Secret Sharing through Cellular Automata

Luca Mariot[1,2]

[1] Dipartimento di Informatica, Sistemistica e Comunicazione (DISCo)
Università degli Studi Milano - Bicocca

luca.mariot@disco.unimib.it

[2] Laboratoire d'Informatique, Signaux et Systèmes de Sophia Antipolis (I3S)
Université Nice Sophia Antipolis

mariot@i3s.unice.fr

May 24, 2016

One-Dimensional Cellular Automata (CA)

Definition

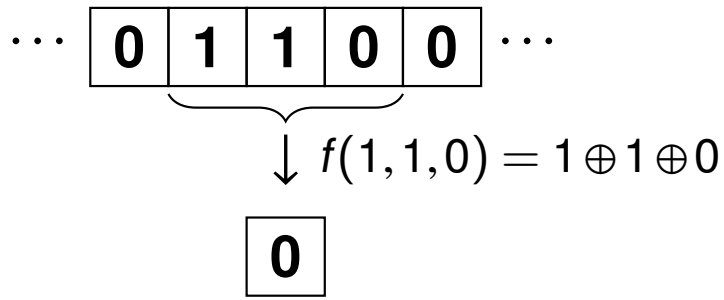
One-dimensional cellular automaton: triple $\langle n, r, f \rangle$ where $n \in \mathbb{N}$ is the number of cells arranged on a one-dimensional array, $r \in \mathbb{N}$ is the radius and $f : \{0,1\}^{2r+1} \rightarrow \{0,1\}$ is the local rule.

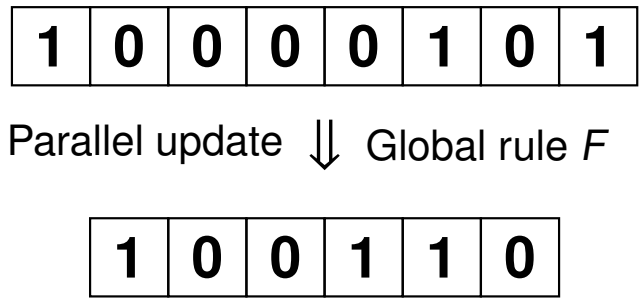
One-Dimensional Cellular Automata (CA)

Definition

One-dimensional cellular automaton: triple $\langle n, r, f \rangle$ where $n \in \mathbb{N}$ is the number of cells arranged on a one-dimensional array, $r \in \mathbb{N}$ is the radius and $f : \{0,1\}^{2r+1} \to \{0,1\}$ is the local rule.

Example: $n = 8$, $r = 1$, $f(s_{i-1}, s_i, s_{i+1}) = s_{i-1} \oplus s_i \oplus s_{i+1}$ (Rule 150)



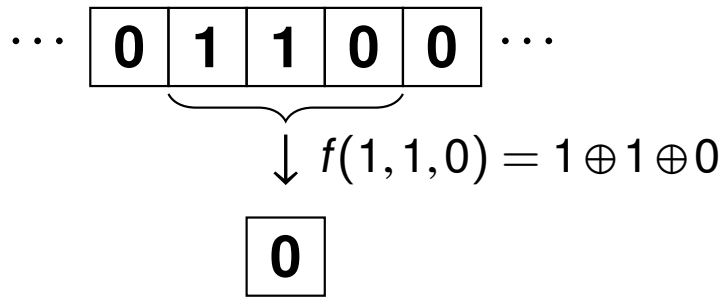


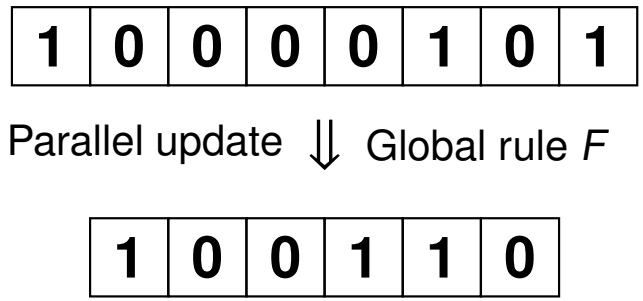
One-Dimensional Cellular Automata (CA)

Definition

One-dimensional cellular automaton: triple $\langle n, r, f \rangle$ where $n \in \mathbb{N}$ is the number of cells arranged on a one-dimensional array, $r \in \mathbb{N}$ is the radius and $f : \{0,1\}^{2r+1} \to \{0,1\}$ is the local rule.

Example: $n = 8$, $r = 1$, $f(s_{i-1}, s_i, s_{i+1}) = s_{i-1} \oplus s_i \oplus s_{i+1}$ (Rule 150)





Remark: No boundary conditions ⇒ The array "shrinks"

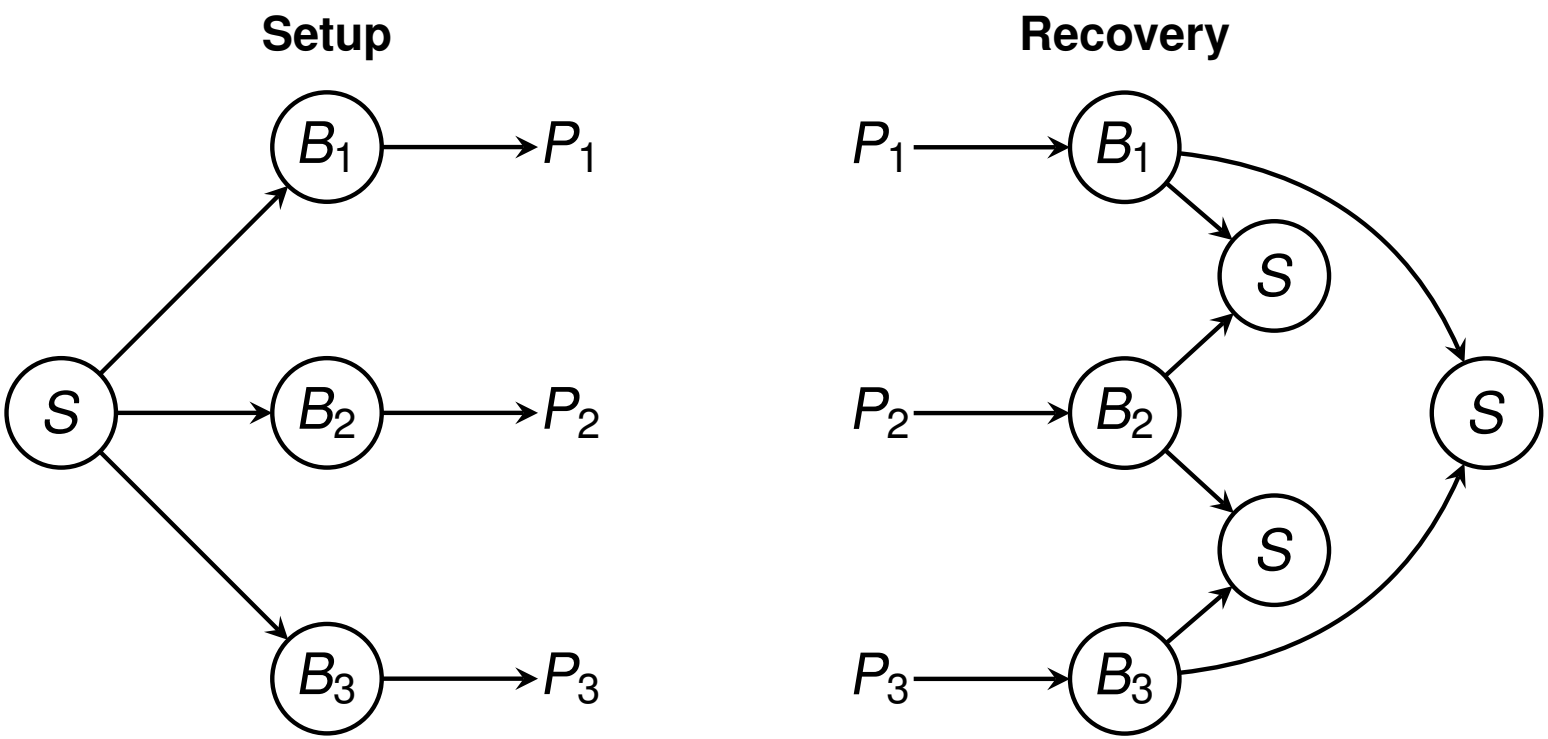
Secret Sharing Schemes (SSS)

- Secret sharing scheme: a procedure enabling a dealer to share a secret S among a set $\mathcal{P}$ of n players
- In (k, n) threshold schemes, at least k players out of n are required to recover S

Secret Sharing Schemes (SSS)

- Secret sharing scheme: a procedure enabling a dealer to share a secret S among a set $\mathcal{P}$ of n players
- In (k, n) threshold schemes, at least k players out of n are required to recover S

Example: $(2,3)$–scheme



Bipermutive Rules

- Rule $f : \{0,1\}^{2r+1} \rightarrow \{0,1\}$ is called bipermutive if there exists $g : \{0,1\}^{2r-1} \rightarrow \{0,1\}$ such that:

$$f(x_1, x_2, \cdots, x_{2r}, x_{2r+1}) = x_1 \oplus g(x_2, \cdots, x_{2r}) \oplus x_{2r+1}$$

Bipermutive Rules

- Rule $f : \{0,1\}^{2r+1} \to \{0,1\}$ is called bipermutive if there exists $g : \{0,1\}^{2r-1} \to \{0,1\}$ such that:

$$f(x_1, x_2, \cdots, x_{2r}, x_{2r+1}) = x_1 \oplus g(x_2, \cdots, x_{2r}) \oplus x_{2r+1}$$

- A preimage $p \in \{0,1\}^{m+2r}$ of $c \in \{0,1\}^m$ is uniquely determined by a block of $2r$ cells

Bipermutive Rules

- Rule $f : \{0,1\}^{2r+1} \to \{0,1\}$ is called bipermutive if there exists $g : \{0,1\}^{2r-1} \to \{0,1\}$ such that:

$$f(x_1, x_2, \cdots, x_{2r}, x_{2r+1}) = x_1 \oplus g(x_2, \cdots, x_{2r}) \oplus x_{2r+1}$$

- A preimage $p \in \{0,1\}^{m+2r}$ of $c \in \{0,1\}^m$ is uniquely determined by a block of $2r$ cells

$p =$	?	?	?	?	0	1	?	?
$c =$		1	0	0	1	1	0	

(a) Initialization

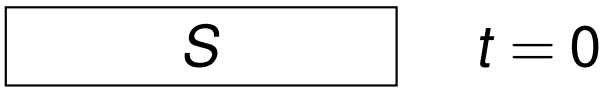
$p =$	1	0	0	0	0	1	0	1
$c =$		1	0	0	1	1	0	

(b) Complete preimage

Figure : Example with bipermutive rule 150

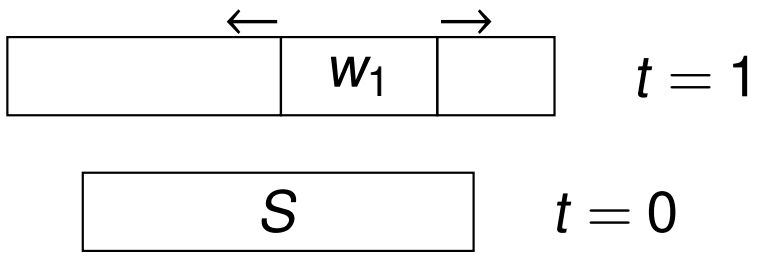
Basic (n, n) Secret Sharing Scheme - Setup Phase

1. The *dealer D* sets the secret S as an m-bit configuration of a CA, and selects a bipermutive rule of radius r such that $2r|m$



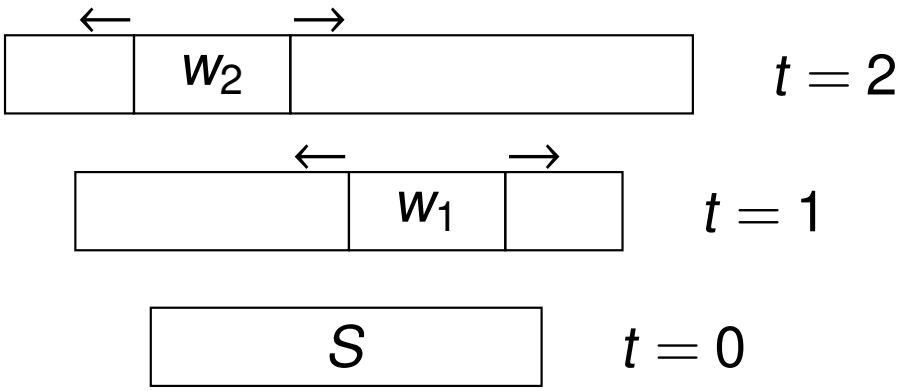
Basic (n, n) Secret Sharing Scheme - Setup Phase

2. D evolves the CA backwards for $T = m(n-1)/2r$ iterations, randomly choosing an initial $2r$-bit block at each step



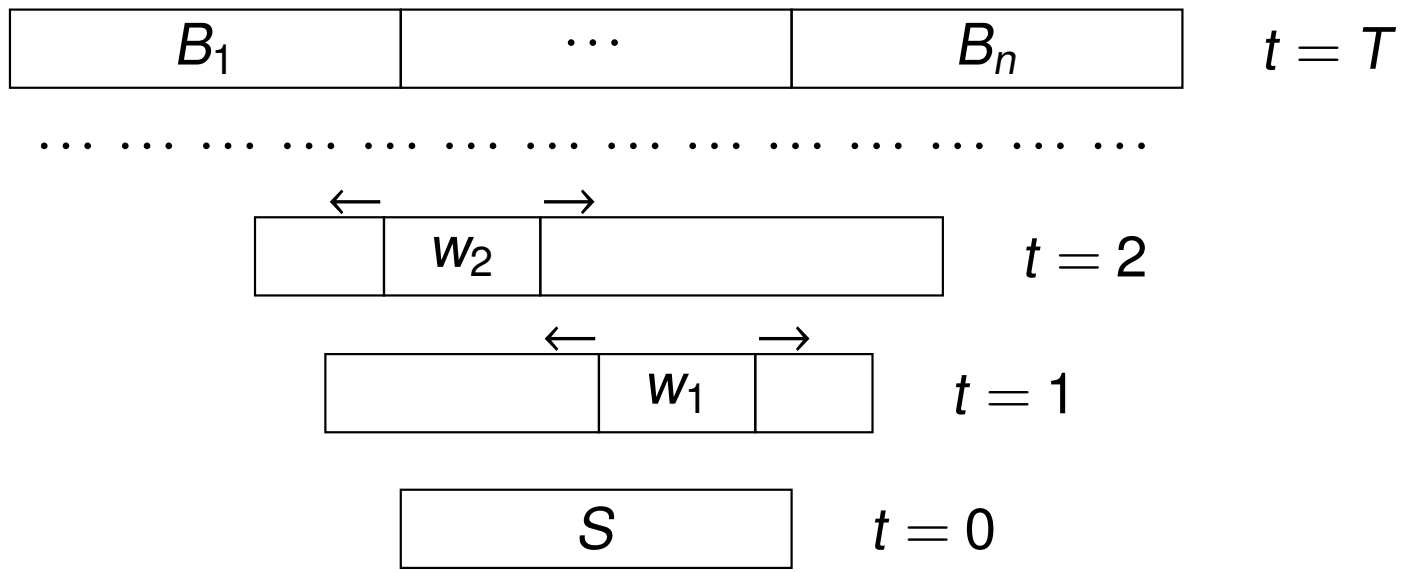
Basic (n, n) Secret Sharing Scheme - Setup Phase

2. D evolves the CA backwards for $T = m(n-1)/2r$ iterations, randomly choosing an initial $2r$-bit block at each step



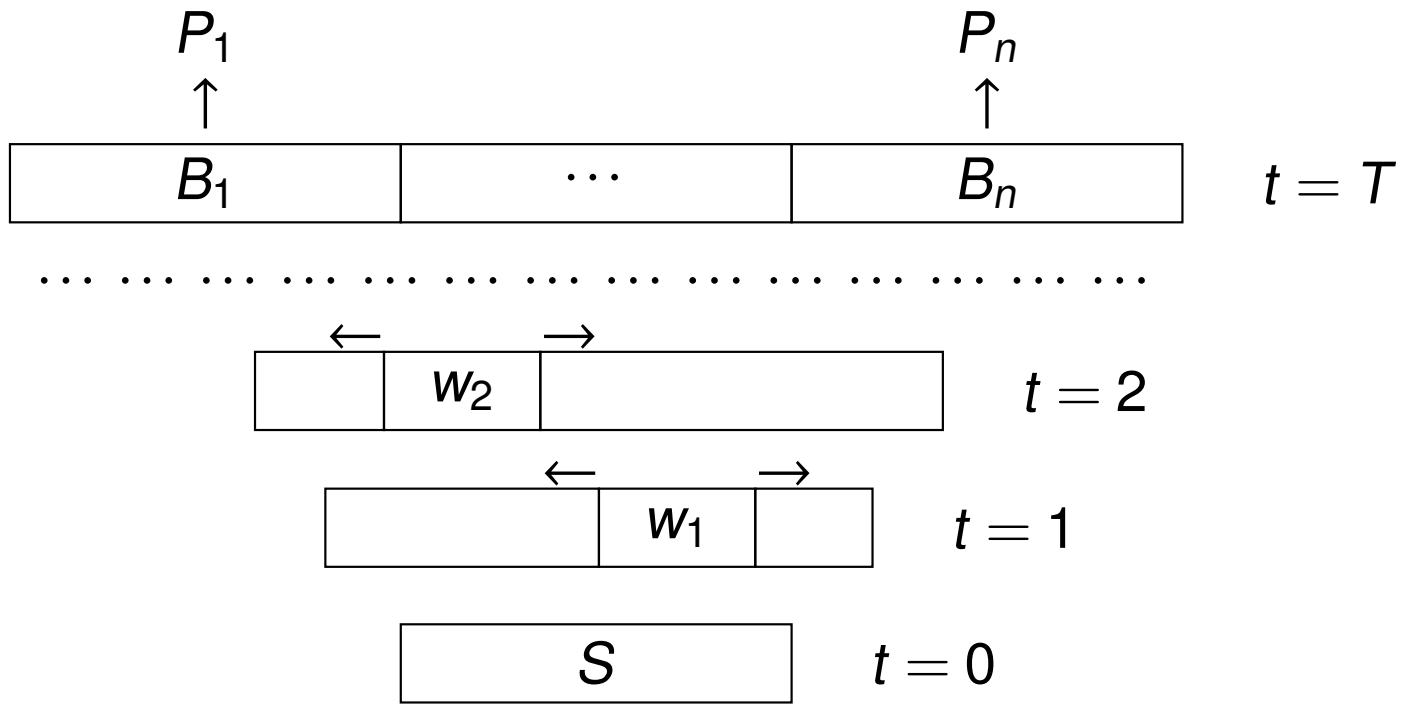
Basic (n, n) Secret Sharing Scheme - Setup Phase

3. After $T = m(n-1)/2r$ iterations, the dealer splits the resulting preimage in n blocks of m bits



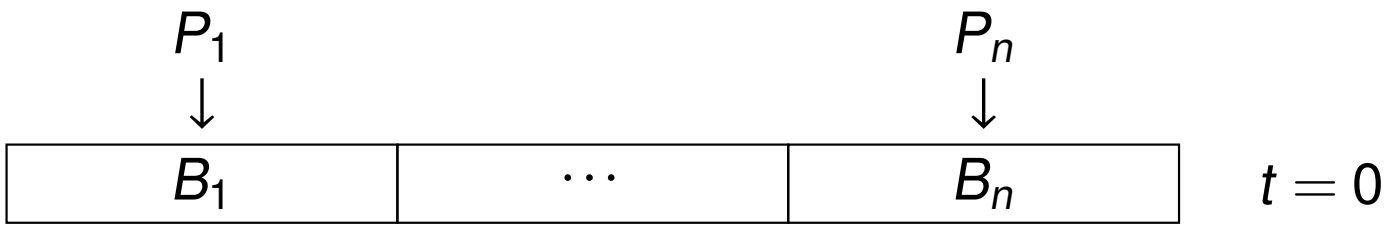
Basic (n, n) Secret Sharing Scheme - Setup Phase

4. D securely sends one block to each player and publishes the bipermutive rule used



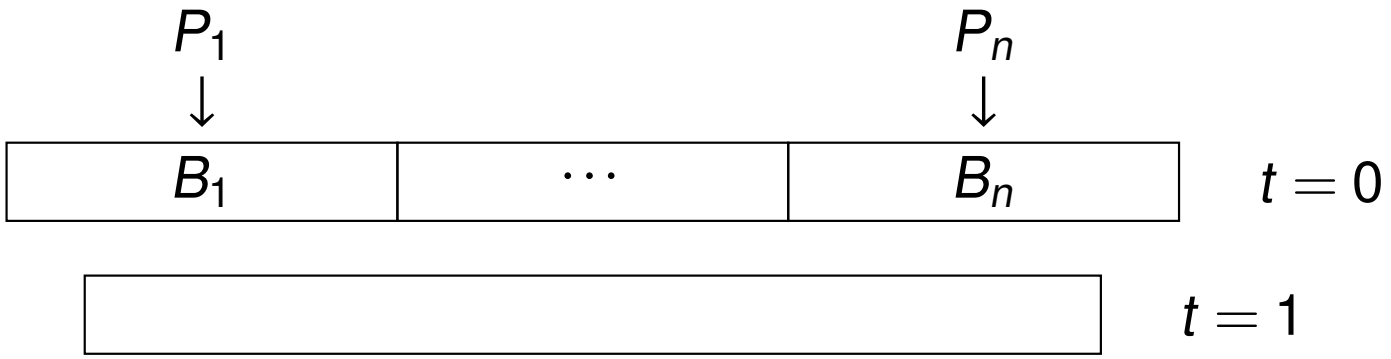
Basic (n, n) Secret Sharing Scheme - Recovery Phase

1. The n players pool their shares in the correct order to get the complete preimage of the CA



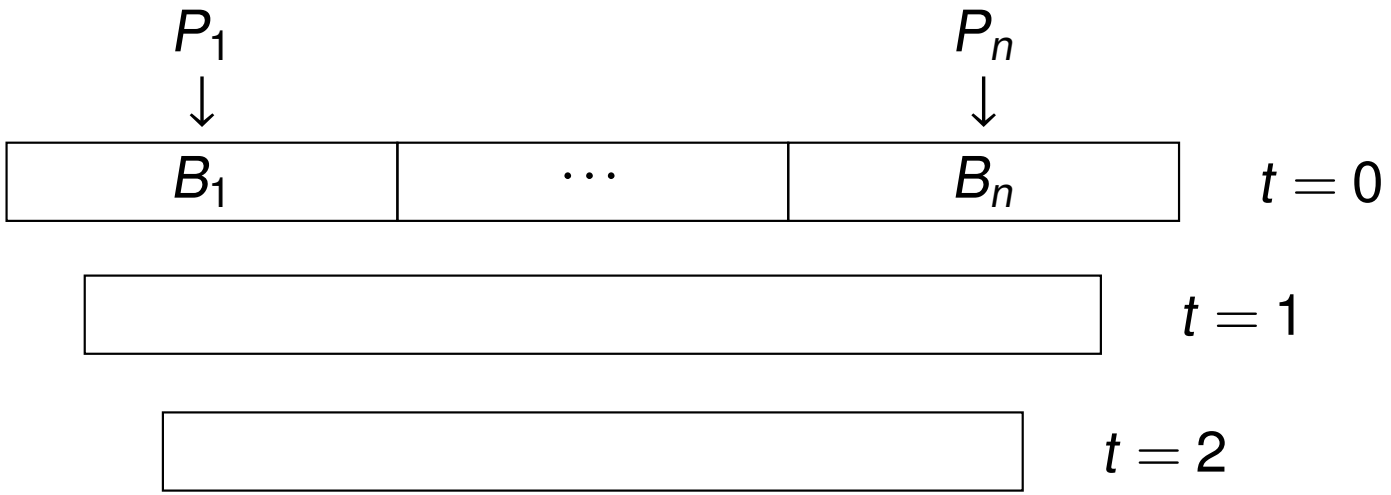
Basic (n, n) Secret Sharing Scheme - Recovery Phase

2. The players evolve the CA forward, using the local rule published by the dealer



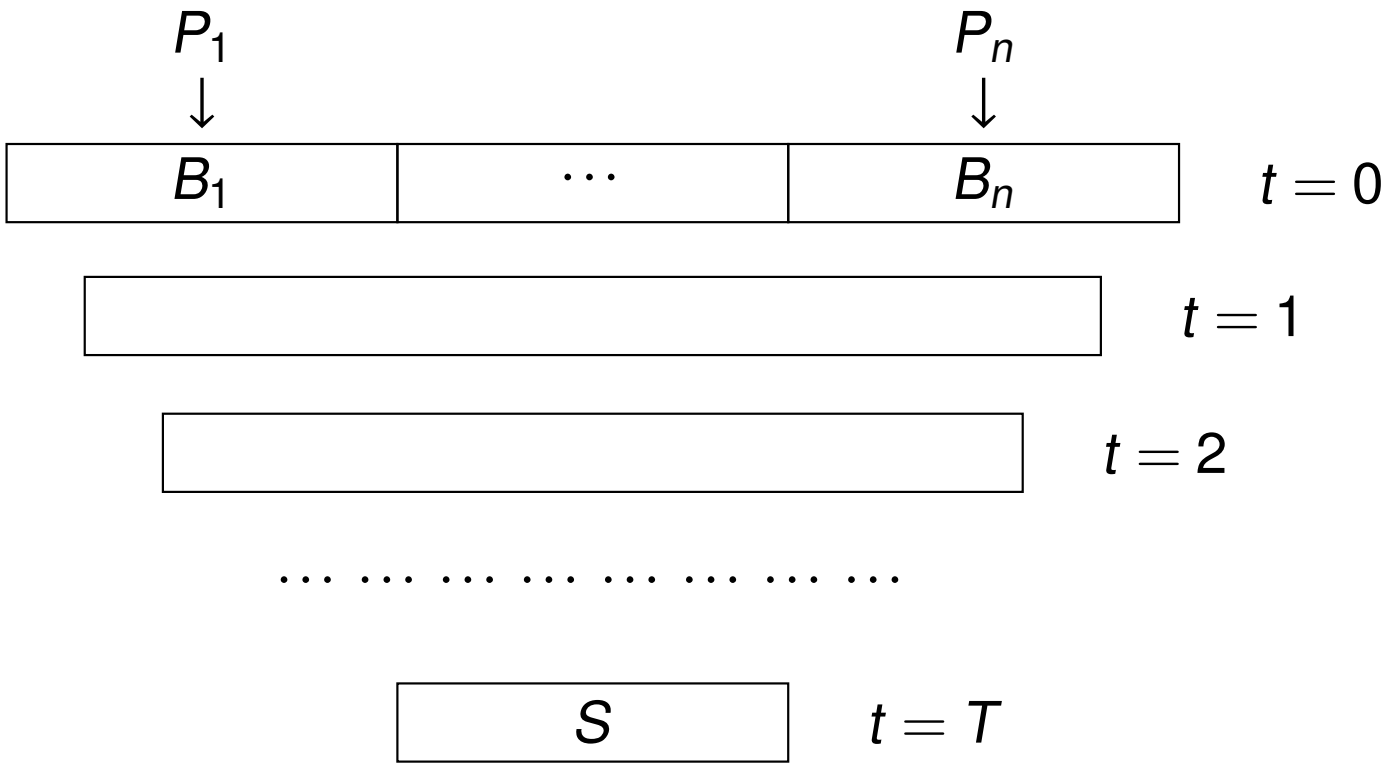
Basic (n, n) Secret Sharing Scheme - Recovery Phase

2. The players evolve the CA forward, using the local rule published by the dealer



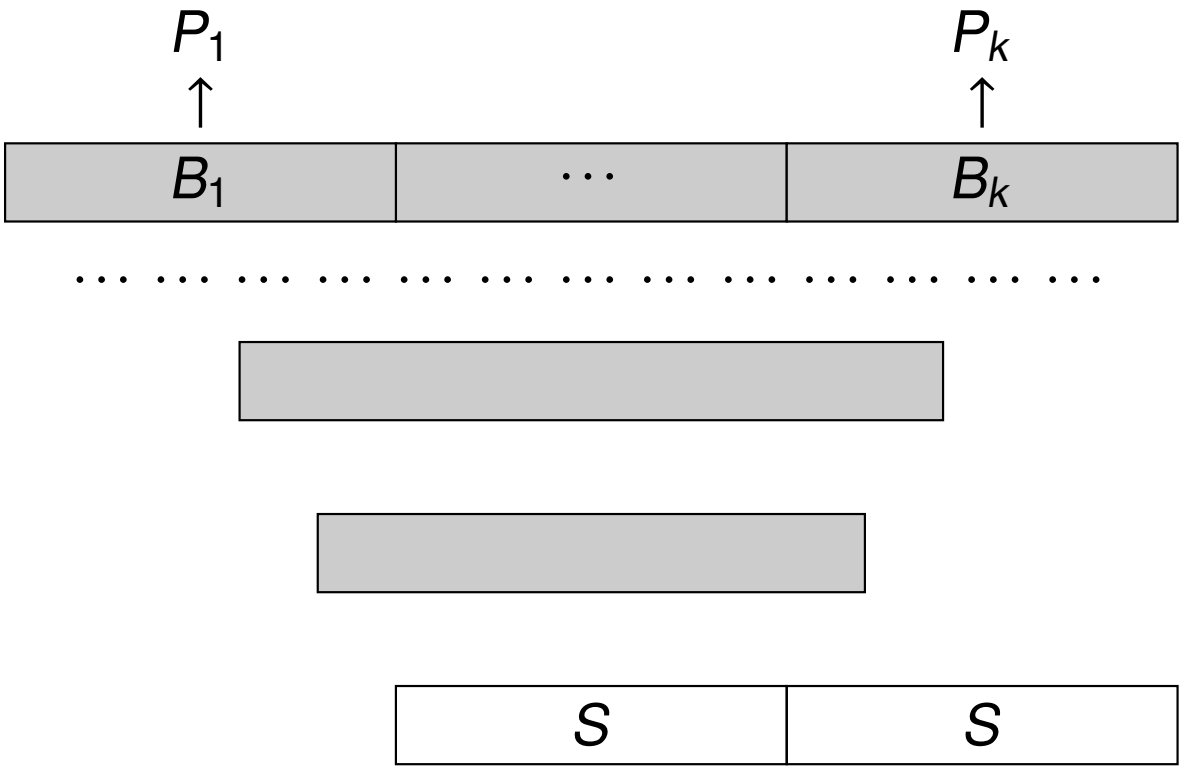
Basic (n, n) Secret Sharing Scheme - Recovery Phase

3. The configuration obtained after $T = m(n-1)/2r$ iterations is the secret S.



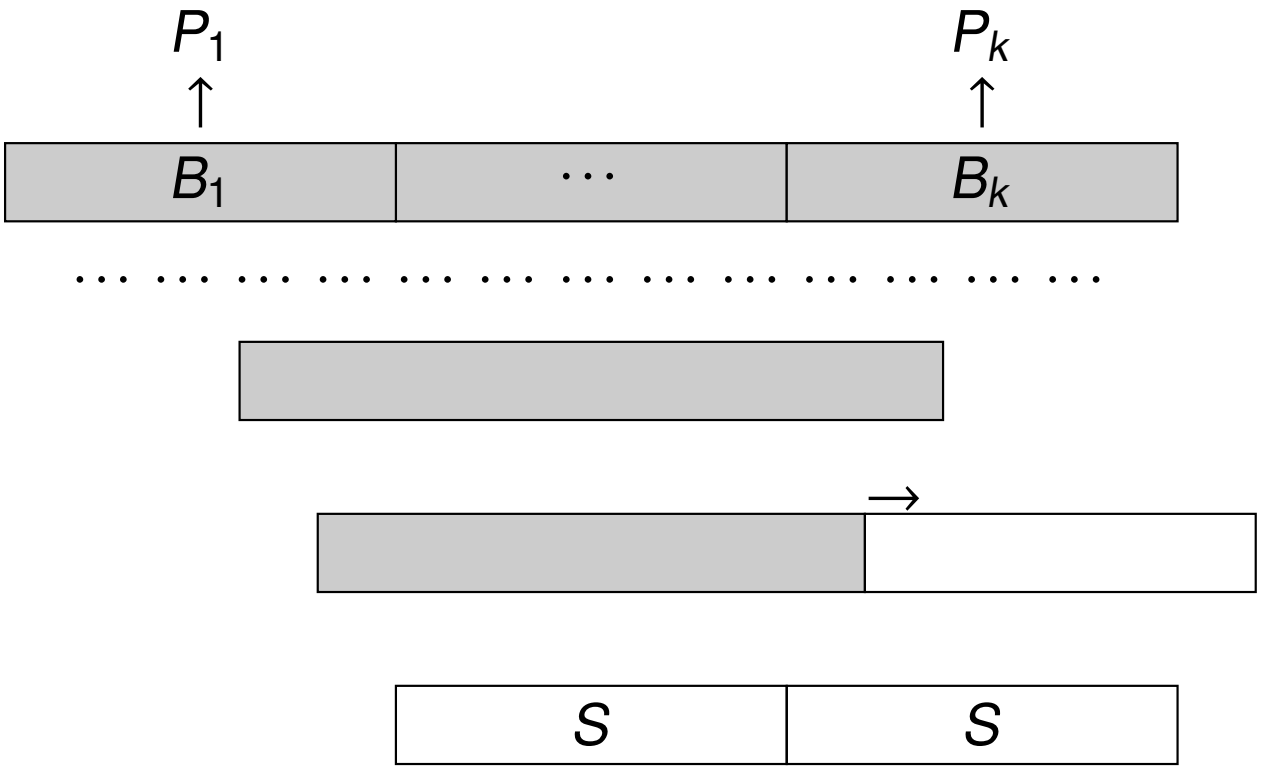
Secret Juxtaposition (1/4)

1. Append a copy of the secret S to the right of the final CA image



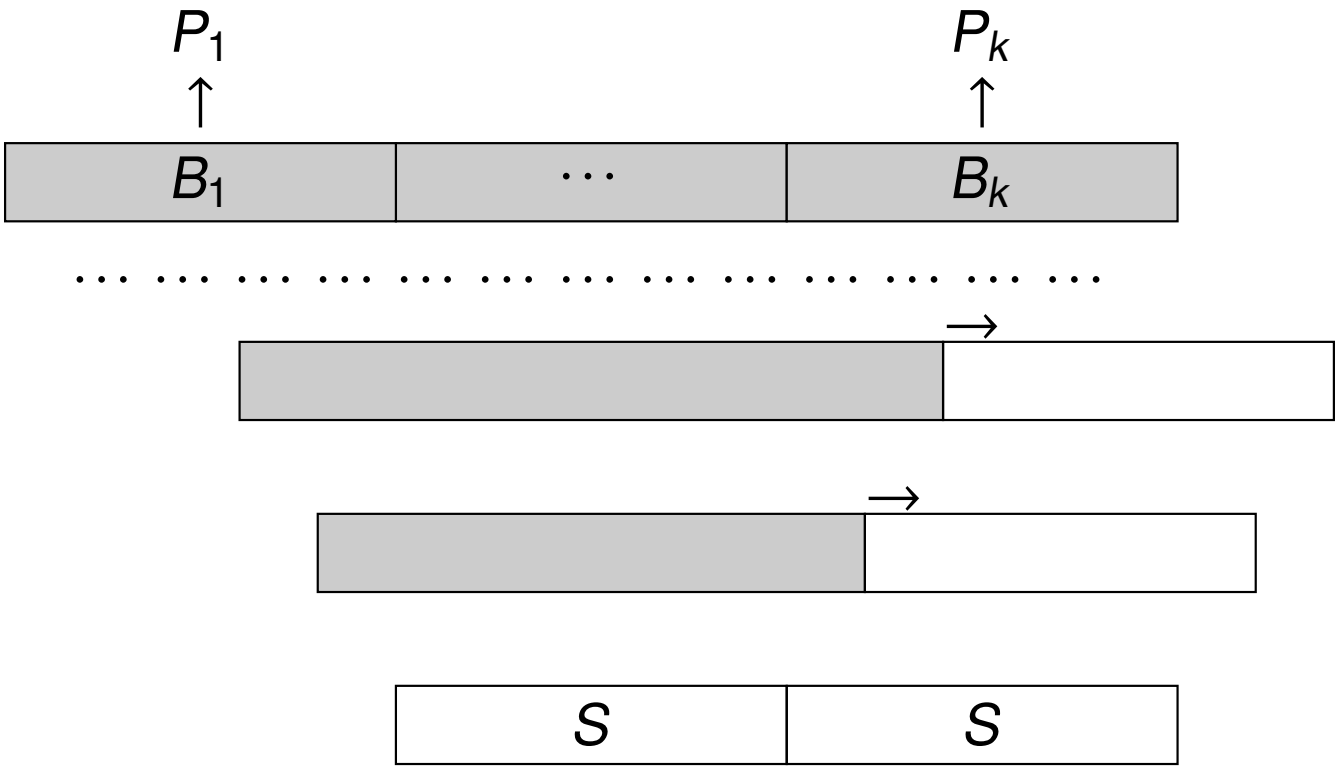
Secret Juxtaposition (2/4)

2. Update the preimages by completing them rightwards (note that it is not necessary to pick extra random bits)



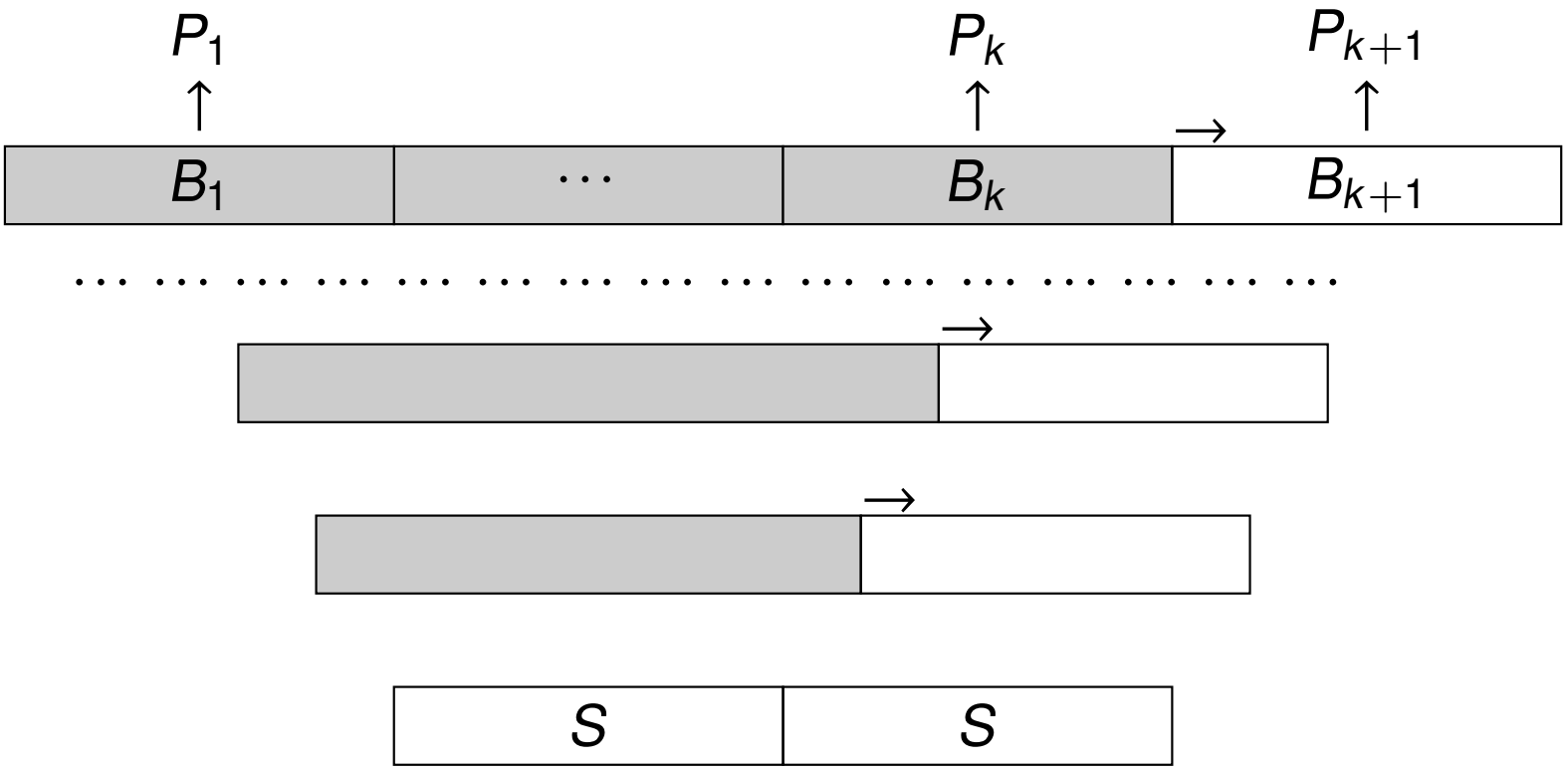
Secret Juxtaposition (3/4)

2. Update the preimages by completing them rightwards (note that it is not necessary to pick extra random bits)



Secret Juxtaposition (4/4)

3. The last preimage contains an additional block for the new player. The sets $\{P_1, \cdots, P_k\}$ and $\{P_2, \cdots, P_{k+1}\}$ can recover S

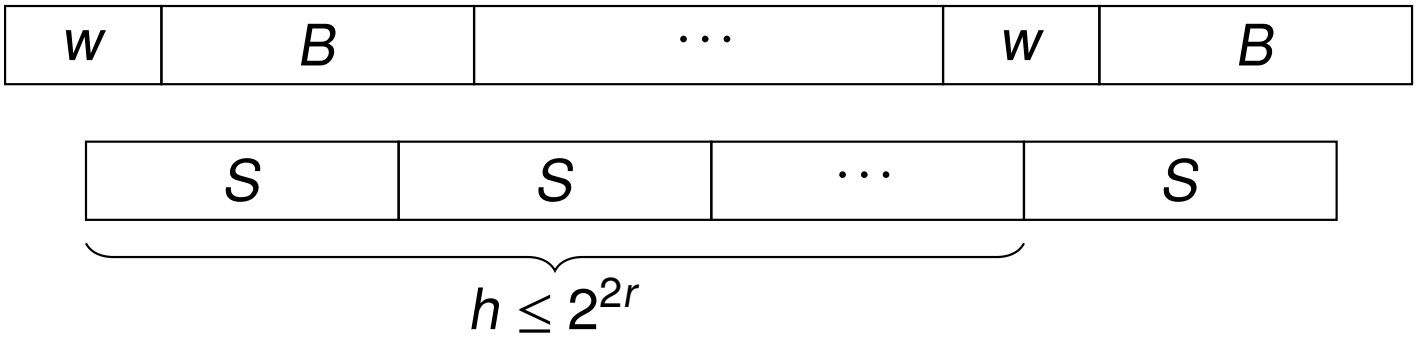


Access Structure of the Scheme

- (k, n)-sequential threshold: at least k consecutive shares are necessary to recover the secret
- By continuing to append copies of the secret, the shares will eventually repeat $\Rightarrow$ cyclic access structure

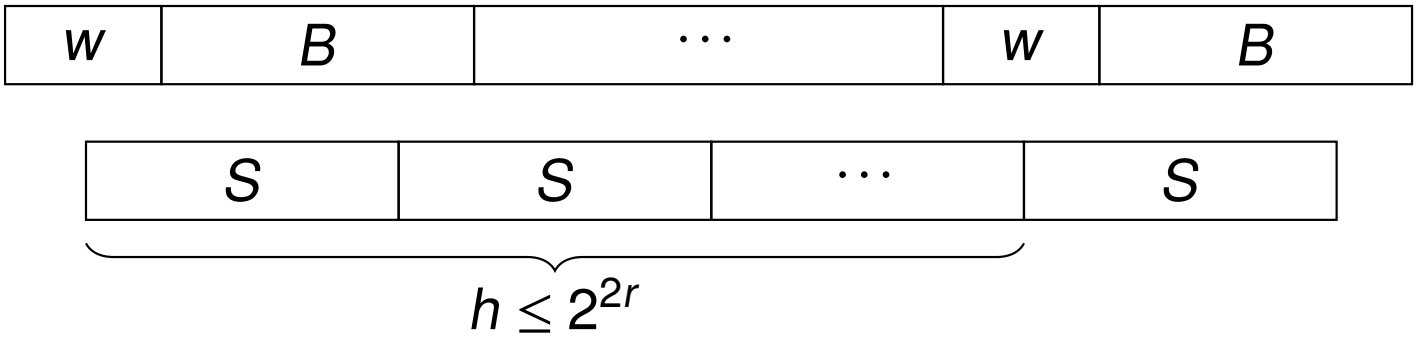
Access Structure of the Scheme

- (k, n)-sequential threshold: at least k consecutive shares are necessary to recover the secret
- By continuing to append copies of the secret, the shares will eventually repeat $\Rightarrow$ cyclic access structure



Access Structure of the Scheme

- (k, n)-sequential threshold: at least k consecutive shares are necessary to recover the secret
- By continuing to append copies of the secret, the shares will eventually repeat $\Rightarrow$ cyclic access structure



What about real threshold schemes with CA?

A Different Angle: Latin Squares

Definition

A *Latin square* of order N is a $N \times N$ matrix L from such that every row and every column are permutations of $[N] = \{1, \cdots, N\}$

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

Orthogonal Latin Squares

Definition

Two Latin squares L_1 and L_2 of order n are *orthogonal* if their superposition yields all the pairs $(x, y) \in [N] \times [N]$.

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

(a) L_1

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

(b) L_2

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

(c) (L_1, L_2)

A set of n pairwise orthogonal Latin squares is denoted as n-MOLS

$(2, n)$-Schemes through n-MOLS

1. The dealer D chooses a row $S \in \{1, \cdots, N\}$ as the secret

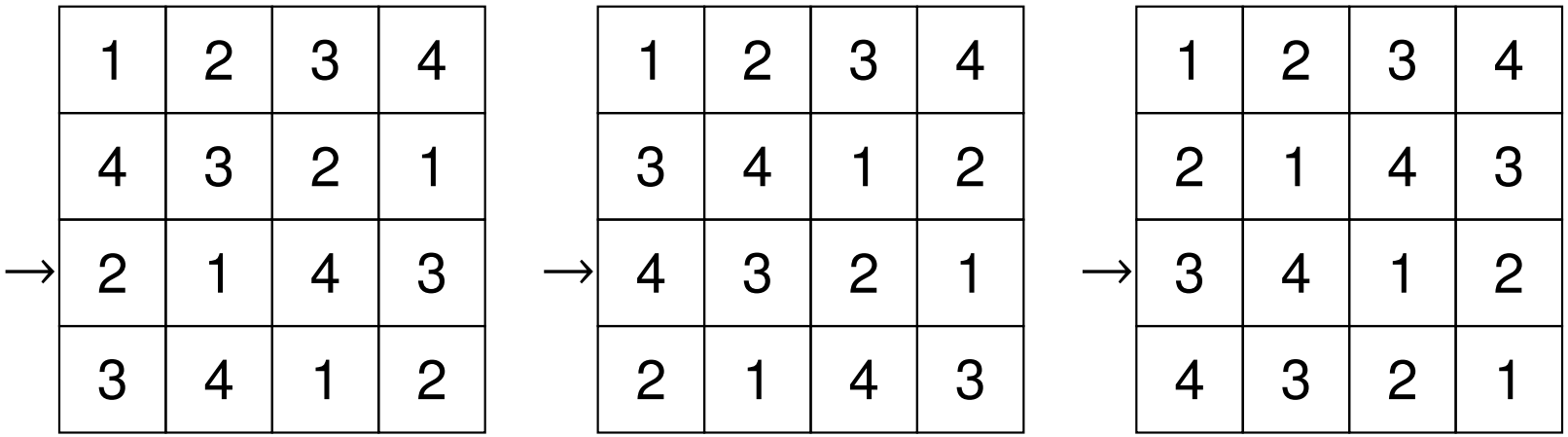
1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

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

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

$(2, n)$-Schemes through n-MOLS

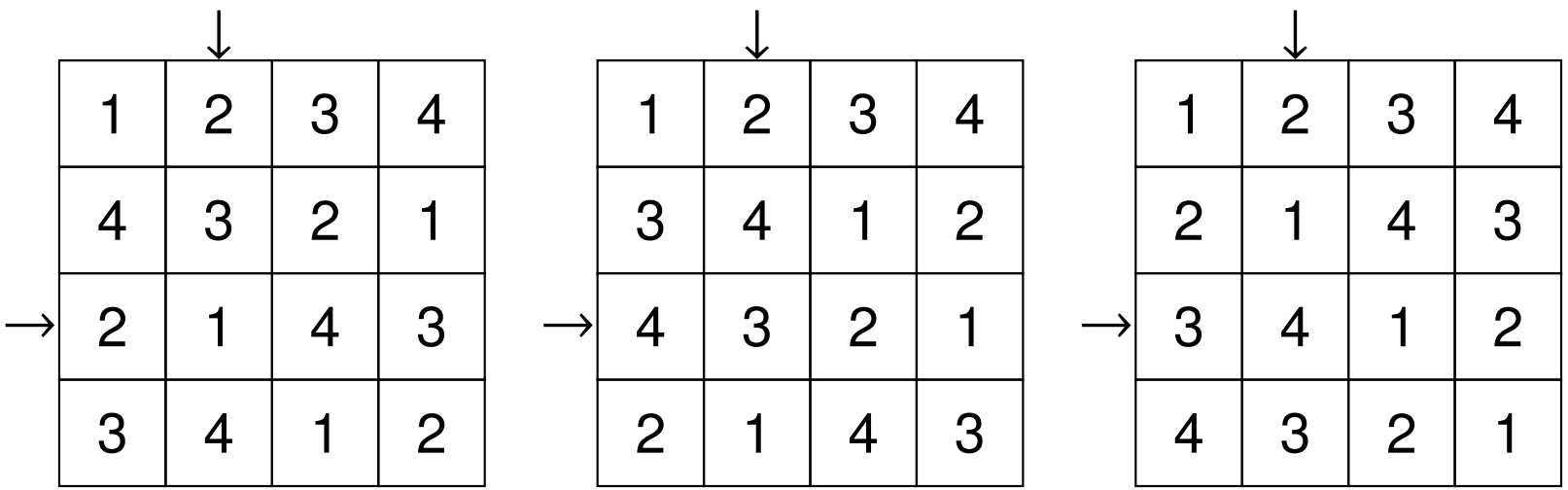
1. The dealer D chooses a row $S \in \{1, \cdots, N\}$ as the secret



Example: $(2,3)$-scheme, $S = 3$

$(2, n)$-Schemes through n-MOLS

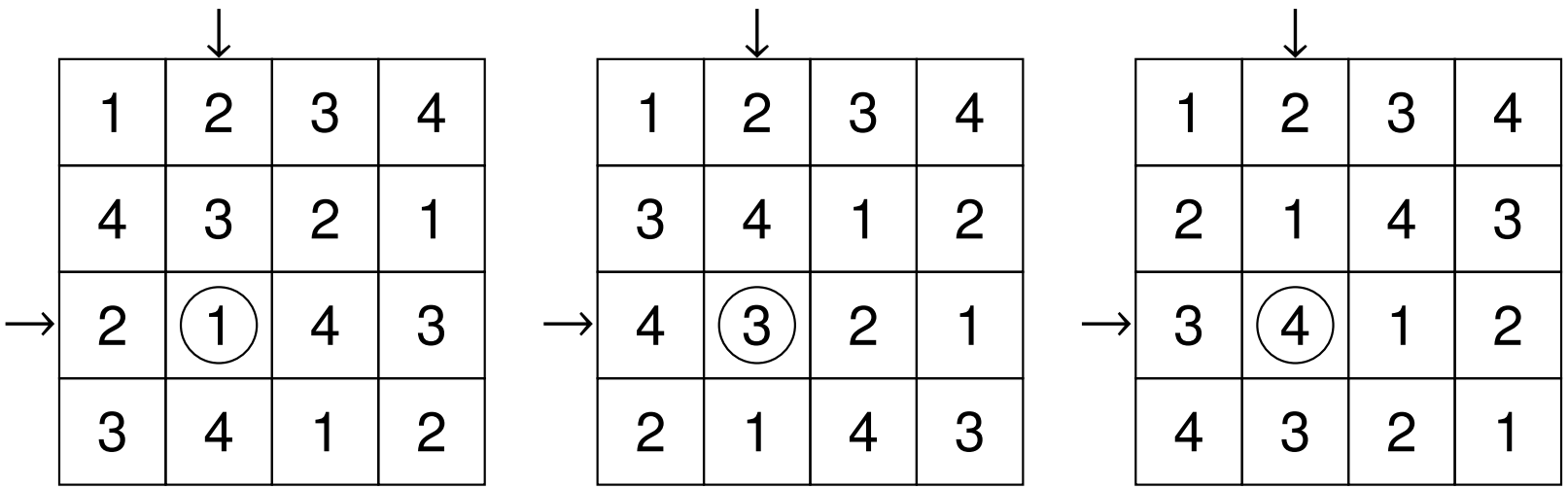
2. D randomly selects a column $j \in \{1, \cdots, N\}$



Example: $S = 3$, $j = 2$

$(2,n)$-Schemes through n-MOLS

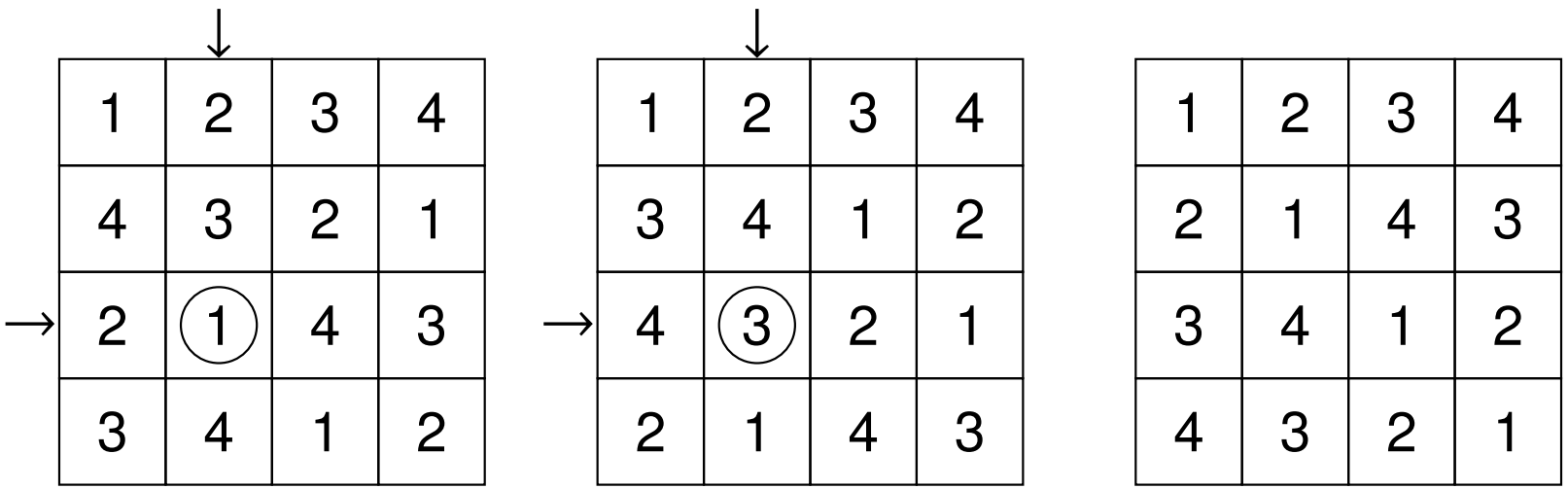
3. The value of $L_i(S,j)$ for $i \in [n]$ is the share of P_i



Example: $(2,3)$-scheme, $S = 3$, $j = 2$, $B_1 = 1$, $B_2 = 3$, $B_3 = 4$

$(2,n)$-Schemes through n-MOLS

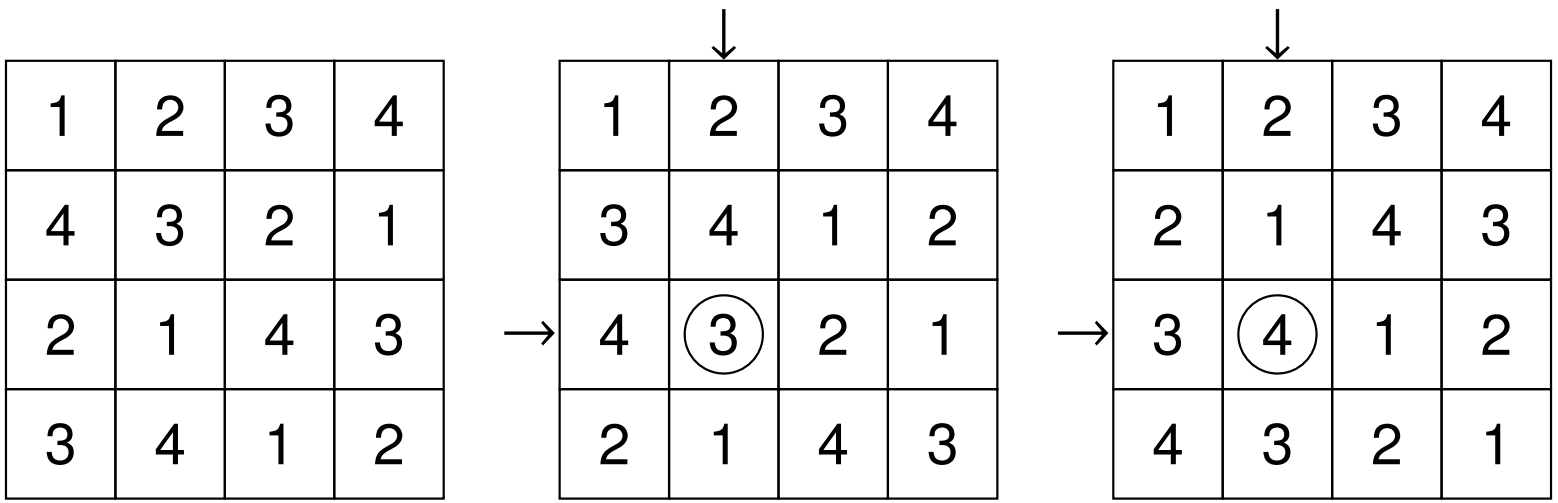
4. Since L_i, L_k are orthogonal, (B_i, B_k) uniquely identify (S, j)



Example: $(2,3)$-scheme, $B_1 = 1$, $B_2 = 3 \Rightarrow (3,2)$

$(2,n)$-Schemes through n-MOLS

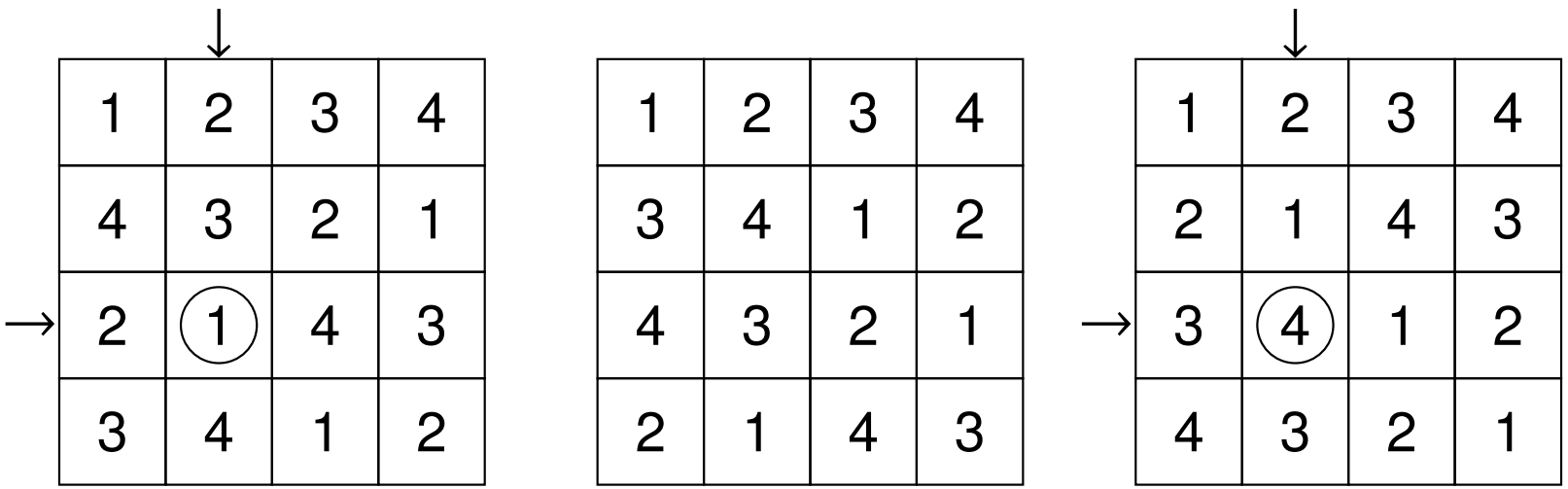
4. Since L_i, L_k are orthogonal, (B_i, B_k) uniquely identify (S, j)



Example: $(2,3)$-scheme, $B_2 = 3$, $B_3 = 4 \Rightarrow (3,2)$

$(2,n)$-Schemes through n-MOLS

4. Since L_i, L_k are orthogonal, (B_i, B_k) uniquely identify (S, j)



Example: $(2,3)$-scheme, $B_1 = 1$, $B_3 = 4 \Rightarrow (3,2)$

Latin Squares through Bipermutive CA

- Problem reduction: determine which CA induce orthogonal Latin squares

Lemma

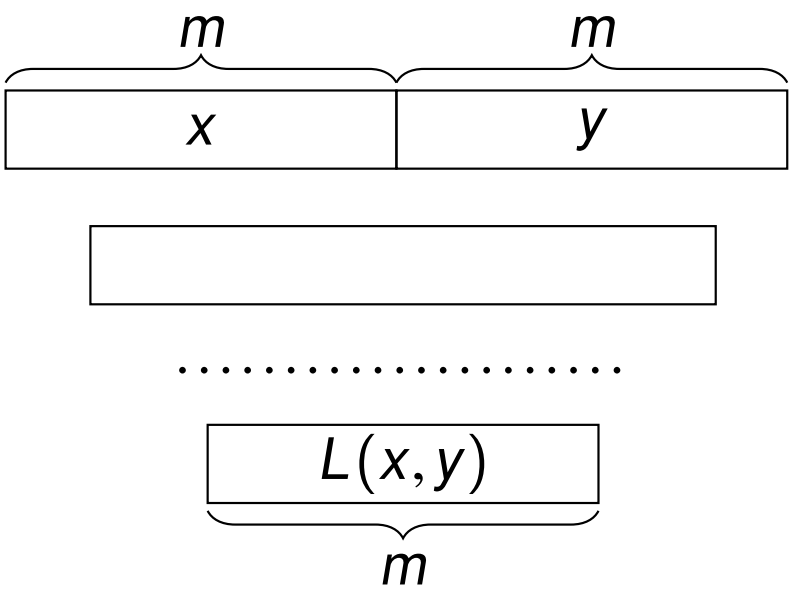
Let $\langle 2m, r, t, f \rangle$ be a bipermutive CA with $2r|m$. Then, the CA generates a Latin square of order $N = 2^m$

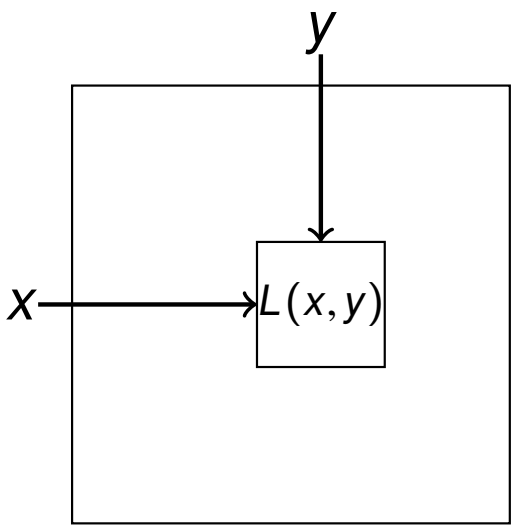
Latin Squares through Bipermutive CA

- Problem reduction: determine which CA induce orthogonal Latin squares

Lemma

Let $\langle 2m, r, t, f \rangle$ be a bipermutive CA with $2r|m$. Then, the CA generates a Latin square of order $N = 2^m$



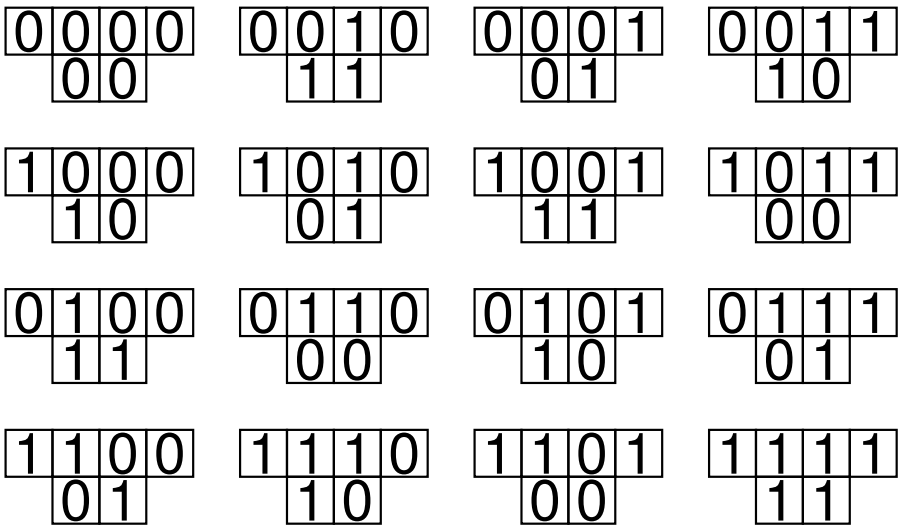


Latin Squares through Bipermutive CA

- Problem reduction: determine which CA induce orthogonal Latin squares

Lemma

Let $\langle 2m, r, t, f \rangle$ be a bipermutive CA with $2r|m$. Then, the CA generates a Latin square of order $N = 2^m$



(a) Rule 150

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

(b) L_{150}

$$00 \mapsto 1, 10 \mapsto 2, 01 \mapsto 3, 11 \mapsto 4$$

Linear CA

- Local rule: linear combination of the neighborhood cells

$$f(x_0, \cdots, x_{2r}) = a_0 x_0 \oplus \cdots \oplus a_{2r} x_{2r} \ , \ a_i \in \mathbb{F}_2$$

Linear CA

- Local rule: linear combination of the neighborhood cells

$$f(x_0, \cdots, x_{2r}) = a_0 x_0 \oplus \cdots \oplus a_{2r} x_{2r} \ , \ a_i \in \mathbb{F}_2$$

- Associated polynomial:

$$f \mapsto P_f(X) = a_0 + a_1 X + \cdots + a_{2r} X^{2r}$$

Linear CA

- Local rule: linear combination of the neighborhood cells

$$f(x_0, \cdots, x_{2r}) = a_0 x_0 \oplus \cdots \oplus a_{2r} x_{2r} \ , \ a_i \in \mathbb{F}_2$$

- Associated polynomial:

$$f \mapsto P_f(X) = a_0 + a_1 X + \cdots + a_{2r} X^{2r}$$

- Global rule: $m \times (m + 2r)$ $2r$-diagonal transition matrix

$$M_F = \begin{pmatrix} a_0 & \cdots & a_{2r} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_0 & \cdots & a_{2r} & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & a_0 & \cdots & a_{2r} \end{pmatrix}$$

$$x = (x_0, \cdots, x_{n-1}) \mapsto M_F x^\top$$

Linear CA

- Local rule: linear combination of the neighborhood cells

$$f(x_0, \cdots, x_{2r}) = a_0 x_0 \oplus \cdots \oplus a_{2r} x_{2r} \ , \ a_i \in \mathbb{F}_2$$

- Associated polynomial:

$$f \mapsto P_f(X) = a_0 + a_1 X + \cdots + a_{2r} X^{2r}$$

- Global rule: $m \times (m + 2r)$ $2r$-diagonal transition matrix

$$M_F = \begin{pmatrix} a_0 & \cdots & a_{2r} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_0 & \cdots & a_{2r} & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & a_0 & \cdots & a_{2r} \end{pmatrix}$$

$$x = (x_0, \cdots, x_{n-1}) \mapsto M_F x^\top$$

- $a_0, a_{2r} \neq 0 \Rightarrow f$ bipermutive

Orthogonal Latin Squares by Linear CA

Theorem

The Latin squares induced by $\langle 2m, r, t, f \rangle$ *and* $\langle 2m, r, t, g \rangle$ *are orthogonal if and only if* $gcd(P_f(X), P_g(X)) = 1$

Orthogonal Latin Squares by Linear CA

Theorem

The Latin squares induced by $\langle 2m, r, t, f\rangle$ and $\langle 2m, r, t, g\rangle$ are orthogonal if and only if $gcd(P_f(X), P_g(X)) = 1$

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

(a) Rule 150

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

(b) 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) Superposition

Figure : $P_{150}(X) = 1 + X + X^2$, $P_{90}(X) = 1 + X^2$ (coprime)

Conclusions and Perspectives

- Recap:
  - A single bipermutive CA can be used to implement a (k, n) sequential threshold scheme
  - A set of n linear CA with coprime rules gives rise to a set of n MOLS (and thus to a $(2, n)$-threshold scheme)
- Future developments:
  - Count (and build!) pairs of coprime polynomials
  - Generalise to higher threshold (using orthogonal hypercubes)

References

- Beimel, A.: Secret-Sharing Schemes: A Survey. In: Proceedings of IWCC 2011. LNCS vol. 6639, pp. 11–46. Springer (2011)
- 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)
- Shamir, A.: How to share a secret. Commun. ACM 22(11):612–613 (1979)
- Stinson, D.R.: Combinatorial Designs: Constructions and Analysis. Springer (2004)