UNIVERSITY OF TWENTE.

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

Durham University

On the transversals of Latin squares generated by nonlinear bipermutive CA

Alberto Dennunzio, Maximilien Gadouleau, **Luca Mariot**

l.mariot@utwente.nl

ACRI 2026

Ghent, July 8, 2026

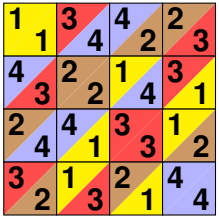
Orthogonal Latin Squares (MOLS)

Definition

A *Latin square* is a $n \times n$ matrix where all rows and columns are permutations of $[n] = \{1, \cdots, n\}$. Two Latin squares 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

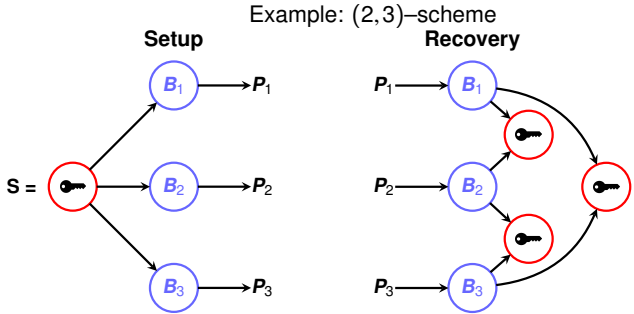
1	4	2	3
3	2	4	1
4	1	3	2
2	3	1	4



- n-**MOLS**: set of n pairwise orthogonal Latin squares [K15]

Cryptographic Application: Secret Sharing Schemes

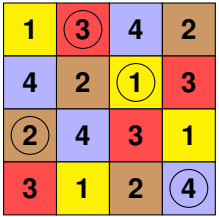
(k, n) **Threshold Secret Sharing Scheme**: a **dealer** shares a **secret** S among n **players** so that at least k players out of n are required to recover S [S79]



Remark: $(2, n)$–scheme $\Leftrightarrow$ set of n-MOLS [S04]

Transversals in Latin Squares

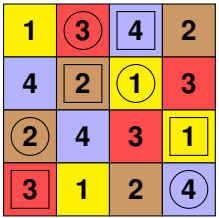
- **Transversal** of an $N \times N$ Latin square: set of N staggered cells where each number from 1 to N appears once



- ◯: $T_1 = \{(1,2),(2,3),(3,1),(4,4)\}$

Transversals in Latin Squares

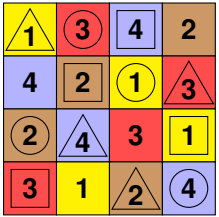
- **Transversal** of an $N \times N$ Latin square: set of N staggered cells where each number from 1 to N appears once



- ◯: $T_1 = \{(1,2),(2,3),(3,1),(4,4)\}$
- □: $T_2 = \{(1,3),(2,2),(3,4),(4,1)\}$

Transversals in Latin Squares

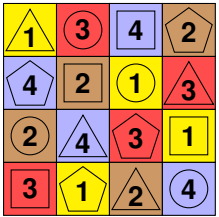
- **Transversal** of an $N \times N$ Latin square: set of N staggered cells where each number from 1 to N appears once



- ◯: $T_1 = \{(1,2),(2,3),(3,1),(4,4)\}$
- □: $T_2 = \{(1,3),(2,2),(3,4),(4,1)\}$
- △: $T_3 = \{(1,1),(2,4),(3,2),(4,3)\}$

Transversals in Latin Squares

- **Transversal** of an $N \times N$ Latin square L: set of N staggered cells where each number from 1 to N appears once



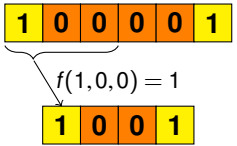
- ◯: $T_1 = \{(1,2),(2,3),(3,1),(4,4)\}$
- □: $T_2 = \{(1,3),(2,2),(3,4),(4,1)\}$
- △: $T_3 = \{(1,1),(2,4),(3,2),(4,3)\}$
- ⬠: $T_4 = \{(4,1),(2,1),(3,3),(4,2)\}$

- **Remark:** if L has N disjoint transversal $\Rightarrow$ L has an *orthogonal mate* [K15]

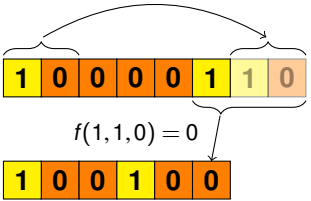
Cellular Automata

- One-dimensional Cellular Automaton (CA): a discrete parallel computation model composed of a finite array of n cells

Example: $n = 6$, $d = 3$, $f(s_i, s_{i+1}, s_{i+2}) = s_i \oplus s_{i+1} \oplus s_{i+2}$ (rule 150)



No Boundary CA – NBCA



Periodic Boundary CA – PBCA

- Each cell updates its state $s \in \mathbb{F}_2 = \{0,1\}$ by applying a local rule $f : \mathbb{F}_2^d \to \mathbb{F}_2$ to itself and the $d-1$ cells on its right [M19, M26]

Latin Squares through Bipermutive CA (1/2)

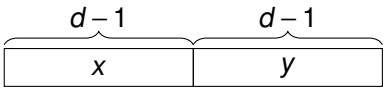
- Bipermutive CA: local rule f is defined as

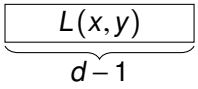
$$f(x_1, \cdots, x_d) = x_1 \oplus g(x_2, \cdots, x_{d-1}) \oplus x_d$$

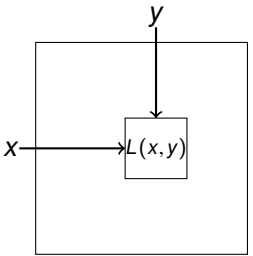
- $g : \mathbb{F}_2^{d-2} \to \mathbb{F}_2$: generating function of f [L13]

Lemma ([M16])

A (no-boundary) CA $F : \mathbb{F}_2^{2(d-1)} \to \mathbb{F}_2^d$ with bipermutive rule $f : \mathbb{F}_2^d \to \mathbb{F}_2$ generates a Latin square of order $N = 2^{d-1}$

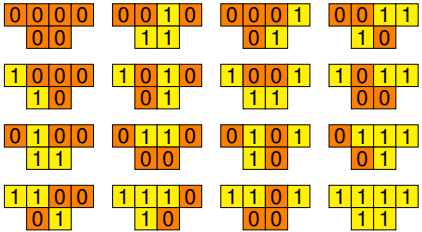






Latin Squares through Bipermutive CA (2/2)

- Example: CA $F : \mathbb{F}_2^4 \to \mathbb{F}_2^2$, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$ (Rule 150)
- Encoding: $00 \mapsto 1, 10 \mapsto 2, 01 \mapsto 3, 11 \mapsto 4$



(a) Rule 150 on 4 bits

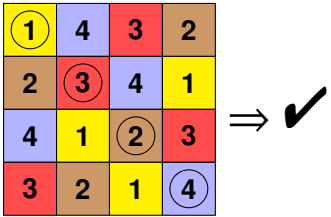
1	4	3	2
2	3	4	1
4	1	2	3
3	2	1	4

(b) Latin square L_{150}

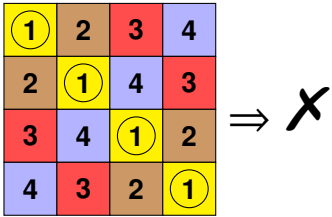
Problem: characterize the transversals of Latin squares generated by bipermutive CA

Transversals on the Main Diagonal

Question: which bipermutive CA have a transversal on the main diagonal?



(a) Rule 150



(b) Rule 90

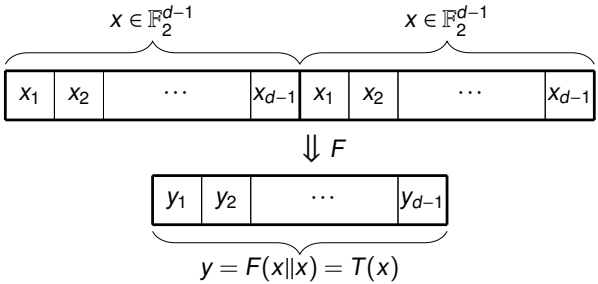
Idea: study the structure of the input configuration on the diagonal

Global Rule Restriction to Main Diagonal

Input configuration form: $(x, x) \in \mathbb{F}_2^{2(d-1)}$ (left and right block coincide)

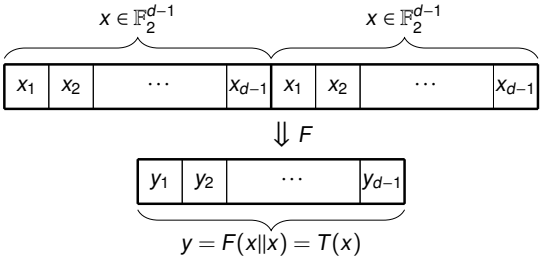
	00	10	01	11
00	1	4	3	2
10	2	3	4	1
01	4	1	2	3
11	3	2	1	4

(a) Rule 150



What is the mathematical form of the global rule?

Global Rule Form on the Main Diagonal



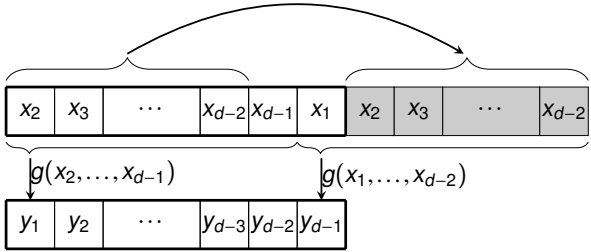
$$\begin{cases} y_1 & = f(x_1, x_2, \ldots, x_{d-1}, x_1) = \cancel{x_1} \oplus g(x_2, \ldots, x_{d-1}) \oplus \cancel{x_1} = g(x_2, \ldots, x_{d-1}) \\ y_2 & = f(x_2, x_3, \ldots, x_1, x_2) = \cancel{x_2} \oplus g(x_3, \ldots, x_1) \oplus \cancel{x_2} = g(x_3, \ldots, x_1) \\ & \vdots \\ y_{d-1} & = f(x_{d-1}, x_1, \ldots, x_{d-2}, x_{d-1}) = \cancel{x_{d-1}} \oplus g(x_1, \ldots, x_{d-2}) \oplus \cancel{x_{d-1}} = g(x_1, \ldots, x_{d-2}) \end{cases}$$

Remark 1: on the diagonal, the local rule depends only on the central $d-2$ cells

PBCA Mapping of the Diagonal Transversal

Remark 2: the transversal map $T : \mathbb{F}_2^{d-1} \to \mathbb{F}_2^{d-1}$ is defined by a PBCA with $d-1$ cells, equipped with $g : \mathbb{F}_2^{d-2} \to \mathbb{F}_2$ as a local rule.

$$\begin{cases} y_1 & = g(x_2, \ldots, x_{d-1}) \\ y_2 & = g(x_3, \ldots, x_1) \\ & \vdots \\ y_{d-1} & = g(x_1, \ldots, x_{d-2}) \end{cases}$$



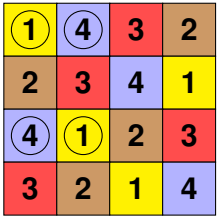
Theorem

The Latin square of the NBCA F has a transversal on the main diagonal if and only if the generating function g induces an invertible PBCA $T : \mathbb{F}_2^{d-1} \to \mathbb{F}_2^{d-1}$.

Computational Search Experiments (Bonus)

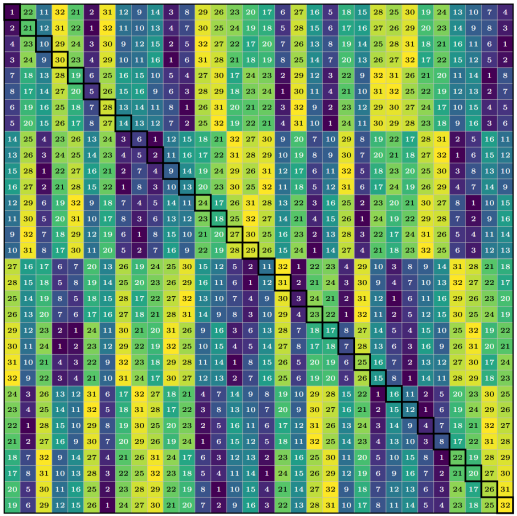
Intercalates	Nonlinearity	Rules
2816	4	8
2944	4	8
3072	4	24
3200	4	16
3328	4	16
3520	4	16
3584	4	8
3648	4	52
3680	4	8
3712	4	16
3744	4	8
3776	4	8
3840	4	8
3904	4	20
3936	4	16
3968	4	8
4032	2	8
4032	4	32
4096	4	24
4160	2	16
4160	4	24
4288	2	40
4352	4	16
4864	4	8
5376	2	32
5888	4	16
$7936^{(\dagger)}$	0	16

- Exhaustive search of bipermutive rules up to $d = 6$
- Only **linear** rules have a transversal on the main diagonal up to $d = 5$
- $d = 6$: 472 rules found, out of which **456 are nonlinear**
- ≥ 28 isotopy classes, linear rules form a single class



- **Intercalate**: 2×2 Latin subsquare
- # of intercalates: **invariant** for isotopy [K15]

Example with $d = 6$, $g(x_1, x_2, x_3, x_4) = x_1 \oplus x_3 \oplus x_1 x_4$



Conclusions

Wrapping up:

- Characterized subclass of (nonlinear) BCA whose Latin squares have a transversal on the main diagonal
- The generating function must induce an invertible PBCA of size $d-1$ [D95, M21]
- Linear rules of this subclass seem to form an isotopy class on their own

Future Directions:

- Characterize other transversals (**idea:** Eulerian cycles on de Bruijn graph [M17])
- Investigate disjointness properties of CA transversals

References

[D95] J. Daemen: Cipher and hash function design strategies based on linear and differential cryptanalysis. Ph.D. thesis, KU Leuven (1995)

[K15] A.D. Keedwell, J. Dénes: Latin squares and their applications. Elsevier (2015)

[L13] A. Leporati and L. Mariot: 1-Resiliency of bipermutive cellular automata rules. In: Proceedings of AUTOMATA 2013, pp. 110–123 (2013)

[M26] L. Manzoni, L. Mariot, G. Menara: Combinatorial designs and cellular automata: A survey. Discret. Appl. Math. 379:656–674 (2026)

[M21] L. Mariot, S. Picek, D. Jakobovic, A. Leporati: Evolutionary algorithms for designing reversible cellular automata. Genet. Prog. Evolvable Mach. 22(4):429–461 (2021)

[M19] L. Mariot, S. Picek, A. Leporati, and D. Jakobovic. Cellular automata based S-boxes. Cryptography and Communications 11(1):41–62 (2019)

[M17] L. Mariot, A. Leporati, A. Dennunzio, E. Formenti: Computing the periods of preimages in surjective cellular automata. Nat. Comput. 16(3):367–381 (2017)

[M16] L. Mariot, E. Formenti, A. Leporati: Constructing Orthogonal Latin Squares from Linear Cellular Automata. In: Exploratory papers of AUTOMATA 2016 (2016)

[S79] A. Shamir: How to share a secret. Commun. ACM 22(11):612–613 (1979)

[S04] D.R. Stinson: Combinatorial designs - constructions and analysis. Springer (2004)