Cellular Automata and Cryptography: Recent Advances and Open Problems

Luca Mariot

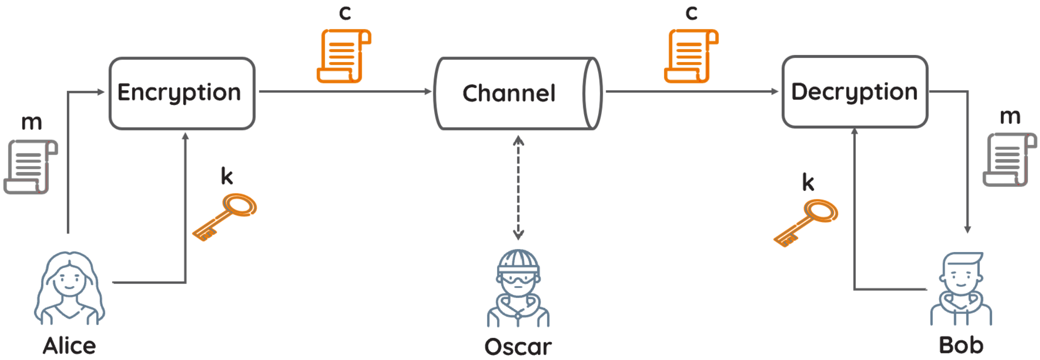
l.mariot@utwente.nl

ACANCOS workshop @UCNC 2026

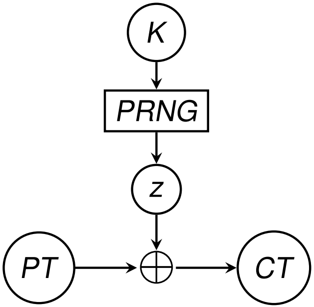
Trieste, June 22, 2026

Introduction to CA-Based Cryptography

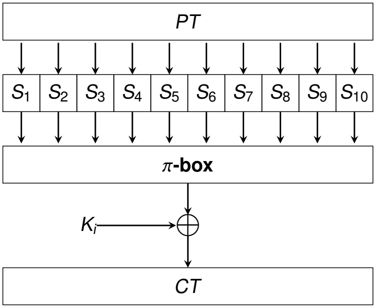
Basic Goal: enable *confidentiality* in communication using a shared symmetric key



- **m**: plaintext
- **c**: ciphertext
- **k**: encryption/decryption key



(a) Stream cipher



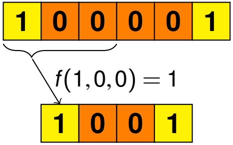
(b) Block cipher

Symmetric ciphers require several **low-level primitives**, such as:

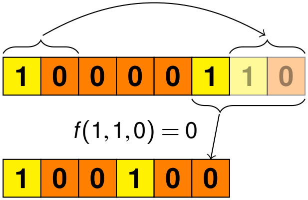
- Pseudorandom number generators (PRNG)
- Boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$ and S-boxes
- Permutation (diffusion) layers, ...

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

Example: $n = 6$, $d = 3$, $\omega = 0$, $f(s_i, s_{i+1}, s_{i+2}) = s_i \oplus s_{i+1} \oplus s_{i+2}$ (rule 150)



No Boundary CA – NBCA

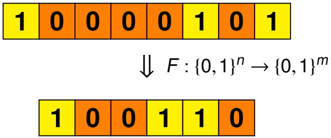


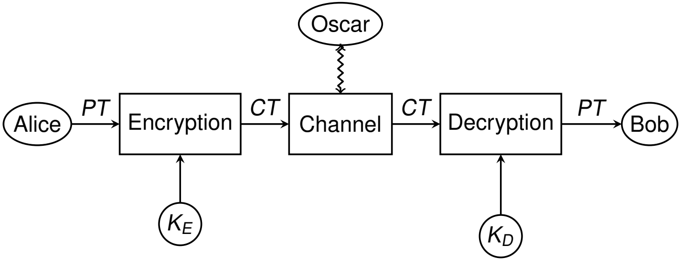
Fixed Boundary CA – FBCA

- Each cell updates its state $s \in \{0,1\}$ by applying a local rule $f : \{0,1\}^d \to \{0,1\}$ to itself, the ω cells on its left and the $d-1-\omega$ cells on its right

Motivations

General Research Goal: Investigate cryptographic primitives defined by CA





Why CA, anyway?

1. **Security from Complexity**: CA can yield very complex dynamical behaviors
2. **Efficient implementation**: Leverage CA parallelism and locality

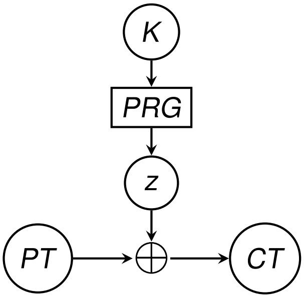
Summary

Types of cyptographic primitives based on CA considered in this talk:

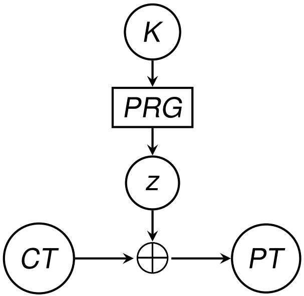
- **Stream Ciphers and Pseudorandom Generators**
- **Block Ciphers and S-boxes**
- **Secret Sharing Schemes**

Stream Ciphers based on CA

Vernam Stream Cipher



(a) Encryption

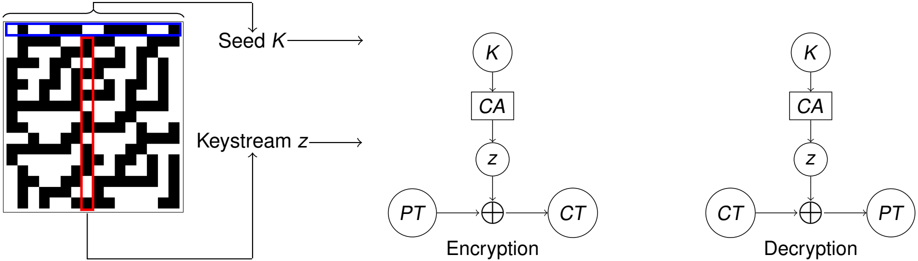


(b) Decryption

- K: secret key
- PRG: Pseudorandom Generator
- z: keystream
- $\bigoplus$: bitwise XOR
- PT: Plaintext
- CT: Ciphertext

CA-based Crypto History: Wolfram's PRNG

- CA-based Pseudorandom Generator (PRG) [W86]: central cell of rule 30 CA used as a stream cipher keystream



- Secret key: (random) initial condition of the CA

Attacks on Wolfram's PRNG [M91]

Analysis of Pseudo Random Sequences Generated by Cellular Automata

Willi Meier [1] Othmar Staffelbach [2]

[1] HTL Brugg-Windisch
CH-5200 Windisch, Switzerland

[2] GRETAG, Althardstrasse 70
CH-8105 Regensdorf, Switzerland

Abstract

The security of cellular automata for stream cipher applications is investigated. A cryptanalytic algorithm is developed for a known plaintext attack where the plaintext is assumed to be known up to the unicity distance. The algorithm is shown to be successful on small computers for key sizes up to N between 300 and 500 bits. For a cellular automaton to be secure against more powerful adversaries it is concluded that the key size N needs to be about 1000 bits.

The cryptanalytic algorithm takes advantage of an equivalent description of the cryptosystem in which the keys are not equiprobable. It is shown that key search can be reduced considerably if one is contented to succeed only with a certain success probability. This is established by an information theoretic analysis of arbitrary key sources with non-uniform probability distribution.

- Wolfram used only *empirical* and *statistical* tests for security analysis
- Meier and Staffelbach [M91] showed a correlation attack exploiting the *quasi-linearity* of rule 30:

$$f(x_1, x_2, x_3) = x_1 XOR (x_2 OR X_3)$$

Consequence: Wolfram's PRNG is useless when equipped with rule 30

Question: Can we fix Wolfram's PRNG?

Cryptographic Properties of Boolean Functions

- A mapping $f : \mathbb{F}_2^n \to \mathbb{F}_2$, most commonly represented by its *Truth Table* (TT) Ω_f
- *Walsh Transform* (WT): represents f as *correlations* with *linear* functions $a \cdot x$

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus a \cdot x}$$

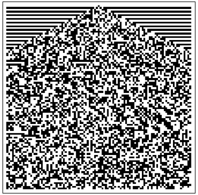
(x_1, x_2, x_3)	000	001	010	011	100	101	110	111
Ω_f	0	1	1	0	1	0	1	0
$W_f(a)$	0	-4	0	4	0	4	0	4

A **Boolean function** used in stream ciphers should be

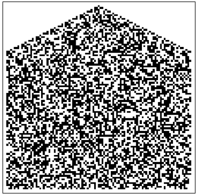
- balanced: $W_f(\underline{0}) = 0$
- highly nonlinear $nl(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \{|W_f(a)|\}$
- correlation immune of high order t (min value s.t. $W_f(a) = 0$ for all a with at most t ones)

Salvaging Wolfram's PRNG

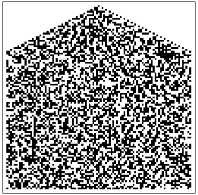
- **Problem** of rule 30: too small to give any meaningful cryptographic property
- Later works considered rules of larger diameters [L13, F14, L14]



(a) Rule 1452976485



(b) Rule 1520018790



(c) Rule 2778290790

- Example: bipermutive rules [L13] satisfy 1st-order correlation immunity, $d = 5$ is the minimum to find also nonlinear rules.

Shortcoming in CA-based Stream Ciphers

- Cryptographic properties are tailored for some PRNG models (combiner, filter, ...)
- But Wolfram's PRNG is not among them! So:

Shortcoming

Security claims for Wolfram-like PRNGs based on the cryptographic properties of the local rule are not enough:

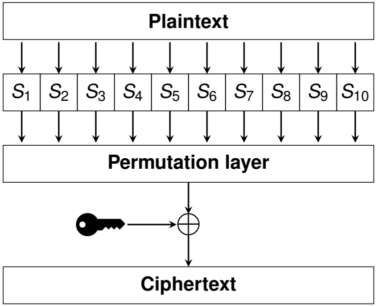
- *Attacks on the combiner or filter model might not be relevant in the CA setting*
- *Cryptographic properties might not capture other attacks unique to the CA model*

Insight

Consistently link the CA model with the security properties and the related attacks

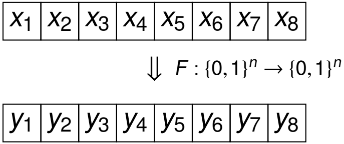
Block Ciphers based on CA

Zoom on SPN Block Ciphers



(a) Substitution-Permutation Network (SPN)

Zoom in on a **S-box** S_i:



(b) S-box S_i

S-boxes in SPN ciphers must satisfy several properties, mainly [C21]:

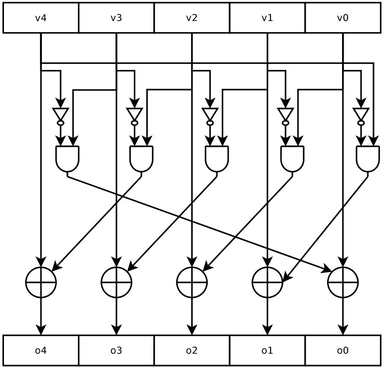
- **invertibility** (for decryption)
- High **nonlinearity** (for linear cryptanalysis)
- Low **differential uniformity** (for differential cryptanalysis)

"Reductionist" CA-Based Crypto: Keccak χ S-box

- Local rule (rule 210):

$$\chi(x_1, x_2, x_3) = x_1 \oplus (1 \oplus (x_2 \cdot x_3))$$

- Invertible for every odd CA size [D95]
- Used as a PBCA with $n = 5$ in the Keccak specification of SHA-3 standard [B11]
- CA iterated for a *single* step, and interleaved with other (non-local) operations

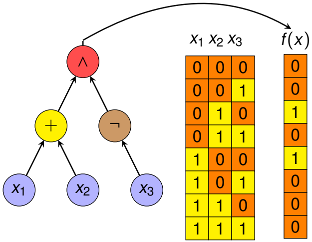


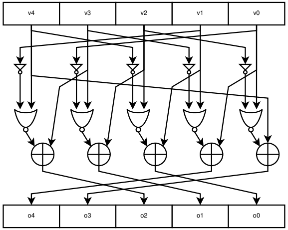
Algebraic approach:

- Theoretical analysis of specific CA rules as S-boxes
- Examples: χ in KECCAK [D95, B11]

Heuristic approach:

- Use of heuristic algorithms to optimize the crypto properties of CA rules [P17a, P17b, M19, M21, D23]
- More flexibility wrt other properties (e.g. implementation cost)





CA also for Diffusion Layers?

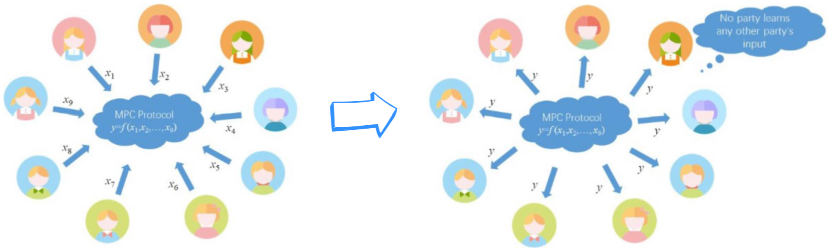
- The propagation of differences is bounded by the CA "speed of light" (diameter)

Image credits: J. Daemen, *On Keccak and SHA-3*,
`http://ice.mat.dtu.dk/slides/KeccakIcebreak-slides.pdf`

- **Consequence:** better to avoid CA in diffusion layers

Recent Advancements – CA ciphers over large prime fields

- Cryptographers are now interested in ciphers on $\mathbb{F}_p$, with p being a large prime number (e.g., $\approx 2^{128}$)



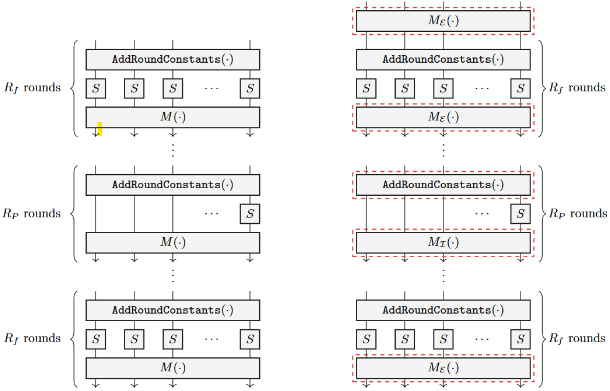
- **Motivation:** cryptographic protocols for SMPC, ZK proofs and FHE performs arithmetic operations in $\mathbb{F}_p$
- Recent designs use CA-like local maps for the mixing layer of these SMPC/ZK-friendly ciphers

Invertible Shift-Invariant Maps on $\mathbb{F}_p$

- **Poseidon hash function**: SPN-like structure
- **Substitution layer**: a periodic CA of short length, e.g. $n = 2, 3$:

$$F(x_0, x_1) = \gamma_0 \cdot x_0 + \gamma_1 \cdot x_1 + \\ + \gamma_2 (x_0 - x_1)^2$$

- **Negative results**: no invertible quadratic CA over $\mathbb{F}_p$ for $n \geq 5$

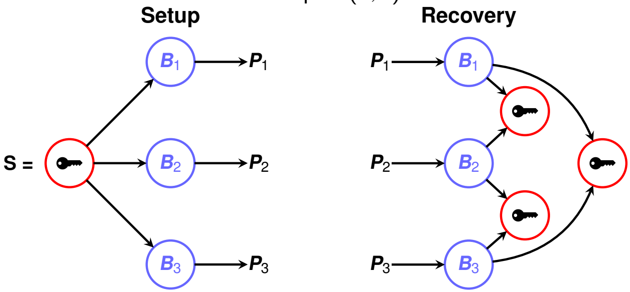


Secret Sharing Schemes based on CA

Threshold 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

Example: $(2, 3)$–scheme



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

Mutually 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

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

- k-**MOLS**: set of k pairwise orthogonal Latin squares

Latin Squares through Bipermutive CA (1/2)

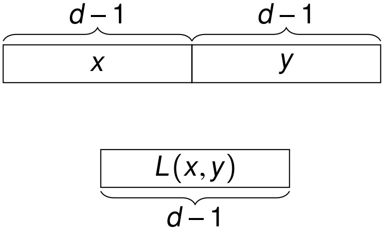
- Bipermutive CA: local rule f is defined as

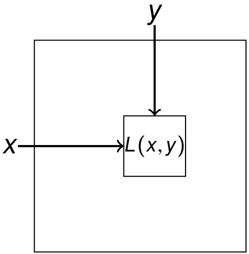
$$f(x_1, \cdots, x_d) = x_1 + \varphi(x_2, \cdots, x_{d-1}) + x_d$$

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

Lemma ([M20])

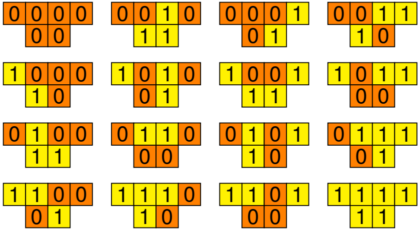
A (no-boundary) CA $F : \mathbb{F}_q^{2(d-1)} \to \mathbb{F}_q^d$ with bipermutive rule $f : \mathbb{F}_q^d \to \mathbb{F}_q$ generates a Latin square of order $N = q^{d-1}$





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}

Linear CA

- Local rule: *linear combination* of the neighborhood cells

$$f(x_1,\cdots,x_d) = a_1x_1 + \cdots + a_dx_d \ , \ a_i \in \mathbb{F}_q$$

- Associated polynomial:

$$f \mapsto p_f(X) = a_1 + a_2X + \cdots + a_dX^{d-1}$$

- $(n-d+1)\times n$ transition matrix:

$$M_F = \begin{pmatrix} a_1 & \cdots & a_d & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_1 & \cdots & a_d & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & a_1 & \cdots & a_d \end{pmatrix}, \quad x \mapsto M_F x^\top$$

- **Remark:** a linear rule is bipermutive iff $a_1, a_d \neq 0$

MOLS from Linear Bipermutive CA (LBCA)

Theorem ([M20])

A set of t linear bipermutive CA $F_1, \dots F_t : \mathbb{F}_q^{2(d-1)} \to \mathbb{F}_q^{d-1}$ generates a family of t-MOLS of order $N = q^{d-1}$ if and only if their associated polynomials are pairwise coprime

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

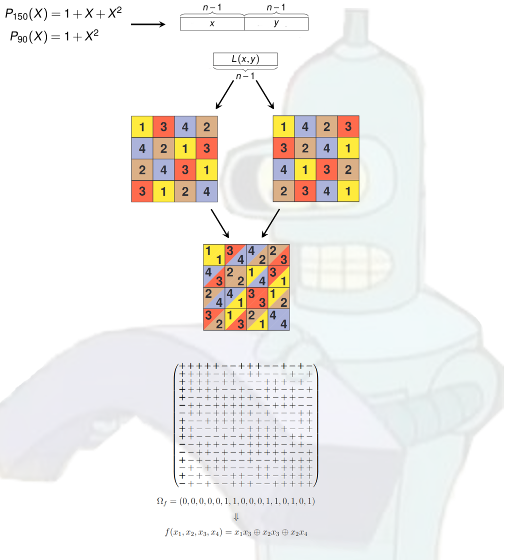
(c) Superposition

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

CA-based Secret Sharing: Recent Advances

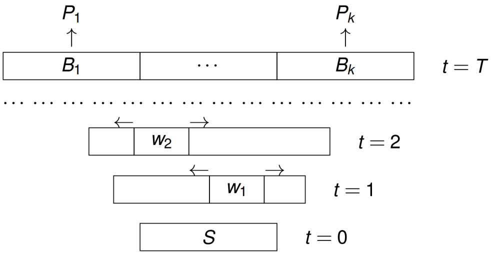
Different crypto applications of the same LBCA-based MOLS construction:

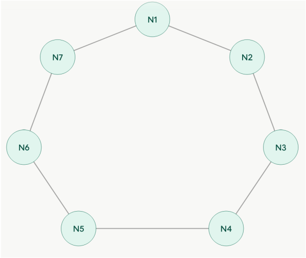
- **Bent functions** in the partial spread class [G23]
- **Maximal period sequences** with perfect diffusion [M23]
- **Anonymous Secret Sharing** (forthcoming, AUTOMATA 2026 [M26])



New Directions: Graph-Based Access Structures

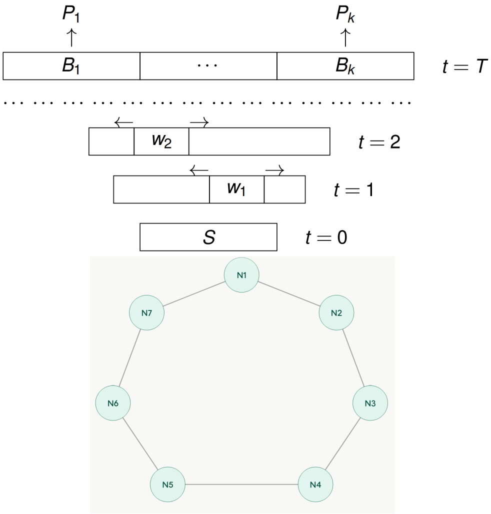
- **Sequential threshold:** shares are *adjacent* blocks of CA preimages
- Any two adjacent shares "collapse" on a copy of the secret via CA forward evolution [M14]
- *Graph perspective*: the shares are arranged on a line (or ring) topology
- What if we consider more general graphs-based access structures?





New Directions: Graph-Based Access Structures

- The ring graph topology stems from the one-dimensional CA topology
- **Idea:** move to **Automata Networks** to model any graph-based access structure
- Link to open questions in computational complexity and theory of cryptography (e.g., MINICRYPT $\stackrel{?}{=}$ CRYPTOMANIA)



Conclusions

Summary and Future Directions

To sum up:

- CA have their place in cryptography
- Actually, people in cryptography use them in their designs, calling them with different names (e.g. liftings, shift-invariant maps, etc.)

Directions for future research:

- For stream ciphers: closely analyze Wolfram's PRNG, find new attacks
- For block ciphers: study invertible CA over large prime fields $\mathbb{F}_p$
- For secret sharing: generalize to thresholds higher than $k = 2$, consider other (graph-based) access structures

References

[B11] G. Bertoni, J. Daemen, M. Peeters, G. Van Assche: The Keccak reference. (January 2011). http://keccak.noekeon.org/

[C21] C. Carlet: Boolean functions for cryptography and coding theory. Cambridge University Press (2021)

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

[D23] M. Djurasevic, D. Jakobovic, L. Mariot, S. Picek, S.: A survey of metaheuristic algorithms for the design of cryptographic Boolean functions. Cryptogr. Commun. 15(6):1171–1197 (2023)

[F14] E. Formenti, K. Imai, B. Martin, J. Yunès: Advances on random sequence generation by uniform cellular automata. In: Computing with New Resources, LNCS vol. 8808, pp. 56–70 (2014)

[G23] M. Gadouleau, L. Mariot, S. Picek: Bent functions in the partial spread class generated by linear recurring sequences. Des. Codes Cryptogr. 91(1):63–82 (2023)

[L14] A. Leporati and L. Mariot: Cryptographic properties of bipermutive cellular automata rules. J. Cell. Autom. 9(5-6):437–475 (2014)

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

[M26] L. Mariot, F. Mazzone, L. Manzoni, A. Leporati: How to reconstruct (anonymously) a secret cellular automaton. CoRR abs/2604.11362 (2026)

[M23] L. Mariot: Enumeration of maximal cycles generated by orthogonal cellular automata. Nat. Comput. 22(3): 477-491 (2023)

[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)

[M20] L. Mariot, M. Gadouleau, M., E. Formenti, A. Leporati: Mutually orthogonal Latin squares based on cellular automata. Des. Codes Cryptogr. 88(2):391–411 (2020)

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

[M14] L. Mariot, A. Leporati: Sharing Secrets by Computing Preimages of Bipermutive Cellular Automata. In: Proc. of ACRI 2014, pp. 417–426 (2014)

[M91] W. Meier, O. Staffelbach: Analysis of pseudo random sequence generated by cellular automata. In: Proc. of EUROCRYPT'91, pp. 186–199 (1991)

[P17a] S. Picek, L. Mariot, B. Yang, D. Jakobovic, N. Mentens: Design of S-boxes defined with cellular automata rules. In: Proceedings of Conf. Computing Frontiers 2017, pp. 409–414 (2017)

[P17b] S. Picek, L. Mariot, A. Leporati, D. Jakobovic: Evolving s-boxes based on cellular automata with genetic programming. In: Proceedings of GECCO 2017 (Companion), pp. 251–252 (2017)

[W86] S. Wolfram. Cryptography with cellular automata. In CRYPTO '85, pp. 429–432 (1986)