

The global function of the CA is a linear transformation, \( \Phi : \mathcal{C} \rightarrow \mathcal{C} \), that yields the configuration at the next time step during the evolution of the CA, that is, \( C^{(t+1)} = \Phi(C^{(t)}) \). If \( \Phi \) is bijective then there exists another cellular automaton, called its inverse, with global function \( \Phi^{-1} \). When such inverse cellular automaton exists, the cellular automaton is called reversible and the evolution backwards is possible.

Let us consider the set of CA with symmetric neighborhoods of radius \( r \), whose local transition function are of the following form:

\[
a^{(t+1)}_i = \sum_{j=-r}^{r} \alpha_j a^{(t)}_{i+j} \pmod{2}, \quad 0 \leq i \leq n - 1,
\]

where \( \alpha_j \in \mathbb{F}_2 \) for every \( j \). They are called linear cellular automata of order \( r \) (\( r \)-th order LCA for short). As there are \( 2r + 1 \) cells in the symmetric neighbourhood of radius \( r \), then there exist \( 2^{2r+1} \) LCAs, and every one of them can be conveniently specified by a decimal integer called rule number: \( \omega \), which is defined as follows:

\[
\omega = \sum_{j=-r}^{r} \alpha_j 2^{r+j},
\]

where \( 0 \leq \omega \leq 2^{2r+1} - 1 \).

The standard paradigm for CA states that the state of every cell at time \( t + 1 \) depends on the state of some cells (its neighbourhood) at time \( t \). Nevertheless,
one can consider CA for which the state of every cell at time \( t + 1 \) not only depends on the states of some cells at time \( t \) but also on the states of (possible) another different groups of cells at times \( t - 1, t - 2, \) etc. This is the basic idea of memory cellular automata (MCA for short) (see [8]). In this paper, we consider a particular type of MCA called \( k \)-th order linear MCA (LMCA for short) for which their local transition functions are of the following form:

\[
a_i^{(t+1)} = f_1(V_i^{(t)}) + f_2(V_i^{(t-1)}) + \cdots + f_k(V_i^{(t-k+1)}) (\text{mod } 2),
\]

with \( 0 \leq i \leq n - 1 \), and \( f_i \) is the local transition function of a particular \( r \)-th order LCA. In this case, the configurations \( C^{(0)}, \ldots, C^{(k-1)} \) are called initial configurations of the \( k \)-th order LMCA.

**Proposition 1.** If \( f_k(V_i^{(t-k+1)}) = a_i^{(t-k+1)} \), then the LMCA given by (3) is a reversible CA, whose inverse CA is another \( k \)-th order LMCA with local transition function:

\[
a_i^{(t+1)} = \sum_{m=0}^{k-2} f_{k-m-1}(V_i^{(t-m)}) + a_i^{(t-k+1)} (\text{mod } 2),
\]

for \( 0 \leq i \leq n - 1 \).

**Proof.** Suppose \( \{C^{(t)}\}_{t \geq 0} \) is the evolution of the LMCA given by (3), where \( C^{(t)} = (a_0^{(t)}, \ldots, a_{n-1}^{(t)}) \) is the configuration at time \( t \), and let \( \{\tilde{C}^{(t)}\}_{t \geq 0} \) be the evolution of the LMCA given by (4), where \( \tilde{C}^{(t)} = (\tilde{a}_0^{(t)}, \ldots, \tilde{a}_{n-1}^{(t)}) \). The proof ends if we show that \( \tilde{C}^{(k+1)} = C^{(t-k+1)} \) when \( \tilde{C}^{(1)} = C^{(1)} \), \( \tilde{C}^{(2)} = C^{(2)} \), \ldots, \( \tilde{C}^{(k)} = C^{(k)} \), for every \( t \). Consequently, by simply applying (4) we obtain:

\[
a_i^{(k+1)} = f_{k-1}(\tilde{V}_i^{(k)}) + f_{k-2}(\tilde{V}_i^{(k-1)}) + \cdots + f_1(\tilde{V}_i^{(2)}) + \tilde{a}_i^{(1)} (\text{mod } 2),
\]

for \( 0 \leq i \leq n - 1 \). As \( \tilde{C}^{(m)} = C^{(t-m+2)} \) with \( 1 \leq m \leq k \), then \( \tilde{V}_i^{(m)} = V_i^{(t-m+2)} \) with \( 1 \leq m \leq k \). As a consequence, taking into account the value of \( C_i^{(t+1)} \) given by (3), the Eq. (5) yields:

\[
a_i^{(k+1)} = f_{k-1}(V_i^{(t-k+2)}) + f_{k-2}(V_i^{(t-k+3)}) + \cdots + f_1(V_i^{(t)}) + a_i^{(t+1)}
\]
\[
= f_{k-1}(V_i^{(t-k+2)}) + f_{k-2}(V_i^{(t-k+3)}) + \cdots + f_1(V_i^{(t)})
\]
\[
+ f_1(V_i^{(t)}) + \cdots + f_{k-2}(V_i^{(t-k+3)}) + f_{k-1}(V_i^{(t-k+2)}) + a_i^{(t-k+1)}
\]
\[
= a_i^{(t-k+1)} (\text{mod } 2),
\]

for every \( 0 \leq i \leq n - 1 \), thus \( \tilde{C}^{(k+1)} = C^{(t-k+1)} \) and we conclude. □
3. The secret sharing scheme based on LMCA

In this section we propose a new secret sharing scheme. It consists of a \((k,n)\)-threshold scheme such that the text to be shared, \(S\), is one of the initial configurations of a \(k\)-th order LMCA, specifically \(S = C^{(0)}\). The rest \(k - 1\) components of the initial configuration, \(C^{(1)}, \ldots, C^{(k-1)}\), are \(k - 1\) random Boolean vectors of the same size than \(S\). The shares to be distributed among the \(n\) participants are \(n\) consecutive configurations of the evolution of the LMCA. The proposed scheme is formed by three phases which are shown in the following subsection.

3.1. Structure of the scheme

As it is mentioned above, the structure of the procedure to share secrets by means of LMCA is divided into three phases: the setup phase, in which the LMCA used is defined as well as its initial conditions; the sharing phase, in which the evolution of the LMCA is computed and, consequently, the shares to be distributed among the participants are obtained; and finally, the recovery phase, which allows the participants to recover the shared secret.

3.1.1. The setup phase

1. The mutually trusted party computes a random integer \(r\) such that \(0 \leq r \leq \lfloor l/2 \rfloor - 1\), where \(l\) is the bit-length size of the secret to be shared. The integer \(r\) stands for the radius of the neighbourhood of the LMCA.
2. The mutually trusted party computes a sequence of \(k - 1\) integers numbers:
\[
\{\omega_1, \ldots, \omega_{k-1}\},
\]
such that \(0 \leq \omega_i \leq 2^{2r + 1} - 1\) with \(1 \leq i \leq k - 1\), by means of a cryptographic secure pseudorandom number generator (see [4, Section 5.5]). These numbers stand for the rule numbers of the LCA constituting the LMCA used.
3. The mutually trusted party constructs the reversible \(k\)-th order LMCA with local transition function:
\[
a_i^{(t+1)} = f_{\omega_1}(V_i^{(t)}) + \cdots + f_{\omega_{k-1}}(V_i^{(t-k+2)}) + a_i^{(t-k+1)}(\text{mod } 2),
\]
where \(f_{\omega_j}\) is the local transition function of the \(r\)-th order LCA with rule number \(\omega_j\), \(1 \leq j \leq k - 1\), and \(0 \leq i \leq n - 1\).
4. The vector representing the secret to be shared is considered as the initial configuration \(C^{(0)}\), and the mutually trusted party computes the rest \(k - 1\) initial configurations: \(C^{(1)}, \ldots, C^{(k-1)}\), by using a cryptographic secure pseudorandom number generator.
3.1.2. The sharing phase

1. The mutually trusted party chooses a random integer number \( m \), such that \( m \geq k \).
2. Starting from the initial configurations \( C^{(0)}, \ldots, C^{(k-1)} \), the mutually trusted party computes the \((n + m - 1)\)-th order evolution of the LMCA:

\[
\{ C^{(0)}, \ldots, C^{(k-1)}, C^{(k)}, \ldots, C^{(m)}, \ldots, C^{(m+n-1)} \}.
\]

3. The shares to be distributed among the \( n \) participants are the last \( n \) configurations computed:

\[
S_1 = C^{(m)}, \ldots, S_n = C^{(n + m - 1)}.
\]

Note that \( m \geq k \) is considered to avoid overlappings between the initial conditions and the shares.

3.1.3. The recovery phase

The following steps are the reveal phase using any consecutive \( k \) (of the \( n \)) shares:

1. To recover the secret, \( C^{(0)} \), a set of consecutive shares of the form

\[
C^{(m+z)}, \ldots, C^{(m+z+k-1)}, \quad 0 \leq z \leq n - k,
\]

is needed.
2. Taking \( C^{(0)} = C^{(m+z+k-1)}, \ldots, \tilde{C}^{(k-1)} = C^{(m+z)} \), and iterating \( m + z + k - 1 \) times the inverse LMCA we obtain the secret: \( C^{(0)} \).

3.2. Security analysis

As the bit-length size of every distributed share is equal to the bit-length size of the secret (both are configurations of the same LMCA), the proposed scheme is ideal. Furthermore, it is also perfect because if only one configuration of the form \( C^{(t - i)} \), with \( 0 \leq i \leq k - 1 \), is unknown, say for example, \( C^{(t-k+1)} = (a_i^{(t-k+1)}) \), where \( 0 \leq i \leq n - 1 \), then there is no information about the configuration \( C^{(t+1)} \) because the evolution of the LMCA is given by the following linear system:

\[
a_i^{(t+1)} = b_i + a_i^{(t-k+1)}(\text{mod } 2), \quad 0 \leq i \leq n - 1,
\]

where

\[
b_i = f_{01} \left( V_i^{(t)} \right) + \cdots + f_{ok-1} \left( V_i^{(t-k+2)} \right).
\]
Consequently, as it is formed by \( n \) equations with \( 2n \) unknown variables: \( a_{i}^{(r+1)}, a_{i}^{(r-k+1)} \), where \( 0 \leq i \leq n - 1 \), then it cannot be solved and, obviously, no information about the configuration \( C^{(r+1)} = (a_{i}^{(r+1)}) \), \( 0 \leq i \leq n - 1 \), is obtained. Note that a similar result holds if the number of unknown configurations is greater than one.

As a consequence, for the secret sharing scheme proposed it is impossible to recover the secret starting from \( k - 1 \) (or less) shares.

3.3. An example

For the sake of simplicity, let us consider a (3,4)-threshold scheme for texts of 64 bits, defined by the reversible LMCA with \( r = 1 \) and local transition function:

\[
a_{i}^{(r+1)} = f_{3}(V_{i}^{(t)}) + f_{5}(V_{i}^{(t-1)}) + a_{i}^{(t-2)} \text{ (mod 2)}, \quad 0 \leq i \leq n - 1, \tag{6}
\]

where \( \omega_{1} = 7 \) and \( \omega_{2} = 5 \), that is:

\[
a_{i}^{(r+1)} = a_{i-1}^{(t)} + a_{i}^{(t)} + a_{i+1}^{(t)} + a_{i-1}^{(t-1)} + a_{i+1}^{(t-1)} + a_{i}^{(t-2)} \text{ (mod 2)},
\]

\( 0 \leq i \leq n - 1. \)

Suppose that the text to be shared is represented by the following sequence of bits:

\[
S = \{0,1,1,1,0,0,1,1,0,1,0,1,1,1,0,1,0,1,1,1,1,0,1,1,1,0,1,1,1,0,0,1,1,0,0,0,0,1,0,1,1,0,0,1,1,0\},
\]

and the rest of configurations needed to initialize the evolution of the automata are:

\[
C^{(1)} = \{1,0,1,1,1,0,1,1,1,1,1,0,1,0,0,1,0,1,0,0,1,0,1,0,1,0,1,1,1,0,0,0,0,1,1,1,1,0,0,0,1,0,1,1,0,0,0,0,1,1\},
\]

\[
C^{(2)} = \{0,1,1,1,1,0,1,0,1,1,1,1,1,1,1,0,0,0,1,0,1,1,1,0,0,1,1,1,1,0,0,1,1,1,0,0,1,0,1,1,1,1,1,1,0,1,1,1,1,0,0,0,0,1,1\},
\]

which have been computed by means of BBS pseudorandom number generator (see [4]).
Then, if $m = 5$ the evolution of the LMCA given by (6) is as follows:

$C^{(3)} = \{1,1,1,0,1,0,1,0,1,1,0,1,1,0,1,0,1,1,1,0,0,1,0,0,1,0,1,0,1,0,1,0,1,0,1,1,1,1\}$,

$C^{(4)} = \{0,0,1,1,1,0,1,1,0,1,0,1,1,1,0,1,0,1,0,0,1,0,1,0,1,0,1,1,1,1,1,1,0,0,0,0,0,1,0,1\}$,

$C^{(5)} = \{1,0,0,0,1,0,0,0,0,0,0,0,1,0,0,1,1,1,0,1,1,1,0,0,0,1,0,1,0,0,0,0,1,0,1,0,0,0,0,0,1,0,1\}$,

$C^{(6)} = \{1,1,0,1,1,0,1,1,0,1,0,1,1,1,0,1,0,1,1,1,0,1,1,1,1,1,1,1,0,1,1,1,0,1,1,1,1,0\}$,

$C^{(7)} = \{1,1,1,0,0,1,1,1,0,0,0,0,0,0,1,1,0,1,0,1,0,0,1,0,1,1,1,1,1,0,0,0,0,1,1,1,1,0,1,0,1,1\}$,

$C^{(8)} = \{1,0,0,0,0,1,1,0,1,1,0,1,0,1,1,0,0,0,0,1,0,0,1,0,1,0,0,0,0,1,0,0,0,1,0,1,0,0,0,0,1,0,1,0,0\}$.

Consequently, the shares to be distributed among the four participants are $C^{(5)}$, $C^{(6)}$, $C^{(7)}$, and $C^{(8)}$.

4. Conclusions

In this paper a new $(k,n)$-threshold scheme for text sharing is presented and it is based in the use of one-dimensional reversible linear memory cellular automata. It is ideal and perfect because the size of the shares to be distributed and the size of the secret are equal, and no information about the secret is obtained if $k - 1$ or less shares are known.

Remark that the access structure (that is, the set of qualified subsets of participants to recover the shared secret) given by this protocol is different from the traditional access structure of a $(k,n)$-threshold scheme. In our case, not all the sets with, at least, $k$ participants can recover the secret, but also those containing a set of the form $\{P_i, \ldots, P_{i+k-1}\}$, with $1 \leq i \leq n+1-k$, where $\{P_1, \ldots, P_n\}$ are the participants.

Acknowledgements

This work has been supported by the Consejería de Educación y Cultura of Junta de Castilla y León (Spain) under grant SA052/03, by Ministerio de Educación y Ciencia (Spain) under grant SEG2004-02418, and by “D. Samuel Solórzano Barruso Memorial Foundation of the University of Salamanca.
References