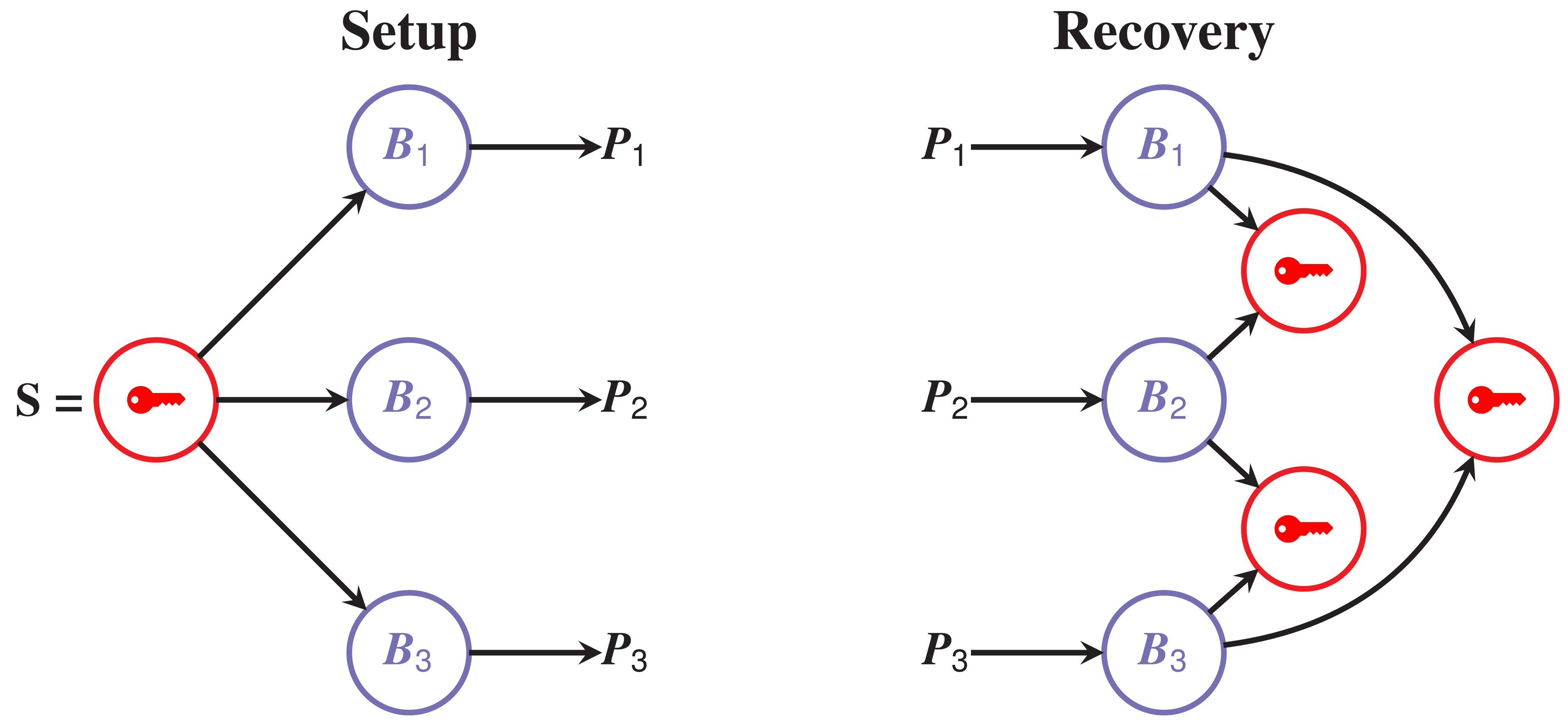
Cellular Automata, Latin Squares and Secret Sharing Schemes

Luca Mariot, Enrico Formenti, Alberto Leporati
Team MDSC, Laboratory I3S
{mariot, enrico.formenti}@i3s.unice.fr, leporati@disco.unimib.it

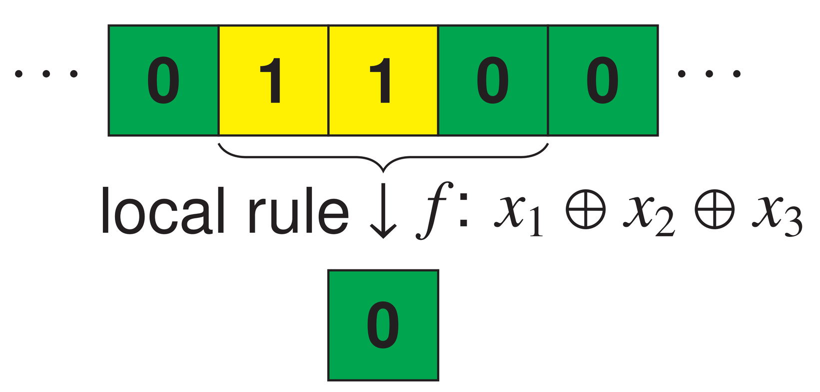
Secret Sharing Schemes

- A *Secret sharing scheme* enables a *dealer* D to split a *secret* S among a set $\{P_1, \cdots, P_n\}$ of *players*, each of whom receives a *share* B_i
- In (k, n) *threshold schemes*, the shares of at least k players out of n are required to recover the secret [3]
- **Goal**: Implement $(2, n)$ schemes using *cellular automata* (CA) and *Latin squares*

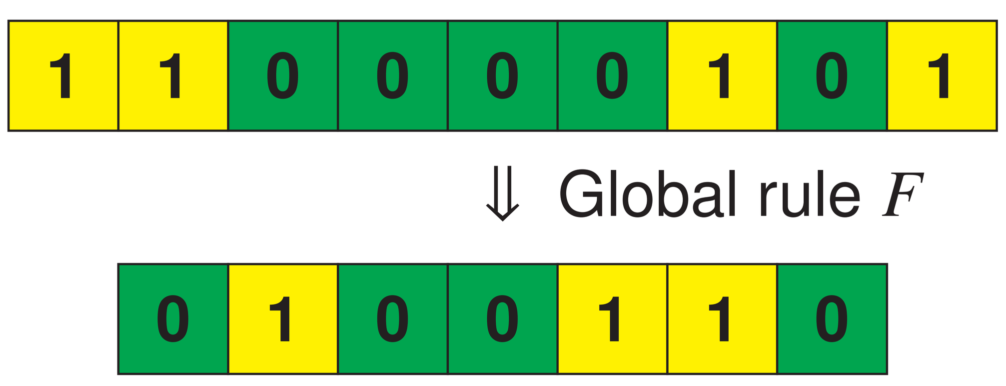


Cellular Automata (CA)

- A *cellular automaton* is composed of a lattice of *cells*, each of which updates its binary state according to a *local rule* f

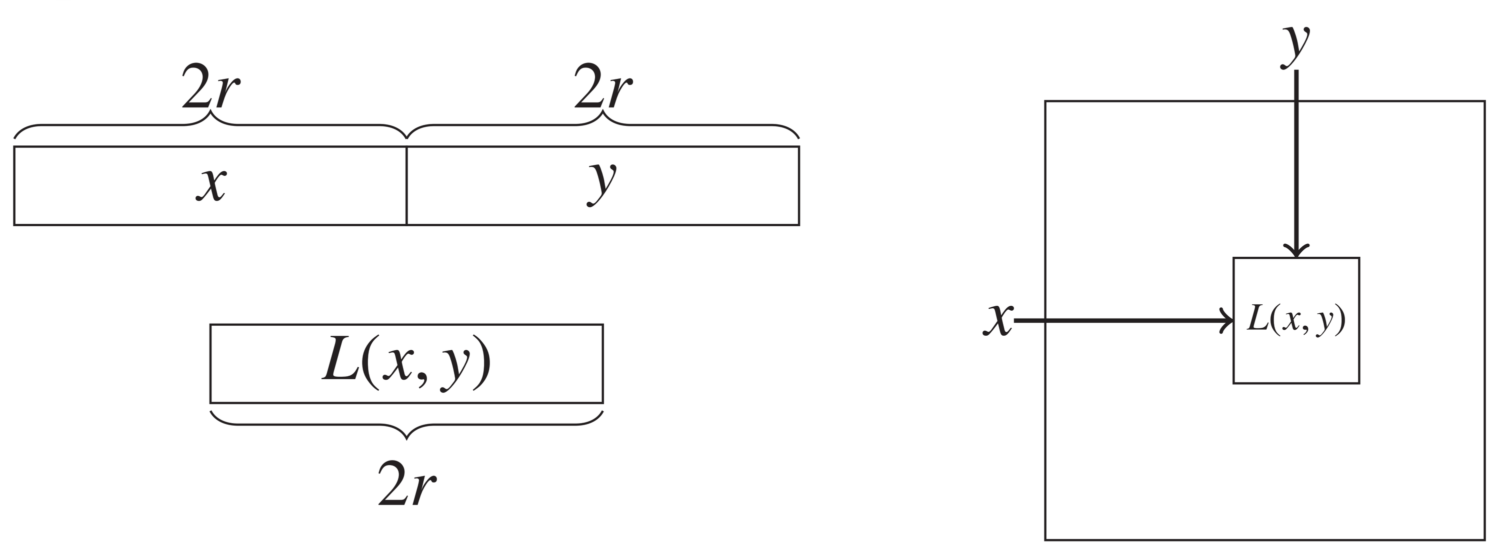


- The CA evolution is given by the application of the *global rule* F on the central cells

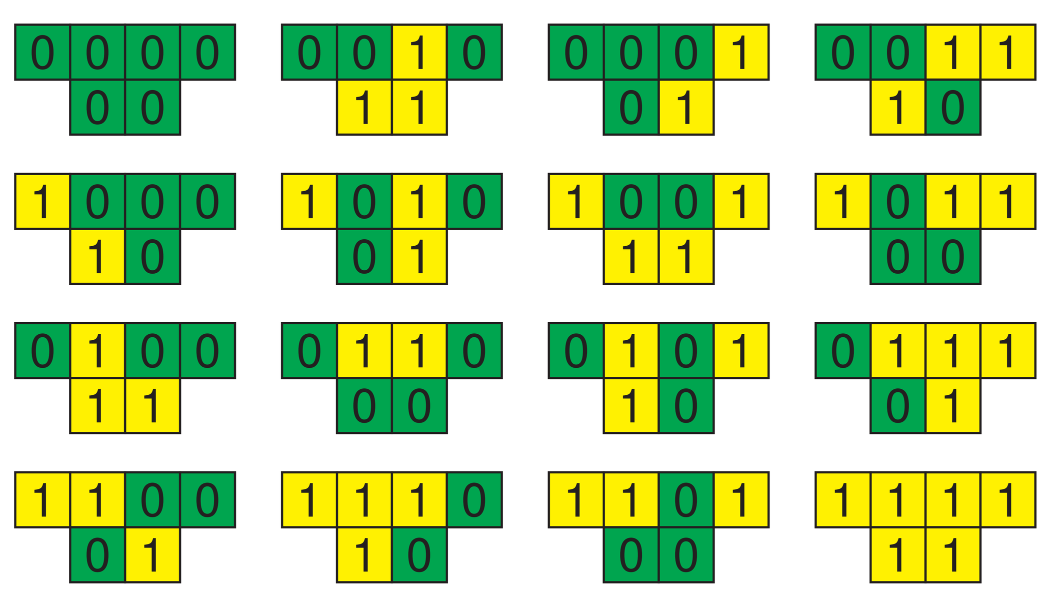


Latin Squares from Bipermutive CA

- A CA with bipermutive rule of radius r generates a Latin square of side 2^{2r}



- Example: radius $r = 1$, $N = 4$, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$



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

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

Latin Squares

- In a *Latin square* of side N, each number from 1 to N is contained exactly once in each row and in each column

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

- Two Latin squares are *orthogonal* if in their *superposition* each pair of numbers from 1 to N occurs exactly once

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

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

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

- **Remark**: A set of n *mutually orthogonal Latin squares* (MOLS) is equivalent to a $(2, n)$ threshold scheme

Main Result and Future Developments

- Two *linear* CA generate orthogonal Latin squares if and only if their associated polynomials are *relatively prime*
- Example: Rule 150 $\mapsto 1 + X + X^2$, Rule 90 $\mapsto 1 + X^2$

Rule 150

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

Rule 90

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

Superposition

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

- **Future development:** Count the number of coprime pairs of polynomials with nonzero constant term and degree n
- This number is related to OEIS sequence A002450 [2], $a(n) = 0, 1, 5, 21, 85, \ldots$ for $n = 1, 2, 3, 4, 5, \ldots$

References

[1] Mariot, L., Formenti, E., Leporati, A.: Constructing Orthogonal Latin Squares from Linear Cellular Automata. In: Exploratory papers of AUTOMATA 2016
[2] The Online Encyclopedia of Integer Sequences (OEIS), Sequence A002450. URL: `https://oeis.org/A002450`
[3] Shamir, A.: How to share a secret. Commun. ACM 22(11):612–613 (1979)