Constructing Orthogonal Latin Squares from Linear Cellular Automata

Luca Mariot[1,2], Enrico Formenti[2] and Alberto Leporati[1]

[1] Dipartimento di Informatica, Sistemistica e Comunicazione, Università degli Studi di Milano-Bicocca, Viale Sarca 336, 20126 Milano, Italy
{luca.mariot,alberto.leporati}@unimib.it
[2] Laboratoire I3S, Université Nice Sophia Antipolis, 2000 Route des Lucioles, 06903 Sophia Antipolis, France
{mariot,enrico.formenti}@i3s.unice.fr

Abstract. We undertake an investigation of combinatorial designs engendered by cellular automata (CA), focusing in particular on orthogonal Latin squares and orthogonal arrays. The motivation is of cryptographic nature. Indeed, we consider the problem of employing CA to define threshold secret sharing schemes via orthogonal Latin squares. We first show how to generate Latin squares through bipermutive CA. Then, using a characterization based on Sylvester matrices, we prove that two linear CA induce a pair of orthogonal Latin squares if and only if the polynomials associated to their local rules are relatively prime.

Keywords: cellular automata · secret sharing schemes · Latin squares · orthogonal arrays · Sylvester matrices · bipermutivity · linearity

1 Introduction

Secret sharing schemes (SSS) are a cryptographic primitive underlying several protocols such as *secure multiparty computation* [1] and *generalized oblivious transfer* [8]. The basic scenario addressed by SSS considers a dealer who wants to share a secret S among a set of n players, so that only certain authorized subsets of players specified in an access structure may reconstruct S. In a (t,n)–*threshold scheme*, at least t out of n players must combine their *shares* in order to recover S, while coalitions with less than t participants learn nothing about the secret (in an information-theoretic sense).

Recently, a SSS based on cellular automata (CA) has been described in [5], where the shares are represented by blocks of a CA configuration. The main drawback of such proposal is that the access structure has a *sequential threshold*: in addition to having at least t players, the shares of an authorized subset must also be adjacent blocks, since they are used to build a spatially periodic preimage of a CA.

In order to design a CA-based SSS with an unrestricted threshold access structure, in this paper we take a different perspective that focuses on *combinatorial designs*. Indeed, it is known that threshold schemes are equivalent to *orthogonal arrays* (OA), and for $t = 2$ the latter correspond to *mutually orthogonal Latin squares* (MOLS).

The aim of this work is to begin tackling the design of a CA-based threshold scheme by investigating which CA are able to generate orthogonal Latin squares. To this end, we first show that every bipermutive cellular automaton of radius r and length $2m$ induces a Latin square of order q^m, where q is the cardinality of the CA state alphabet and m is any multiple of $2r$. We then investigate which pairs of bipermutive CA induce orthogonal Latin squares, by first observing through some experiments that only some pairs of *linear* CA seem to remain orthogonal upon iteration. We thus prove that the orthogonality condition holds if and only if the Sylvester matrix built by juxtaposing the transition matrices of two linear CA is invertible, i.e. if and only if the polynomials associated to their local rules are relatively prime. Finally, we show what are the consequences of this result for the design of CA-based threshold schemes. In particular, we remark that the dealer can efficiently perform the sharing phase by evolving a set of linear CA, but the question of how two players recombine their shares to recover the secret remains open.

The remainder of this paper is organized as follows. Section 2 covers the preliminary definitions and facts about cellular automata, Latin squares, orthogonal arrays and secret sharing schemes necessary to describe our results. Section 3 presents the main contributions of the paper, namely the proof that a pair of linear CA induce orthogonal Latin squares if and only if the associated polynomials are coprime. Finally, Section 4 puts the results in perspective, and discusses an open problem for further research on the topic.

2 Basic Definitions

2.1 Cellular Automata

In this work, we consider one-dimensional CA as *finite compositions of functions*, as the next definition summarizes:

Definition 1. *Let n, r, t be positive integers such that $t < \left\lfloor \frac{n}{2r} \right\rfloor$, and let $f : A^{2r+1} \to A$ be a function of $2r+1$ variables over a finite set A of $q \in \mathbb{N}$ elements. The* cellular automaton *(CA) $\langle n, r, t, f \rangle$ is a map $\mathcal{F} : A^n \to A^{n-2rt}$ defined by the following composition of functions:*

$$\mathcal{F} = F_{t-1} \circ F_{t-2} \circ \cdots \circ F_1 \circ F_0 \ , \tag{1}$$

where for $i \in \{0, \cdots, t-1\}$ function $F_i : A^{n-2ri} \to A^{n-2r(i+1)}$ is defined as:

$$F_i(x) = (f(x_0, \cdots, x_{2r}), f(x_1, \cdots, x_{2r+1}), \cdots, f(x_{n-2r(i+1)-1}, \cdots, x_{n-2ri-1})) \ , \tag{2}$$

for all $x = (x_0, \cdots, x_{n-2ri-1}) \in A^{n-2ri}$. In particular n, r and f are respectively called the length, *the* radius *and the* local rule *of the CA, while for all $i \in \{0, \cdots, t-1\}$ function F_i is called the* global rule *of the CA at step i.*

In some of the results proved in this paper we assume that the state alphabet A is a *finite field*, i.e. $A = \mathbb{F}_q$ for $q = p^\alpha$ where p is a prime number and $\alpha \in \mathbb{N}$.

A local rule $f : A^{2r+1} \to A$ is *rightmost permutive* (respectively, *leftmost permutive*) if, by fixing the value of the first (respectively, last) $2r$ variables the resulting restriction on the rightmost (respectively, leftmost) variable is a permutation over A. A local rule which is both leftmost and rightmost permutive is *bipermutive*, and a CA $\mathcal{F}$ whose local rule is bipermutive is a *bipermutive CA*.

Denoting by $+$ and $\cdot$ respectively sum and multiplication over the finite field $\mathbb{F}_q$, a local rule $f : \mathbb{F}_q^{2r+1} \to \mathbb{F}_q$ is *linear* if there exist $a_0, a_1, \cdots, a_{2r} \in \mathbb{F}_q$ such that

$$f(x_0, x_1, \cdots, x_{2r}) = a_0 x_0 + a_1 x_1 + \cdots + a_{2r} x_{2r} \ . \tag{3}$$

Analogously, a CA $\mathcal{F}$ whose local rule is linear is called a *linear* (or *additive*) CA. Notice that a linear rule is bipermutive if and only if both a_0 and a_{2r} are not null. The polynomial associated to a linear rule $f : \mathbb{F}_q^{2r+1} \to \mathbb{F}_q$ with coefficients $a_0, \cdots, a_{2r}$ is defined as

$$p_f(X) = a_0 + a_1 X + \cdots + a_{2r} X^{2r} \in \mathbb{F}_q[X] \ . \tag{4}$$

In a linear CA $\langle n, r, t, f \rangle$ with local rule f defined by the coefficients $a_0, \cdots, a_{2r} \in \mathbb{F}_q$, the global rule $F_i : \mathbb{F}_q^{n-2ri} \to \mathbb{F}_q^{n-2r(i+1)}$ at step $i \in \{0, \cdots, t-1\}$ is a linear application defined by the following matrix of $n - 2r(i+1)$ rows and $n - 2ri$ columns:

$$M_{F_i} = \begin{pmatrix} a_0 & \cdots & a_{2r} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_0 & \cdots & a_{2r} & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & a_0 & \cdots & a_{2r} \end{pmatrix} \ . \tag{5}$$

Thus, the global rule F_i is defined as $F_i(x) = M_{F_i} x^\top$ for all $x \in \mathbb{F}_q^{n-2r(i+1)}$, and the composition $\mathcal{F}$ corresponds to the multiplication of the matrices $M_{F_{t-1}} \cdots M_{F_0}$.

Consider now the case where $n = 2rt + 1$. The CA $\mathcal{F}$ maps vectors of $2rt + 1$ components to a single element of A. We call this particular function the *t–th iterate* of rule f, and we denote it by f^t. This leads to the following equivalence:

Lemma 1. *Let $\mathcal{F} : A^n \to A^m$ be a $\langle n, r, t, f \rangle$ CA with local rule $f : A^{2r+1} \to A$ such that $n = mk$ and $m = 2rs$ for $k, s \in \mathbb{N}_+$, and $t = m(k-1)/2r$. Then, $\mathcal{F}$ is equivalent to the iterated CA $\langle n, rt, 1, f^t \rangle$ $\mathcal{F}^{(t)} : A^n \to A^m$, i.e. for all $x = (x_0, \cdots, x_{n-1}) \in A^n$ it holds that*

$$\mathcal{F}(x) = \mathcal{F}_t(x) = (f^t(x_0, \cdots, x_{2rt}), f^t(x_1, \cdots, x_{2rt+1}), \cdots, f^t(x_{n-2rt-1}, \cdots, x_{n-1})) \ . \tag{6}$$

In particular, if $f : \mathbb{F}_q^{2r+1} \to \mathbb{F}_q$ is linear with associated polynomial $p_f(X)$, one can show (see e.g. [3]) that $f^t : \mathbb{F}_q^{2rt+1} \to \mathbb{F}_q$ is linear for all $t \in \mathbb{N}$, and its polynomial equals

$$p_{f^t}(X) = [p_f(X)]^t \ . \tag{7}$$

Thus, the coefficients of the iterated linear rule f^t are simply the coefficients of the polynomial $p_f(X)^t$.

2.2 Latin Squares, Orthogonal Arrays and Secret Sharing

We recall only some facts about Latin squares and orthogonal arrays which are relevant for threshold schemes, following the notation of Stinson [7].

Definition 2 (Latin square). *Let X be a finite set of $v \in \mathbb{N}$ elements. A* Latin square *of order v over X is a $v \times v$ matrix L with entries from X such that every row and every column are permutations of X. Two Latin squares L_1 and L_2 of order v defined over X are* orthogonal *if $(L_1(i_1, j_1), L_2(i_1, j_1)) \neq (L_1(i_2, j_2), L_2(i_2, j_2))$ for all $(i_1, j_1) \neq (i_2, j_2)$. In other words, L_1 and L_2 are orthogonal if by superposing them one obtains all pairs of the Cartesian product $X \times X$. A collection of k Latin squares $L_1, \cdots, L_k$ of order v which are pairwise orthogonal is called a set of k* mutually orthogonal Latin squares *(MOLS).*

Definition 3 (Orthogonal array). *Let X be a finite set of v elements, and let t, k and λ be positive integers such that $2 \leq t \leq k$. A t–(v, k, λ)* orthogonal array *(t–(v, k, λ)–OA, for short) is a $\lambda v^t \times k$ rectangular matrix with entries from X such that, for any subset of t columns, every t–uple $(x_1, \cdots, x_t) \in X^t$ occurs in exactly λ rows.*

A t–$(v, k, 1)$–OA can be used to implement a (t, n)*–threshold scheme* with $n = k - 1$ players $P_1, \cdots, P_{k-1}$ as follows. The dealer randomly chooses with uniform probability the secret S from the support set X and a row $A(i, \cdot)$ in the OA such that the last component equals S. Next, for all $j \in \{1, \cdots, k-1\}$ the dealer distributes to player P_j the share $s_j = A(i, j)$. Since the array is orthogonal with $\lambda = 1$, any subset of t players $P_{j_1}, \cdots, P_{j_t}$ can recover the secret, the reason being that the shares $(s_{j_1}, \cdots, s_{j_t})$ form a t–uple which uniquely identifies row $A(i, \cdot)$. Conversely, suppose that $t - 1$ players $P_{i_1}, \cdots, P_{i_{t-1}}$ try to determine the secret. Then, the $(t-1)$–uple $s = (s_{j_1}, \cdots, s_{j_{t-1}})$ occurs in the columns $j_1, \cdots, j_{t-1}$ in v rows of the array. By considering also the last column, one obtains a t–uple $(s_{j_1}, \cdots, s_{j_{t-1}}, A(i_h, k))$ for all $1 \leq h \leq v$. Since $\lambda = 1$, it must be the case that all these t–uples are distinct, and thus they must differ in the last component. Hence, the v rows where the $(t-1)$–uple $(s_{j_1}, \cdots, s_{j_{t-1}})$ appears determine a permutation on the last column, and thus all the values for the secret are equally likely.

When $t = 2$ and $\lambda = 1$, the resulting orthogonal array is a $v^2 \times k$ matrix in which every pair of columns contains all ordered pairs of symbols from X. In this case, the orthogonal array is simply denoted as $OA(k, v)$, and it is equivalent to a set of $k - 2$ MOLS. As a matter of fact, suppose that $L_1, \cdots, L_{k-2}$ are $k-2$ MOLS of order v. Without loss of generality, we can assume that $X = \{1, \cdots, v\}$. Then, consider a matrix A of size $v^2 \times k$ defined as follows:

- The first two columns are filled with all ordered pairs $(i, j) \in X \times X$ arranged in lexicographic order.
- For all $1 \leq i \leq v^2$ and $3 \leq h \leq k$, the entry (i, h) of A is defined as

$$A(i, h) = L_{h-2}(A(i, 1), A(i, 2)) \ . \tag{8}$$

In other words, column h is filled by reading the elements of the Latin square L_{h-2} from the top left down to the bottom right.

The resulting array is a $OA(k, v)$: indeed, let h_1, h_2 be two of its columns. If $h_1 = 1$ and $h_2 = 2$ one gets all the ordered pairs of symbols from X in lexicographic order. If $h_1 = 1$ (respectively, $h_1 = 2$) and $h_2 \geq 3$, one obtains all pairs because the h_1-th row (respectively, column) of L_{h_2-2} is a permutation over X. Finally, for $h_1 \geq 3$ and $h_2 \geq 3$ one still gets all ordered pairs since the Latin squares L_{h_1-2} and L_{h_2-2} are orthogonal. Due to lack of space, we omit the inverse direction from $OA(k, v)$ to $k-2$ MOLS. The reader can find further details about the construction in [7].

3 Main Results

We begin by showing that any bipermutive cellular automaton of radius r and length $2m$ induces a Latin square of order $N = q^m$, under the condition that m is a multiple of $2r$. To this end, we first need some additional notation and definitions.

Given an alphabet A of q symbols, in what follows we assume that a total order $\leq$ is defined over the set of m–uples A^m, and that $\phi : A^m \to [N]$ is a monotone one-to-one mapping between A^m and $[N] = \{1, \cdots, q^m\}$, where the order relation on $[N]$ is the usual order on natural numbers. We denote by $\psi = \phi^{-1}$ the inverse mapping of ϕ.

The following definition introduces the notion of square associated to a CA:

Definition 4. *Let m, r and t be positive integers such that $m = 2rt$, and let $f : A^{2r+1} \to A$ be a local rule of radius r over alphabet A with $|A| = q$. The* square *associated to the CA $\langle 2m, r, t, f\rangle$ with map $\mathcal{F} : A^{2m} \to A^m$ is the square matrix $\mathcal{S}_\mathcal{F}$ of size $q^m \times q^m$ with entries from A^m defined for all $1 \leq i, j \leq q^m$ as*

$$\mathcal{S}_\mathcal{F}(i,j) = \phi(\mathcal{F}(\psi(i)||\psi(j))) \ , \tag{9}$$

where $\psi(i)||\psi(j) \in A^{2m}$ denotes the concatenation of vectors $\psi(i), \psi(j) \in A^m$.

Hence, the square $\mathcal{S}_\mathcal{F}$ is defined by encoding the first half of the CA configuration as the row coordinate i, the second half as the column coordinate j and the output of the CA $\mathcal{F}(\psi(i)||\psi(j))$ as the entry in cell (i, j).

The next lemma shows that fixing the leftmost or rightmost $2r$ input variables in the global rules of a bipermutive CA yields a permutation between the remaining variables and the output:

Lemma 2 ([5]). *Let $\mathcal{F} : A^n \to A^{n-2rt}$ be a bipermutive CA $\langle n, r, t, f\rangle$ defined by local rule $f : A^{2r+1} \to A$, and let $F_i : A^{n-2ri} \to A^{n-2r(i+1)}$ be its global rule at step $i \in \{0, \cdots, t-1\}$. Then, by fixing at least $d \geq 2r$ leftmost or rightmost variables in $x \in A^{n-2ri}$ to the values $\tilde{x} = (\tilde{x}_0, \cdots, \tilde{x}_{d-1})$, the resulting restriction $F_i|_{\tilde{x}} : A^{n-2r(i+1)} \to A^{n-2r(i+1)}$ is a permutation.*

On account of Lemma 2, we now prove that the squares associated to bipermutive CA are in fact Latin squares. The proof follows the argument laid out in Lemma 2 of [5].

Lemma 3. *Let $f : A^{2r+1} \to A$ be a bipermutive local rule defined over A with $|A| = q$, and let $m = 2rt$ where $t \in \mathbb{N}$. Then, the square $L_\mathcal{F}$ associated to the bipermutive CA $\langle 2m, r, t, f\rangle$ $\mathcal{F} : A^{2m} \to A^m$ is a Latin square of order q^m over $X = \{1, \cdots, q^m\}$.*

Proof. *Let $i \in \{1, \cdots, q^m\}$ be a row of $L_\mathcal{F}$, and let $\psi(i) = x = (x_0, \cdots, x_{m-1}) \in A^m$ be the vector associated to i with respect to the total order $\leq$ on A^m. Consider now a vector $c_0 \in A^{2m}$ whose first m coordinates coincide with x, and let $c_1 = F_0(c_0)$ be the image of c under the global rule F_0. Then, by Lemma 2 there is a permutation $\pi_0 : A^m \to A^m$ between the rightmost m variables of c_0 and the rightmost m ones of c_1. Likewise, since the leftmost $m - 2r$ coordinates of c_1 are determined by applying the restriction of F_0 to x, it follows that there exists a permutation $\pi_1 : A^m \to A^m$ between the rightmost m variables of c_1 and the rightmost m ones of $c_2 = F_1(c_1)$. More in general, since m is a multiple of $2r$, for all steps $i \in \{2, \cdots, t-1\}$ there are always at least $2r$ leftmost variables of c_{i-1} determined, and thus by Lemma 2 there is a permutation $\pi_i : A^m \to A^m$*

between the rightmost m variables of $c_{i-1} = F_{i-1}(c_{i-2})$ and the rightmost m variables of $c_i = F_i(c_{i-1})$. Consequently, there exists a permutation $\pi : A^m \to A^m$ between the rightmost m variables of c_0 and the output value of $\mathcal{F}(c_0)$, defined as:

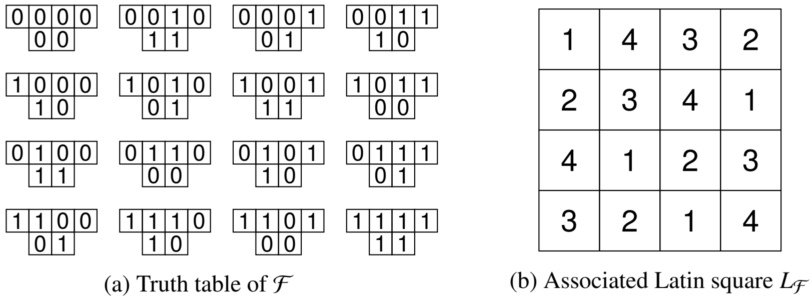
$$\pi = \pi_{t-1} \circ \pi_{t-2} \circ \cdots \circ \pi_1 \circ \pi_0 \ . \tag{10}$$

For all q^m choices of the rightmost m variables of c_0, the values at $L_{\mathcal{F}}(i,\cdot)$ are determined by computing $\phi(\mathcal{F}(c_0))$. As a consequence, the i-th row of $L_{\mathcal{F}}$ is a permutation of $X = \{1,\cdots,q^m\}$. A symmetric argument holds when considering a column j of $L_{\mathcal{F}}$ with $1 \le j \le q^m$, which fixes the rightmost m variables of $\mathcal{F}$ to the value $\psi(j)$. Hence, every column of $L_{\mathcal{F}}$ is also a permutation of X, and thus $L_{\mathcal{F}}$ is a Latin square of order q^m. □

As an example, for $A = \mathbb{F}_2$ and radius $r = 1$, Figure 1 reports the Latin square $L_{\mathcal{F}}$ the bipermutive CA $\mathcal{F} : \mathbb{F}_2^4 \to \mathbb{F}_2^2$ with rule 150, defined as $f_{150}(x_0, x_1, x_2) = x_0 \oplus x_1 \oplus x_2$.

We now aim at characterizing pairs of CA which generate orthogonal Latin squares. For alphabet $A = \mathbb{F}_2$ and radius $r = 1$ there exist only two bipermutive rules up to complementation and reflection, which are rule 150 and rule 90, the latter defined as $f_{90}(x_0, x_1, x_2) = x_0 \oplus x_2$. Both rules are linear, and for length $n = 4$ their associated Latin squares are orthogonal, as shown in Figure 2. For $r = 2$ and length $2m = 8$, a computer search among all 256 bipermutive rules of radius 2 yields 426 pairs of CA which generate orthogonal Latin squares of order $2^4 = 16$, among which are both linear and nonlinear rules. However, for length $2m = 16$ only 21 pairs of linear rules still generate Latin squares of order $2^8 = 256$. For this reason, we narrowed our investigation only to linear rules. When $m = 2r$, the following result gives a necessary and sufficient condition on the CA matrices:

Lemma 4. *Let $\mathcal{F} : \mathbb{F}_q^{4r} \to \mathbb{F}_q^{2r}$ and $\mathcal{G} : \mathbb{F}_q^{4r} \to \mathbb{F}_q^{2r}$ be linear CA of radius r, respectively with linear rules $f(x_0,\cdots,x_{2r}) = a_0x_0 + \cdots a_{2r}x_{2r}$ and $g(x_0,\cdots,x_{2r}) = b_0x_0 + \cdots b_{2r}x_{2r}$, where $a_0, b_0, a_{2r}, b_{2r} \neq 0$. Additionally, let $M_{\mathcal{F}}$ and $M_{\mathcal{G}}$ be the $2r\times4r$ matrices associated*



0000 00	0010 11	0001 01	0011 10
1000 10	1010 01	1001 11	1011 00
0100 11	0110 00	0101 10	0111 01
1100 01	1110 10	1101 00	1111 11

(a) Truth table of $\mathcal{F}$

1	4	3	2
2	3	4	1
4	1	2	3
3	2	1	4

(b) Associated Latin square $L_{\mathcal{F}}$

Fig. 1: Example of Latin square of order 4 induced by rule 150. Mapping ϕ is defined as $\phi(00) \mapsto 1$, $\phi(10) \mapsto 2$, $\phi(01) \mapsto 3$, $\phi(11) \mapsto 4$.

1	4	3	2
2	3	4	1
4	1	2	3
3	2	1	4

(a) Latin square of rule 150

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

(b) Latin square of rule 90

1,1	4,2	3,3	2,4
2,2	3,1	4,4	1,3
4,3	1,4	2,1	3,2
3,4	2,3	1,2	4,1

(c) Superposed square

Fig. 2: Orthogonal Latin squares generated by bipermutive CA with rule 150 and 90.

to the global rules $F_0 = \mathcal{F}$ and $G_0 = \mathcal{G}$ respectively, and define the $4r \times 4r$ matrix M as

$$M = \begin{pmatrix} M_{\mathcal{F}} \\ M_{\mathcal{G}} \end{pmatrix} = \begin{pmatrix} a_0 & \cdots & a_{2r} & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & a_0 & \cdots & a_{2r} & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & 0 & a_0 & \cdots & a_{2r} \\ b_0 & \cdots & b_{2r} & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & b_0 & \cdots & b_{2r} & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & 0 & b_0 & \cdots & b_{2r} \end{pmatrix} . \tag{11}$$

Then, the Latin squares $L_{\mathcal{F}}$ and $L_{\mathcal{G}}$ generated by $\mathcal{F}$ and $\mathcal{G}$ are orthogonal if and only if the determinant of M over $\mathbb{F}_q$ is not null.

Proof. *Denote by $z = x||y$ the concatenation of vectors x and y. We have to show that the function $\mathcal{H} : \mathbb{F}_q^{2r} \times \mathbb{F}_q^{2r} \to \mathbb{F}_q^{2r} \times \mathbb{F}_q^{2r}$, defined for all $(x, y) \in \mathbb{F}_q^{2r} \times \mathbb{F}_q^{2r}$ as*

$$\mathcal{H}(x, y) = (\mathcal{F}(z), \mathcal{G}(z)) = (\tilde{x}, \tilde{y}) \tag{12}$$

is bijective. Let us rewrite Equation (12) *as a system of two equations:*

$$\begin{cases} \mathcal{F}(z) = M_{\mathcal{F}} z^T = \tilde{x} \\ \mathcal{G}(z) = M_{\mathcal{G}} z^T = \tilde{y} \end{cases} \tag{13}$$

As M consists of the juxtaposition of $M_{\mathcal{F}}$ and $M_{\mathcal{G}}$, Equation (13) *defines a linear system in $4r$ equations and $4r$ unknowns with associated matrix M. Thus, we have that $\mathcal{H}(x, y) = Mz^T$, and $\mathcal{H}$ is bijective if and only if the determinant of M is not null.* □

Remark that matrix M in Equation (11) is a *Sylvester matrix*, and its determinant is the *resultant* of the two polynomials $p_f(X)$ and $p_g(X)$ associated to f and g respectively. The resultant of two polynomials is nonzero if and only if they are relatively prime (see [4]). Clearly, if $p_f(X)$ and $p_g(X)$ are relatively prime, then for any $t \in \mathbb{N}$ their powers $p_f(X)^t$ and $p_g(X)^t$ will be relatively prime as well. Additionally, $p_f(X)^t$ and $p_g(X)^t$ are the polynomials of the t-th iterates f^t and g^t. By Lemma 1, the linear CA $\langle 2m, r, t, f \rangle$ and $\langle 2m, r, t, g \rangle$ with maps $\mathcal{F}, \mathcal{G} : A^{2m} \to A^m$ are equivalent to the linear CA $\langle 2m, rt, 1, f^t \rangle$ and $\langle 2m, rt, 1, g^t \rangle$ with maps $\mathcal{F}_t, \mathcal{G}_t : A^{2m} \to A^m$ for any multiple $m \in \mathbb{N}$ of $2r$. We thus have the following result:

Theorem 1. *Let $f, g : \mathbb{F}_q^{2r+1} \to \mathbb{F}_q$ be linear bipermutive rules of radius $r \in \mathbb{N}$. Then, for any $t \in \mathbb{N}$ and $m = 2rt$, the squares $L_{\mathcal{F}}$ and $L_{\mathcal{G}}$ of order q^m respectively associated to the linear CA $\langle 2m, r, t, f\rangle$ $\mathcal{F} : \mathbb{F}_q^{2m} \to \mathbb{F}_q^m$ and the linear CA $\langle 2m, r, t, g\rangle$ $\mathcal{G} : \mathbb{F}_q^{2m} \to \mathbb{F}_q^m$ are orthogonal if and only if the polynomials $p_f(X)$ and $p_g(X)$ are relatively prime.*

4 Conclusions and Perspectives

By Theorem 1, one can generate a set of n MOLS of order q^m through linear CA of radius r by finding n pairwise relatively prime polynomials of degree $2r$, where $2r|m$. Random generation would work quite well in practice: as mentioned in [2], the probability that n randomly selected polynomials over $\mathbb{F}_q$ are relatively prime is $1 - \frac{1}{q^{n-1}}$.

Given the equivalence between MOLS and OA, Theorem 1 also gives some additional insights on how to design a CA-based secret sharing scheme with threshold $t = 2$. In particular, suppose that the secret S is a vector of $\mathbb{F}_q^m$, and there are n players $P_1, \cdots, P_n$. The dealer picks n relatively prime polynomials of degree $2r$, and builds the corresponding linear rules $f_1, \cdots, f_n$ of radius r. Successively, the dealer concatenates the secret S with a random vector $R \in \mathbb{F}_q^m$, thus obtaining a configuration $C \in \mathbb{F}_q^{2m}$ of length $2m$. Adopting the point of view of OA, this step corresponds to the phase where the dealer chooses one of the rows of the array whose first component is the secret. In order to determine the remaining components of the row, and thus the shares to distribute to the players, for all $i \in \{1, \cdots, n\}$ the dealer evolves the CA $\mathcal{F}_i$ with rule f_i starting from configuration C. The value $B_i = \mathcal{F}_i(C)$ constitutes the share of player P_i.

However, observe that the recovery phase for two players P_i, P_j respectively holding shares B_i and B_j is not straightforward. As a matter of fact, even by assuming that P_i and P_j know the local rules f_i and f_j (a reasonable assumption, since the OA is usually considered to be public), there is no obvious way to recompute preimage C by iterating the two CA backwards. We plan to investigate this issue in future research.

References

1. Chaum, D., Crépeau, C., Damgård, I.: Multiparty Unconditionally Secure Protocols. In: Proceedings of STOC 1988, pp. 11–19. ACM (1988)
2. Hou, X.-D., Mullen, G.D.: Number of irreducible polynomials and pairs of relatively prime polynomials in several variables over finite fields. Finite Fields Th. App. 15(3):304–331 (2009)
3. Ito, M., Osato, N., Nasu, M.: Linear Cellular Automata over Z_m. J. Comput. Syst. Sci. 27(1):125–140 (1983)
4. Lidl, R., Niederreiter, H.: Introduction to finite fields and their applications. Cambridge University Press, Cambridge (1994)
5. Mariot, L., Leporati, A.: Sharing Secrets by Computing Preimages of Bipermutive Cellular Automata. In: Proceedings of ACRI 2014. LNCS vol. 8751, pp. 417–426. Springer (2014)
6. Shamir, A.: How to share a secret. Commun. ACM 22(11):612–613 (1979)
7. Stinson, D.R.: Combinatorial Designs: Constructions and Analysis. Springer (2004)
8. Tassa, T.: Generalized oblivious transfer by secret sharing. Des. Codes Cryptogr. 58(1):11–21 (2011)