Behind the scenes of a new construction for bent functions

Luca Mariot
luca.mariot@ru.nl

Joint work with Maximilien Gadouleau and Stjepan Picek

MathCifris Seminar – Trento, November 2, 2022
Summary

Introduction: an (unlucky) paper

Part 1: Cellular Automata and Mutually Orthogonal Latin Squares

Part 2: The Complicated Construction

Part 3: A Simplified Construction with Linear Recurring Sequences

Conclusions
Introduction: an (unlucky) paper


Published online August 13, 2022 [GMP22]
Peer-review Timeline

BFA 2020

End 2019

Dec 2019: submission
Mar 2020: Reject

2020

CCDS

Dec 2020: submission
Oct 2020: submission
Dec 2020: Reject

2021

Mar 2021: Major rev.
Dec 2021: Rev. 1
Feb 2022: Minor rev.

DESI

May 2022: Minor rev.
Jun 2022: Rev. 3
Jul 2022: Rev. 4

2022

Jun 2022: Minor rev.

Jul 2022: Rev. 2
Mar 2022: Rev. 2

ACCEPT!

Luca Mariot

Behind the scenes of a new construction for bent functions
Boolean Functions in Symmetric Ciphers

Boolean functions $f : \{0, 1\}^n \rightarrow \{0, 1\}$ are used in [C21]

- **Stream ciphers**, to design the keystream generator (KSG)
- **Block ciphers**, as the coordinate functions of $S$-boxes ($S_i$)
Boolean Functions - Basic Representations

▶ **Truth table**: a $2^n$-bit vector $\Omega_f$ specifying $f(x)$ for all $x \in \{0, 1\}^n$

<table>
<thead>
<tr>
<th>$(x_1, x_2, x_3)$</th>
<th>000</th>
<th>100</th>
<th>010</th>
<th>110</th>
<th>001</th>
<th>101</th>
<th>011</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Omega_f$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

▶ **Algebraic Normal Form (ANF)**: Sum (XOR) of products (AND)

$$f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3 \oplus x_2 x_3$$

▶ **Walsh Transform**: correlation with linear functions $a \cdot x$,

$$W(f, a) = \sum_{x \in \{0, 1\}^n} (-1)^{f(x) \oplus a \cdot x}$$ for all $a \in \{0, 1\}^n$
Bent Functions

- **Parseval’s Relation**, valid on any Boolean function:
\[
\sum_{a \in \{0,1\}^n} [W(f, a)]^2 = 2^{2n} \text{ for all } f : \{0,1\}^n \rightarrow \{0,1\}
\]

- **Bent functions**: \(W(f, a) = \pm 2^{\frac{n}{2}}\) for all \(a \in \{0,1\}^n\)
  - Reach the highest possible **nonlinearity**
  - Exist only for \(n\) even and they are **unbalanced**

Example: \(f(x_1, x_2, x_3, x_4) = x_1 x_3 + x_1 x_4 + x_2 x_4\)
Constructions of Bent Functions

Given \( n = 2m \):

- **Maiorana-McFarland** [M73]: \( f : \mathbb{F}_2^n \to \mathbb{F}_2 \) is defined as
  \[
  f(x, y) = x \cdot \pi(y) \oplus g(y)
  \]
  where \( \pi : \mathbb{F}_2^m \to \mathbb{F}_2^m \) is any permutation of \( \mathbb{F}_2^m \) and \( g : \mathbb{F}_2^m \to \mathbb{F}_2 \) is any function of \( m \) variables

- **Partial spreads** [D74]: \( f \in \mathcal{PS}^- \ (f \in \mathcal{PS}^+) \) is defined as
  \[
  \text{supp}(f) = \bigcup_{S \in \mathcal{P}} (S \setminus \{0\}) \quad \left( \text{supp}(f) = \bigcup_{S \in \mathcal{P}} S \right),
  \]
  with \( S \) a family of \( 2^{m-1} + 1 \) \( m \)-dimensional subspaces of \( \mathbb{F}_2^n \) with pairwise trivial intersection

Luca Mariot

Behind the scenes of a new construction for bent functions
Part 1: Cellular Automata and Mutually Orthogonal Latin Squares
Cellular Automata

- A vectorial function \( F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m \) with uniform coordinates

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

- 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 \textit{Latin square} is a $n \times n$ matrix where all rows and columns are permutations of $[n] = \{1, \cdots, n\}$. Two Latin squares are \textit{orthogonal} if their superposition yields all the pairs $(x, y) \in [n] \times [n]$.

\begin{itemize}
  \item \textbf{$k$-MOLS}: set of $k$ pairwise orthogonal Latin squares
  \item \textbf{$k$-MOLS} are equivalent to $OA(n^2, k, n, 2)$
\end{itemize}
Bipermutive CA: local rule $f$ is defined as

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

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

Lemma ([E93, M16])

A CA $F : \mathbb{F}_q^{2(d-1)} \rightarrow \mathbb{F}_q^d$ with bipermutive rule $f : \mathbb{F}_q^d \rightarrow \mathbb{F}_q$ generates a Latin square of order $N = q^{d-1}$
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 $L_{150}$
Linear CA

- Local rule: *linear combination* of the neighborhood cells
  
  \[ f(x_1, \ldots, x_d) = a_1 x_1 + \cdots + a_d x_d, \quad a_i \in \mathbb{F}_q \]

- Associated polynomial:
  
  \[ f \mapsto p_f(X) = a_1 + a_2 X + \cdots + a_d X^{d-1} \]

- Global rule: \( F : \mathbb{F}_q^n \to \mathbb{F}_q^{n-d+1} \) is described by a \( (n-d+1) \times n \) transition matrix:

  \[
  M_F = \begin{pmatrix}
  a_1 & \cdots & a_d & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
  0 & a_1 & \cdots & a_d & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\
  \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
  0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \quad a_1 \quad \cdots \quad a_d
  \end{pmatrix}
  \]

  \[ x = (x_1, \cdots, x_n) \mapsto M_F x^\top \]

- **Remark**: a linear rule is bipermutative iff \( a_1, a_d \neq 0 \)
Sylvester Matrices

- Two linear bipermutive CA with rules $f, g : \mathbb{F}_q^d \rightarrow \mathbb{F}_q$ generate orthogonal Latin squares iff the following matrix is invertible:

$$M_{F,G} = \begin{pmatrix}
    a_1 & \cdots & a_d & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\
    0 & a_1 & \cdots & a_d & 0 & \cdots & \cdots & \cdots & 0 \\
    \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\
    0 & \cdots & \cdots & \cdots & 0 & a_1 & \cdots & a_d \\
    b_1 & \cdots & b_d & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\
    0 & b_1 & \cdots & b_d & 0 & \cdots & \cdots & \cdots & 0 \\
    \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\
    0 & \cdots & \cdots & \cdots & 0 & b_1 & \cdots & b_d \\
\end{pmatrix}$$

- ... but this is the **Sylvester matrix** of the two polynomials $p_f, p_g$, and $\det(M_{F,G} \neq 0 \iff \gcd(p_f, p_g) = 1$
MOLS from Linear Bipermutive CA (LBCA)

Theorem ([MGLF20])

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

(a) Rule 150

(b) Rule 90

(c) Superposition

Figure: $P_{150}(X) = 1 + X + X^2$, $P_{90}(X) = 1 + X^2$ (coprime)
Counting MOLS from linear CA

Number of coprime polynomials over $\mathbb{F}_2$ of degree $n$ and nonzero constant term:

$$a(n) = 4^{n-1} + a(n-1) = \frac{4^{n-1} - 1}{3}$$

$= 0, 1, 5, 21, 85, ...$

Corresponds to OEIS A002450

Generalized to any finite field, along with size of largest family of pairwise coprime polynomials, in:

Part 2: The Complicated Construction
Hadamard Matrices

- **Hadamard Matrix**: a \( n \times n \) matrix with \( \pm 1 \) entries and s.t. \( H \cdot H^\top = I_n \)

\[
H = \begin{pmatrix}
+ & + & + & + \\
+ & - & + & - \\
+ & + & - & - \\
+ & - & - & + \\
\end{pmatrix}, \quad n = 4
\]

- **Necessary condition**: \( n = 1,2 \) or \( n = 4k \)

- **Hadamard Conjecture**: a Hadamard matrix exists for every \( n = 4k \)
Theorem (Dillon, 1974 [D74])

Given $f : \{0, 1\}^n \rightarrow \{0, 1\}$ and $\hat{f}(x) = (-1)^{f(x)}$. Define the $2^n \times 2^n$ matrix $H$ for all $x, y \in \{0, 1\}^n$ as:

$$H(x, y) = \hat{f}(x \oplus y)$$

Then, $f$ is a bent function if and only if $H$ is a Hadamard matrix.

Example: $f(x_1, x_2) = x_1 x_2$

<table>
<thead>
<tr>
<th>$x_1$</th>
<th>$x_2$</th>
<th>$x_1 x_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

$$H = \begin{pmatrix}
+ & + & + & - \\
+ & + & - & + \\
+ & - & + & + \\
- & + & + & +
\end{pmatrix}$$
Orthogonal Array $OA(t, N)$ for $t$ MOLS of order $N$: $N^2 \times t$ matrix where each column is the "linearization" of a Latin square

Theorem (Bush, 1973 [B73])

Given a set of $t$ MOLS of order $N = 2t$, and $A$ the associated $OA(t, 2t)$, define the $4t^2 \times 4t^2$ matrix $H$ as follows:

$$H(i, j) = \begin{cases} +1 & \text{if } i = j \\ -1 & \text{if } i \neq j \text{ and } \exists k \in \{1, \cdots, t\} \text{ s.t. the column } k \text{ of } A \text{ has the same symbol in rows } i \text{ and } j \\ +1 & \text{otherwise} \end{cases}$$

for $i, j \in \{1, \cdots, 4t^2\}$. Then, $H$ is a symmetric Hadamard matrix.

Luca Mariot

Behind the scenes of a new construction for bent functions
Remark: Not all $t$-MOLS sets give rise to a Hadamard matrix with the $\hat{f}(x \oplus y)$ structure required for a bent function!

Smallest counterexample: $n = 6$, $t = 2^{\frac{n-2}{2}} = 4$, $N = 2t = 8$

The resulting $64 \times 64$ Hadamard matrix does not give a bent function
Question: Are the MOLS arising from linear CA suitable for constructing bent functions?

We consider only CA over $\mathbb{F}_q$ with $q = 2^l$, $l \in \mathbb{N}$

The order of the Hadamard matrix must be $4t^2 = 2^n$

We need $t$ coprime polynomials of degree $b = d - 1$:

$$2^{lb} = 2t \iff lb = 1 + \log_2 t$$

Since both $l$ and $b$ are integers, $t = 2^w$ for $w \in \mathbb{N}$
Theorem

Let $H$ be the Hadamard matrix of order $2^{2(w+1)}$ defined by the $t$ LBCA $F_1, \cdots, F_t : \mathbb{F}_q^{2b} \rightarrow \mathbb{F}_q^b$, and define $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, $n = 2(w + 1)$ as:

$$f(x) = \begin{cases} 
0, & \text{if } x = 0 \\
1, & \text{if } x \neq 0 \text{ and } \exists k \in \{1, \cdots, t\} \text{ s.t. } F_k(x) = 0 \\
0, & \text{otherwise}
\end{cases}$$

Then, it holds that:

$$H(x, y) = \hat{f}(x \oplus y)$$

and thus $f$ is a bent function

Remark: The linearity of the CA is crucial to grant this result (and costed us our first reject!)
Example

\[ p_f(X) = 1 + X^2 \]

\[
\begin{array}{cccc}
1 & 2 & 3 & 4 \\
2 & 1 & 4 & 3 \\
3 & 4 & 1 & 2 \\
4 & 3 & 2 & 1 \\
\end{array}
\]

\[ p_g(X) = 1 + X + X^2 \]

\[
\begin{array}{cccc}
1 & 4 & 3 & 2 \\
2 & 3 & 4 & 1 \\
4 & 1 & 2 & 3 \\
3 & 2 & 1 & 4 \\
\end{array}
\]

\[ L_1 L_2 = \begin{pmatrix}
1 & 1 \\
2 & 4 \\
3 & 3 \\
4 & 2 \\
1 & 3 \\
4 & 4 \\
3 & 1 \\
3 & 4 \\
4 & 1 \\
1 & 2 \\
2 & 3 \\
4 & 3 \\
3 & 2 \\
2 & 1 \\
1 & 4 \\
\end{pmatrix}
\]

\[ H = \begin{pmatrix}
\end{pmatrix}
\]

\[ \Omega_f = (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \]

\[ f(x_1, x_2, x_3, x_4) = x_1 x_3 \oplus x_2 x_3 \oplus x_2 x_4 \]

Figure 3: Example of bent function of \( n = 4 \) variables generated by the \( t = 2 \) MOLS of order \( 2t = 4 \) defined by the LBCA with rule 90 and 150, respectively. The two Latin squares are represented on the left in the OA form. The first row and the first column of the Hadamard matrix \( H \) coincide with the polarity truth table of the function.
Existence and Counting

Combinatorial questions addressed in [GMP20]:

- **Existence:** for even $n$, does a large enough family of coprime polynomials exist?
- **Counting:** how many families of this kind exist (= number of CA-based bent functions)?
Existence and Counting

Theorem ([GMP20])

Let \( l, b, w \in \mathbb{N} \) such that \( lb = 1 + w \), and \( q = 2^l \). Then:

- There is a family of \( t = 2^w \) pairwise coprime polynomials of degree \( b \) over \( \mathbb{F}_q \) if and only if \( b \in \{1, 2\} \)
- The number of bent functions of \( n = 2(w + 1) \) variables that can be obtained by Theorem 4 is:
  - \( (2^{w+1} - 1), \) when \( b = 1 \)
  - \( \sum_{A=0}^{l_2} \binom{l_2}{A} \sum_{B=0}^{2^w - A} \binom{l_1 - B}{B} \frac{(2(2^w - B - A))!}{(2^w - B - A)!2^{2w - B - A}}, \) where \( l_2 = \frac{1}{2}(q^2 - q) \) and \( l_1 = q - 1 \), when \( b = 2 \).

Remark: each family can always be augmented with the polynomials 1 and \( X^b \)
Part 3: A Simplified Construction with Linear Recurring Sequences
Reviewers Feedback

- First attempt: BFA, reject (incomplete proof)
- Second attempt: CCDS, reject (complicated construction, no guarantee the obtained bent functions are new)
- Third attempt: DESI, major revision

Strictest (and most enthusiastic!) review:

This paper must be published in some form! :) It has the potential of becoming a major reference on bent functions because it identifies a new source of partial spreads large enough to give bent functions!

... But not in its present form which buries and obscures their great new result in many pages of material on subjects which, in retrospect, are unnecessary for a lucid exposition of their new results. It may be in order to briefly mention how they were led to their theorem via the CA, Latin square, MOLS and Bush
Linear Recurring Sequences (LRS)

- Sequence \( \{x_i\}_{i \in \mathbb{N}} \) satisfying the following relation:

\[
a_0 x_i + a_1 x_{i+1} + \ldots + a_{d-1} x_{i+d-1} = x_{i+d}
\]

- Computed by a Linear Feedback Shift Register (LFSR):

- Feedback polynomial:

\[
f(X) = a_0 + a_1 X + \cdots + a_{d-1} X^{d-1} + X^d
\]
Let $S(f(X))$ be the set of all sequences satisfying a linear recurrence with feedback polynomial $f(X)$.

Take the *projection* these sequences onto their $2d$ coordinates.

We obtain a $d$-dim subspace $S_f \subseteq \mathbb{F}_q^{2d}$ which is the kernel of the linear map $F : \mathbb{F}_q^{2d} \to \mathbb{F}_q^d$:

$$F(x_0, \cdots, x_{2d-1})_i = a_0 x_i + a_1 x_{i+1} + \cdots + a_{d-1} x_{i+d-1} + x_{i+d},$$

with matrix

$$M_F = \begin{pmatrix}
a_0 & \cdots & a_{d-1} & 1 & \cdots & \cdots & \cdots & \cdots & 0 \\
0 & a_0 & \cdots & a_{d-1} & 1 & \cdots & \cdots & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & a_0 & \cdots & a_{d-1} & 1
\end{pmatrix}$$

... but this is *exactly* the global rule of a linear CA!
Lemma

Given \( f, g \in \mathbb{F}_q[X] \) over \( \mathbb{F}_q \) of degree \( d \geq 1 \), defined as:
\[
\begin{align*}
  f(X) &= a_0 + a_1 X + \cdots + a_{d-1} X^{d-1} + X^d, \\
  g(X) &= b_0 + b_1 X + \cdots + b_{d-1} X^{d-1} + X^d,
\end{align*}
\]
Then, the kernels of \( F, G : \mathbb{F}_q^{2d} \to \mathbb{F}_q^d \) have trivial intersection if and only if \( \gcd(f, g) = 1 \)

Consequence: a family of \( t \) pairwise coprime polynomials defines a partial spread
Equivalence to $PS_{ap}$ functions for degree $b = 1$

- **Bivariate form** of the Desarguesian spread for $n = 2m$ [M16]:
  
  \[
  DS = \{ E_a \subseteq F_{2m} \times F_{2m} : a \in F_{2m} \} \cup E_\infty
  \]
  
  where:
  
  \[
  E_a = \{ (x, ax) \in F_{2m} \times F_{2m} : x \in F_{2m} \}
  \]
  
  \[
  E_\infty = \{ (0, y) \in F_{2m} \times F_{2m} : y \in F_{2m} \}
  \]

- Form of the linear map $F_i$ when $b = 1$:
  
  \[
  F_i(x_0, x_1) = a_i x_0 + x_1
  \]

- Kernel of $F_i$: $\ker(F_i) = \{ (x_0, x_1) \in F_{2m} \times F_{2m} : x_1 = a_i x_0 \} = \{ (x, a_i x) \in F_{2m} \times F_{2m} : x \in F_{2m} \} = E_{a_i} \in DS$

**Lemma**

*Our construction coincides with the class $PS_{ap}$ when $b = 1$.***
2-Rank Distributions for $n = 8$, $b = 1$

- needed: $t = 8$ pairwise coprime polynomials of deg. 1 on $\mathbb{F}_2^n$
- No need to check for $\mathcal{PS}^+$ in this case
- $\# \mathcal{PS}^-$ functions: $\binom{17}{8} = 24310$
- **2-rank**: rank of the translate design $f(x \oplus y)$

<table>
<thead>
<tr>
<th>Rank</th>
<th>#Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>510</td>
</tr>
<tr>
<td>36</td>
<td>4080</td>
</tr>
<tr>
<td>40</td>
<td>2040</td>
</tr>
<tr>
<td>42</td>
<td>17680</td>
</tr>
<tr>
<td>Total</td>
<td>24310</td>
</tr>
</tbody>
</table>

- **Main result**: verification (and extension) of Weng et al.’s counting results [W07]
2-Rank Distributions for $n = 8, b = 2$

<table>
<thead>
<tr>
<th>Type</th>
<th>Rank</th>
<th>#Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$PS^-$</td>
<td>36</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>42</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>44</td>
<td>123</td>
</tr>
<tr>
<td></td>
<td>46</td>
<td>78</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>273</td>
</tr>
<tr>
<td>$PS^+$</td>
<td>40</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>44</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>46</td>
<td>18</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>82</td>
</tr>
</tbody>
</table>

- **Ingredients**: $t = 8$ pairwise coprime polynomials of degree $b = 2$ over $\mathbb{F}_{2^2}$ ($t + 1 = 9$ for $PS^+$ functions)
- **# $PS^-$ functions**: 273
- **# $PS^+$ functions**: 82
- **1st Finding**: none of these functions is in $\mathcal{M}^\#$ ($UB_\mathcal{M} = 30$)
- **2nd Finding**: many of these functions ($\text{rank} > 42$) are not even in $\mathcal{PS}_{ap}$
Conclusions
Remarkable findings:

▶ (very convoluted) construction of bent functions via CA, Latin Squares and Hadamard matrices
▶ Simplification based on kernels of LRS subspaces
▶ Resulting bent functions coincide with $PS_{ap}$ for degree $b = 1$
▶ For $b = 2$, many functions are not in $PS_{ap}$

Open problems:

▶ Are functions stemming from polynomials of degree $b = 2$ really new?
▶ Implementation of CA-based bent functions via LFSR [ML18]
▶ Is it possible to get more functions without constraints on the constant term of the polynomials?
<table>
<thead>
<tr>
<th>Reference</th>
<th>Citation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cambridge University Press (2021)</td>
</tr>
<tr>
<td></td>
<td>1009–1023 (1993)</td>
</tr>
<tr>
<td>[GMP22]</td>
<td>M. Gadouleau, L. Mariot, S. Picek. Bent functions in the partial</td>
</tr>
<tr>
<td></td>
<td>spread class generated by linear recurring sequences. Des. Codes and</td>
</tr>
<tr>
<td></td>
<td>Cryptogr. (2022) DOI: <a href="https://doi.org/10.1007/s10623-022-01097-1">https://doi.org/10.1007/s10623-022-01097-1</a></td>
</tr>
<tr>
<td></td>
<td>IACR Cryptol. ePrint Arch. 2020: 1272 (2020)</td>
</tr>
<tr>
<td></td>
<td>orthogonal latin squares based on cellular automata. Des. Codes</td>
</tr>
<tr>
<td></td>
<td>Squares from Linear Cellular Automata. In: Exploratory papers of</td>
</tr>
<tr>
<td></td>
<td>AUTOMATA 2016 (2016)</td>
</tr>
<tr>
<td>[ML18]</td>
<td>L. Mariot, A. Leporati: A cryptographic and coding-theoretic perspective</td>
</tr>
<tr>
<td></td>
<td>Their Appl. 13(4), 1096–1116 (2007)</td>
</tr>
</tbody>
</table>

Luca Mariot  Behind the scenes of a new construction for bent functions