Building Correlation Immune Functions from Sets of Mutually Orthogonal CA

Luca Mariot, Luca Manzoni

luca.mariot@ru.nl

AUTOMATA 2022 – 11 October 2022
Correlation Immune Boolean Functions in Crypto

- **Boolean function**: mapping $f : \{0, 1\}^n \to \{0, 1\}$
- **Correlation Immunity of order $t$**: output of $f$ is statistically independent from any subset of at most $t$ inputs

Applications in symmetric crypto:

- Combine the output of $n$ LFSR for **stream encryption** [C21]
- CA-based **pseudorandom number generators** [L13, F14]
- Masking countermeasures for **side-channel analysis** [C12, K14]
Representation of Boolean Functions

- **Truth table**: vector $\Omega_f$ specifying $f(x)$ for all $x \in \mathbb{F}_2$
- **Walsh Transform**: correlation with the *linear* functions defined as $\omega \cdot x = \omega_1 x_1 \oplus \cdots \oplus \omega_n x_n$

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

| $(x_1, x_2, x_3)$ | 000 | 100 | 010 | 110 | 001 | 101 | 011 | 111 |
|-------------------|-----|-----|-----|-----|-----|-----|-----|-----|
| $\Omega_f$        | 0   | 1   | 1   | 0   | 1   | 0   | 0   | 1   |
| $\hat{F}(\omega)$ | 0   | 0   | 0   | 0   | 0   | 0   | 0   | 8   |

Example: $n = 3, f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$
Correlation Immunity: Walsh Characterization

- \( f \) is \( t \)-correlation immune iff \( W_f(a) = 0 \) for all \( a \) s.t. \( 1 \leq HW(a) \leq t \), where \( HW \) is the Hamming weight of \( a \) [X88]

Example: \( t = 2 \)

| \((x_1, x_2, x_3)\) | 000 | 100 | 010 | 110 | 001 | 101 | 011 | 111 |
|---------------------|-----|-----|-----|-----|-----|-----|-----|-----|
| \( \Omega_f \)     | 0   | 1   | 1   | 0   | 1   | 0   | 0   | 1   |
| \( \hat{F}(\omega) \)| 0   | 0   | 0   | 0   | 0   | 0   | 0   | 8   |

\[\downarrow\]

\( f \) is 2-order correlation immune

- Relevance in side-channel: \( t \)-order CI functions \( \Rightarrow \)
  Boolean masking resistant to SCA attacks of order \( t \)
Orthogonal Arrays (OA)

- \((N, k, s, t)\) **Orthogonal Array**: \(N \times k\) matrix \(A\) such that each \(t\)-uple occurs \(\lambda = N/s^t\) times in each \(N \times t\) submatrix.

![Example OA (8, 4, 2, 3)]

- Applications in statistics, coding theory, cryptography
Correlation Immunity: OA Characterization

- **Support** of $f$: sets of input vectors $x$ that map to 1 under $f$

| $x_1$ | $x_2$ | $x_3$ | $f(x)$ |
|-------|-------|-------|--------|
| 0     | 0     | 0     | 0      |
| 0     | 0     | 1     | 1      |
| 0     | 1     | 0     | 1      |
| 0     | 1     | 1     | 0      |
| 1     | 0     | 0     | 1      |
| 1     | 0     | 1     | 0      |
| 1     | 1     | 0     | 0      |
| 1     | 1     | 1     | 1      |

| $x_1$ | $x_2$ | $x_3$ |
|-------|-------|-------|
| 0     | 0     | 1     |
| 0     | 1     | 0     |
| 1     | 0     | 0     |
| 1     | 1     | 1     |

$\downarrow$

**OA**$(4,3,2,2)$

---

**Theorem ([C92])**

$f : \{0,1\}^n \rightarrow \{0,1\}$ is $t$-order CI $\iff$ Support of $f$ is an OA$(N,n,2,t)$, with $N = |\text{Supp}(f)|$
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

| 1 | 0 | 0 | 0 | 0 | 1 |
|---|---|---|---|---|---|

$f(1, 0, 0) = 1$

| 1 | 0 | 0 | 1 |

Periodic Boundary CA – PBCA

| 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |

$f(1, 1, 0) = 0$

| 1 | 0 | 0 | 1 | 0 | 0 |

Each cell updates its state $s \in \{0, 1\}$ by evaluating a local rule $f : \{0, 1\}^d \rightarrow \{0, 1\}$ on itself and the $d - 1$ cells on its right.
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 $(x, y) \in [n] \times [n]$.

- **$k$-MOLS**: set of $k$ pairwise orthogonal Latin squares
- **$k$-MOLS** are equivalent to $OA(n^2, k, n, 2)$
Bipermutive CA: denoting $\mathbb{F}_2 = \{0, 1\}$, local rule $f$ is defined as

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

$\varphi : \mathbb{F}_2^{d-2} \to \mathbb{F}_2$: generating function of $f$

Lemma ([E93, M16])

A 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 $N = 2^{d-1}$

$$L(x, y)$$

Luca Mariot, Luca Manzoni
Building Correlation Immune Functions from Sets of Mutually Orthogonal CA
Example: CA $F : \mathbb{F}_2^4 \rightarrow \mathbb{F}_2^2$, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$ (Rule 150)

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

(a) Rule 150 on 4 bits

(b) Latin square $L_{150}$

$k$-Mutually Orthogonal Cellular Automata (MOCA): $k$ bipermutive CA $F, G$ generating a set of $k$-MOLS
Example with Linear CA: Rules 90-150

- Bipermutive Linear rule: \( f(x) = x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_{d-1} x_{d-1} \oplus x_d \)
- Polynomial rule: \( P_f(X) = 1 + a_2 X + \cdots + a_{d-1} X^{d-2} + X^{d-1} \)

Theorem ([M20])

Two bipermutive linear rules generates OCA if and only if their associated polynomials are coprime

\[ P_{150}(X) = 1 + X + X^2 \]

\[ P_{90}(X) = 1 + X^2 \quad \text{(coprime)} \]
Construction of CI functions from MOCA

**Procedure:**

- **Input:** $k$-MOCA $F_1, \cdots, F_k : \mathbb{F}_2^{2b} \rightarrow \mathbb{F}_2^b$ of diameter $d = b + 1$
- Construct the set of $k$-MOLS over $[2^b]$ using the combinatorial algorithms from [M17, M18]
- "Linearize" the $k$-MOLS in a $2^b \times k$ OA
- Convert each entry in the OA in **binary**
- **Output:** the converted binary array

**Lemma**

The output array is an OA($2^b, kb, 2, 2$).
Computational Search Results

- **Consequence**: $k$-MOCA generate supports of Boolean functions with $n = kb$ variables with CI order at least 2
- Exhaustive search of 3-MOCA with $d = 4, 5$, $d = b + 1$
- Checked CI order with Walsh Transform

**Table**: Classification of correlation immune functions generated by 3-MOCA of diameter $d \in \{4, 5\}$.

| $d$ | #3-MOCA | $n$ | $w_H$ | $Cl$ | #CI | Min$w_H$ |
|-----|---------|-----|-------|------|-----|----------|
| 4   | 2       | 9   | 64    | 3    | 2   | 20       |
| 5   | 36      | 12  | 256   | 3    | 27  | 24       |
| 5   | 36      | 12  | 256   | 4    | 9   | 24       |

- **Main finding**: all functions are at least 3-CI
Wrapping up:

- We proved that $k$-MOCA generate correlation immune functions of order at least 2
- Experimentally, we noticed that $k$-MOCA functions actually have order at least 3

Future directions:

- Theoretically: are there MOCA that give CI functions with $t = 2$?
- Practically: reduce the Hamming weight of the functions, using evolutionary algorithms [M21]
References

- [C92] P. Camion, C. Carlet, P. Charpin, N. Sendrier: On Correlation-Immune Functions. Proceedings of CRYPTO 1991, pp. 86-100 (1992)
- [C21] C. Carlet: Boolean functions for cryptography and coding theory. Cambridge University Press (2021)
- [C12] C. Carlet, J.-L. Danger, S. Guilley, H. Maghrebi: Leakage Squeezing of Order Two. Proceedings of INDOCRYPT 2012, pp. 120-139 (2012)
- [E93] Eloranta, K.: Partially Permutive Cellular Automata. Nonlinearity 6(6), 1009–1023 (1993)
- [F14] E. Formenti, K. Imai, B. Martin, J.-B. Yunès: Advances on Random Sequence Generation by Uniform Cellular Automata. Computing with New Resources 2014: 56-70 (2014)
- [K14] S. Karmakar, D.R. Chowdhury: Leakage squeezing using cellular automata and its application to scan attack. J. Cell. Autom. 9(5-6) (2014) 417–436
- [L13] A. Leporati and L. Mariot: 1-Resiliency of Bipermutive Cellular Automata Rules. Proceedings of Automata 2013, pp. 110-123 (2013)
- [M21] L. Mariot: Deriving Smaller Orthogonal Arrays from Bigger Ones with Genetic Algorithm. CoRR abs/2111.13047 (2021)
- [M20] L. Mariot, M. Gadouleau, E. Formenti, A. Leporati: Mutually orthogonal latin squares based on cellular automata. Des. Codes Cryptogr. 88(2): 391-411 (2020)
- [M18] L. Mariot, A. Leporati: Inversion of Mutually Orthogonal Cellular Automata. Proceedings of ACRI 2018, pp. 364-376 (2018)
- [M17] L. Mariot, E. Formenti, A. Leporati: Enumerating Orthogonal Latin Squares Generated by Bipermutive Cellular Automata. Proceedings of AUTOMATA 2017, pp. 151-164 (2017)
- [M16] L. Mariot, E. Formenti, A. Leporati: Constructing Orthogonal Latin Squares from Linear Cellular Automata. In: Exploratory papers of AUTOMATA 2016 (2016)
- [X88] G.-Z. Xiao, J. L. Massey: A spectral characterization of correlation-immune combining functions. IEEE Trans. Inf. Theory 34(3): 569-571 (1988)