Correlation-immune Boolean functions and parameters of orthogonal arrays

Rebeka Kiss

Supervisor: **Dr. Gábor Péter Nagy**

University of Szeged, SZTE

19th June 2021

Motivation

- Application of Boolean functions: **Cryptography**
- The aim: Reducing the vulnerability of crypto-systems
- One of the attacks is the **Siegenthaler** attack: existence of a correlation between the output of the function and the input bits.
- Another problem: **Side Channel Attacks** (SCA): An attack based on information gained from the implementation of a computer system, for example timing information, power consumption, electromagnetic leaks or even sound.
- Defense against the Siegenthaler and Side Channel attacks with **correlation-immune functions.**

Correlation-immune functions

- An $f : \mathbb{F}_2^k \longrightarrow \mathbb{F}_2$ Boolan function is said to be **correlation immune of order** t $(1 \leq t \leq k)$ with notation **CI(t)**, if for any fixed subset of t variables the probability that, given the value of $f(x)$, the t variables have any fixed set of values is always 2^{-t}, no matter what the choice of the fixed set of t values is.

Example

The support of a **second degree CI-function** f, where $f : \mathbb{F}_2^4 \longrightarrow \mathbb{Z}_2, f(x_1, x_2, x_3, x_4) = x_1 + x_3 + x_4$:

x_1	x_2	x_3	x_4
1	0	0	0
1	1	0	0
0	0	1	0
0	1	1	0
0	0	0	1
0	1	0	1
1	0	1	1
1	1	1	1

- The question is **the minimal size of the support** (minimum-weight) of an n-variable, t-th order correlation-immune function. Let $\omega(n, t)$ denote this value.
- We can answer from another aspect: **orthogonal arrays**.
- **Supports** of t-th order correlation immune functions give **simple orthogonal arrays** with strength t when their elements are written as the rows of an array.

Orthogonal arrays

- A binary array with N rows and k columns said to be an **orthogonal array** if in every subset of the columns with t elements every binary t-tuple appears in exactly $N/2^t$ rows, where t is called the **strength** of this orthogonal array.
- Some of them have special property: in **simple orthogonal arrays** there is no repetition among the rows.

OA(8,4,2,2)

- **OA property**: every 2-tuple appears exactly twice in every 8×2 subarray.

$$
\begin{array}{cccc}
1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1
\end{array}
$$

OA(8,4,2,2)

- **OA property**: every 2-tuple appears exactly twice in every 8×2 subarray.

1	0	0	0
1	1	0	0
0	0	1	0
0	1	1	0
0	0	0	1
0	1	0	1
1	0	1	1
1	1	1	1

OA(8,4,2,2)

- **OA property**: every 2-tuple appears exactly twice in every 8×2 subarray.

1	0	0	0
1	1	0	0
0	0	1	0
0	1	1	0
0	0	0	1
0	1	0	1
1	0	1	1
1	1	1	1

OA(8,4,2,2)

- **OA property**: every 2-tuple appears exactly twice in every 8×2 subarray.

1	0	0	0
1	1	0	0
0	0	1	0
0	1	1	0
0	0	0	1
0	1	0	1
1	0	1	1
1	1	1	1

OA(8,4,2,2)

- **OA property**: every 2-tuple appears exactly twice in every 8×2 subarray.

1	0	0	0
1	1	0	0
0	0	1	0
0	1	1	0
0	0	0	1
0	1	0	1
1	0	1	1
1	1	1	1

OA(8,4,2,2)

- **OA property**: every 2-tuple appears exactly twice in every 8×2 subarray.

1	0	0	0
1	1	0	0
0	0	1	0
0	1	1	0
0	0	0	1
0	1	0	1
1	0	1	1
1	1	1	1

OA(8,4,2,2)

- **OA property**: every 2-tuple appears exactly twice in every 8×2 subarray.

1	0	0	0
1	1	0	0
0	0	1	0
0	1	1	0
0	0	0	1
0	1	0	1
1	0	1	1
1	1	1	1

Parameters of orthogonal arrays

- A problem: Does there exist an orthogonal array with given parameters k and t?
- If we know the number of columns and the strength what is **the minimal value** N for which an OA with N rows exists?
- Already for small parameters it is difficult to answer.
- Further conditions: we are looking for **simple orthogonal arrays**.

Papers about CI-functions

- **C. Carlet and S. Guilley**, Correlation-immune Boolean functions for easing counter-measures to side channel attacks.
- **C. Carlet and X. Chen**, Constructing Low-Weight dth-Order Correlation-Immune Boolean Functions Through the Fourier-Hadamard Transform.
- These papers deal thoroughly with the subject of **SCA and correlation-immune functions**.
- They contain a **table** with the **minimal size of the support** of an n -variable, d-th order correlation-immune functions.
- There were missing entries in the table.

The table

Table 2. Values $\min_{f:\mathbb{F}_2^n \to \mathbb{F}_2/d\text{-CI.}} card\,(supp(f))$

n \ d	1	2	3	4	5	6	7	8	9	10	11	12	13
1	**2**												
2	**2**	**4**											
3	**2**	**4**	**8**										
4	**2**	**8**	**8**	**16**									
5	**2**	**8**	**16**	**16**	**32**								
6	**2**	**8**	**16**	**32**	**32**	**64**							
7	**2**	**8**	**16**	**64**	**64**	**64**	**128**						
8	**2**	**12**	**16**	**64**	**128**	**128**	**128**	**256**					
9	**2**	**12**	**24**	**128**	**128**	**256**	**256**	**256**	**512**				
10	**2**	**12**	**24**	**128**	**256**	*512*	*512*	*512*	*512*	*1024*			
11	**2**	**12**	**24**	?	?	*512*	*1024*	*1024*	*1024*	*1024*	*2048*		
12	**2**	**16**	**24**	?	?	?	*1024*	*2048*	*2048*	*2048*	*2048*	*4096*	
13	**2**	**16**	*32*	?	?	?	?	*4096*	*4096*	*4096*	*4096*	*4096*	*8192*

- In case $t = 2$ and $t = 3$, there is a connection between **Hadamard matrices** and orthogonal arrays.

Theorem

Orthogonal arrays $OA(4\lambda, 4\lambda - 1, 2, 2)$ *and* $OA(8\lambda, 4\lambda, 2, 3)$ *exist if and only if there exists a* ***Hadamard matrix of order*** 4λ.

- Already in the simple case $t = 2$ arises a serious problem, a basic unsolved problem in discrete mathematics.

Hadamard Conjecture

A Hadamard matrix exists if n is $1, 2$ or a multiple of 4.

- Equivalently an $OA(4\lambda, 4\lambda - 1, 2, 2)$ and an $OA(8\lambda, 4\lambda, 2, 3)$ exist for all λ.

There is a connection between orthogonal arrays and **linear codes**.

Theorem (Delsarte, 1973)

If C is a $(k, N, d)_2$ linear code for some d with dual distance $d^\perp$ then the codewords of C form the rows of an $OA(N, k, 2, d^\perp - 1)$. Conversely the code corresponding to an $OA(N, k, 2, t)$ is a $(k, N, d)_2$ for some d with dual distance $d^\perp = t + 1$.

Claude Carlet's Conjecture

For a fixed strength t the minimal size of the support of n-variable, t-th order correlation-immune functions does not decrease when n grows.

- In other words $\omega(n, t)$ is a **non-decreasing** function in n for a fixed t value. At **NSUCRYPTO** there were included a few problems about the existence of OA-s with the following parameters:
- The case n=12, t=6 (NSUCRYPTO 2016).
- The case n=11, t=4 (NSUCRYPTO 2017).

The table with our results

We were able to fill out **all of the missing entries** of the table.

n \ d	1	2	3	4	5	6	7	8	9	10	11	12	13
1	2												
2	2	4											
3	2	4	8										
4	2	8	8	16									
5	2	8	16	16	32								
6	2	8	16	32	32	64							
7	2	8	16	64	64	64	128						
8	2	12	16	64	128	128	128	256					
9	2	12	24	128	128	256	256	256	512				
10	2	12	24	128	256	512	512	512	512	1024			
11	2	12	24	**128**	**256**	512	1024	1024	1024	1024	2048		
12	2	16	24	**128**	**256**	**768***	1024	2048	2048	2048	2048	4096	
13	2	16	32	**128***	**256**	**1024***	**1536***	4096	4096	4096	4096	4096	8192

Theorem

An $OA(N, n, 2, 2u)$ *exists if and only if an* $OA(2N, n+1, 2, 2u+1)$ *exists.*

- We used some theorems contained in the book of Hedayat, Sloane and Stufken.
- **A. S. Hedayat, N. J. A. Sloane, and J. Stufken**. Orthogonal arrays. Springer Series in Statistics. Theory and applications.
- The theorems were stated for orthogonal arrays in general, our task was to prove that they are **also true for simple orthogonal arrays.**

- We used Bulutoglu and Margot's **linear programming method**.
- For large parameters the LP method runs too long.
- Another idea: in advance we supposed that the orthogonal array has a quite small **automorphism group** and then we used the LP method.

Bulutoglu and Margot's linear programming method

- **Bulutoglu**, D. A.; **Margot**, Francois (2008): Classification of Orthogonal Arrays by Integer Programming. Carnegie Mellon University. Journal contribution. https://doi.org/10.1184/R1/6704414.v1
- We used **Python** to implement the method and the **SCIP Optimization Suite** to solve the problems.
- We partially improved the method with predetermined automorphism groups.

Thank you for your kind attention!