Hadamard Matrices, d-Linearly Independent Sets and Correlation-Immune Boolean Functions with Minimum Hamming Weights

Qichun Wang*

Abstract

It is known that correlation-immune (CI) Boolean functions used in the framework of side channel attacks need to have low Hamming weights. In 2013, Bhasin et al. studied the minimum Hamming weight of d-CI Boolean functions, and presented an open problem: the minimal weight of a d-CI function in n variables might not increase with n. Very recently, Carlet and Chen proposed some constructions of low-weight CI functions, and gave a conjecture on the minimum Hamming weight of 3-CI functions in n variables.

In this paper, we determine the values of the minimum Hamming weights of d-CI Boolean functions in n variables for infinitely many n's and give a negative answer to the open problem proposed by Bhasin et al. We then present a method to construct minimum-weight 2-CI functions through Hadamard matrices, which can provide all minimum-weight 2-CI functions in $4k-1$ variables. Furthermore, we prove that the Carlet-Chen conjecture is equivalent to the famous Hadamard conjecture. Most notably, we propose an efficient method to construct low-weight n-variable CI functions through d-linearly independent sets, which can provide numerous minimum-weight d-CI functions. Particularly, we obtain some new values of the minimum Hamming weights of d-CI functions in n variables for $n \leq 13$. We conjecture that the functions constructed by us are of the minimum Hamming weights if the sets are of absolute maximum d-linearly independent. If our conjecture holds, then all the values for $n \leq 13$ and most values for general n are determined.

Keywords: Boolean functions, Correlation-immune, Minimum-weight, Hadamard matrices, d-linearly independent sets.

MSC 2010: 94C10, 05B20, 11T71, 03E75.

*School of Computer Science and Technology, Nanjing Normal University, Nanjing, P.R.China 210046. E-mail: qcwang@fudan.edu.cn.

1 Introduction

Side-channel analysis is a very powerful technique which target implementations of block ciphers [11, 12, 15, 16]. To resist side channel attacks, many possible countermeasures have been proposed, and correlation-immune (CI) Boolean functions with low Hamming weights can be used in the framework [5, 13, 14, 19]. To reduce the cost overhead of countermeasures, one needs to construct d-CI functions with the weight as small as possible, or maximizing d for a given weight [2, 5].

In [2], Bhasin et al. studied the minimum Hamming weight of d-CI Boolean functions, and presented an open problem: the minimal weight of a d-CI function in n variables might not increase with n. In [4], Carlet and Chen proposed some constructions of low-weight CI functions, and conjectured that the minimum Hamming weight of 3-CI functions in n variables is $8\lceil\frac{n}{4}\rceil$.

In this paper, we prove that the minimum Hamming weight of 3-CI n-variable Boolean functions is lower bounded by $8\lceil\frac{n}{4}\rceil$, and then present a method to construct minimum-weight 2-CI functions through Hadamard matrices, which can provide all minimum-weight 2-CI Boolean functions in $4k-1$ variables. We thus determine the values of the minimum Hamming weights for infinitely many n's and give a negative answer to the open problem proposed by Bhasin et al. Furthermore, we prove that the Carlet-Chen conjecture is equivalent to the famous Hadamard conjecture. Most notably, we propose an efficient method to construct low-weight n-variable CI functions through d-linearly independent sets, which can provide numerous minimum-weight d-CI functions. Particularly, we obtain some new values of the minimum Hamming weights of d-CI functions in n variables for $n \leq 13$. We conjecture that the functions constructed by us are of the minimum Hamming weights if the sets are of absolute maximum d-linearly independent. If our conjecture holds, then all the values for $n \leq 13$ and most values for general n are determined.

The paper is organized as follows. In Section 2, the necessary background is established. We then study the relationship between Hadamard matrices and minimum-weight d-CI functions in Section 3. In Section 4, we study the relationship between d-linearly independent sets and low-weight d-CI functions. We end in Section 5 with conclusions.

2 Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the finite field $\mathbb{F}_2$. We denote by $\mathcal{B}_n$ the set of all n-variable Boolean functions, from $\mathbb{F}_2^n$ into $\mathbb{F}_2$.

Any Boolean function $f \in \mathcal{B}_n$ can be represented by its truth table

$$[f(0,0,\ldots,0), f(1,0,\ldots,0), f(0,1,\ldots,0), f(1,1,\ldots,0), \ldots, f(1,1,\ldots,1)].$$

Let $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$. The Hamming weight of $\mathbf{a}$, denoted by $w_H(\mathbf{a})$, is the cardinality of the set $\{1 \leq i \leq n | a_i = 1\}$.

Let $Supp(f) = \{\mathbf{x} \in \mathbb{F}_2^n | f(\mathbf{x}) = 1\}$ be the support of a Boolean function $f \in B_n$, whose cardinality $|Supp(f)|$ is called the *Hamming weight* of f, and will be denoted by $w_H(f)$. Clearly, f is determined by $Supp(f)$ uniquely. We say that f is *balanced* if $w_H(f) = 2^{n-1}$.

Let $f \in \mathcal{B}_n$. f is called correlation-immune of order d (in brief, d-CI) if and only if

$$\sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus \mathbf{v} \cdot \mathbf{x}} = 0,$$

for any $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ satisfying $1 \leq w_H(\mathbf{v}) \leq d$, where $\mathbf{v} \cdot \mathbf{x} = v_1 x_1 + \cdots + v_n x_n$ is the usual inner product [3, 6, 18, 21].

Clearly, for $\mathbf{0} \neq \mathbf{v} \in \mathbb{F}_2^n$, we have

$$\sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus \mathbf{v} \cdot \mathbf{x}} = \sum_{\mathbf{x} \in Supp(f)} (-1)^{1 \oplus \mathbf{v} \cdot \mathbf{x}} + \sum_{\mathbf{x} \notin Supp(f)} (-1)^{\mathbf{v} \cdot \mathbf{x}} = -2 \sum_{\mathbf{x} \in Supp(f)} (-1)^{\mathbf{v} \cdot \mathbf{x}}.$$

Therefore, f is d-CI if and only if

$$\sum_{\mathbf{x} \in Supp(f)} (-1)^{\mathbf{v} \cdot \mathbf{x}} = 0,$$

for any $\mathbf{v} \in \mathbb{F}_2^n$ satisfying $1 \leq w_H(\mathbf{v}) \leq d$.

A matrix H of order n is called a Hadamard matrix if $HH^T = nI_n$, where I_n is the $n \times n$ identity matrix and H^T is the transpose of H [9].

3 Hadamard matrices and minimum Hamming weights of d-CI Boolean functions

3.1 On the minimum weight of 3-CI Boolean functions

Using the same notation as that of [4], we denote the minimum Hamming weight of d-CI nonzero Boolean functions in n variables as $w_{n,d}$.

Lemma 3.1 (Proposition 2.6 of [4]). *Let d be an even integer such that $n \geq d \geq 2$. Then $w_{n+1,d+1} = 2w_{n,d}$.*

Theorem 3.2. *Let $n \geq 3$ be any integer. Then $w_{n,3} \geq 8\lceil \frac{n}{4} \rceil$. That is, $w_{n,2} \geq 4\lceil \frac{n+1}{4} \rceil$, for $n \geq 2$.*

Proof. By Lemma 3.1, it is sufficient to prove that $w_{n,2} \geq 4\lceil \frac{n+1}{4} \rceil$, for $n \geq 2$. Suppose there is an $n \geq 2$ such that $m = w_{n,2} < 4\lceil \frac{n+1}{4} \rceil$. Then there exists a 2-CI $f \in \mathcal{B}_n$ with the Hamming weight m. It is well known that $\deg(f) \leq n-2$ and m is a multiple of 4. Therefore, $m \leq 4\lceil \frac{n+1}{4} \rceil - 4 < n+1$. Let the support of f be $\{(a_{i1}, a_{i2}, \ldots, a_{in})\}$, where $1 \leq i \leq m$. Let M be the matrix

$$M = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} = [\mathbf{p}_1, \ldots, \mathbf{p}_n],$$

where $\mathbf{p}_j = (a_{1j}, a_{2j}, \ldots, a_{mj})^T$ and $1 \leq j \leq n$. Since f is 2-CI, we have $w_H(\mathbf{p}_j) = \frac{m}{2}$ and $w_H(\mathbf{p}_{j_1} \oplus \mathbf{p}_{j_2}) = \frac{m}{2}$, where $1 \leq j \leq n$ and $1 \leq j_1 < j_2 \leq n$. Therefore,

$$\mathbf{p}_{i_1}^T \mathbf{p}_{i_2} = \begin{cases} \frac{m}{2} & if\ i_1 = i_2, \\ \frac{m}{4} & otherwise. \end{cases}$$

We construct an $m \times (n+1)$ matrix H as follows.

$$H = \begin{bmatrix} 1 & (-1)^{a_{11}} & (-1)^{a_{12}} & \cdots & (-1)^{a_{1n}} \\ 1 & (-1)^{a_{21}} & (-1)^{a_{22}} & \cdots & (-1)^{a_{2n}} \\ \cdots & \cdots & \cdots & \cdots & \\ 1 & (-1)^{a_{m1}} & (-1)^{a_{m2}} & \cdots & (-1)^{a_{mn}} \end{bmatrix}.$$

Then

$$H^T H = mI,$$

where I is the identity $(n+1) \times (n+1)$ matrix. Therefore,

$$n+1 = rank(H^T H) \leq rank(H) \leq m < n+1,$$

which is a contradiction, and the result follows. □

By Theorem 3.2, if we can find a 2-CI n-variable Boolean function with the weight $4\lceil \frac{n+1}{4} \rceil$, then the values of $w_{n,2}$ and $w_{n+1,3}$ are both determined. We now give a method to construct minimum-weight 2-CI n-variable functions through Hadamard matrices, for infinitely many n's.

Construction 1: Let H be any $4k \times 4k$ Hadamard matrix. By negating columns of H, we can get a matrix whose first row is $(1, 1, \ldots, 1)$. We delete this row and denote the induced $(4k-1) \times 4k$ matrix as

$$\widetilde{H} = \begin{bmatrix} (-1)^{a_{1,1}} & (-1)^{a_{1,2}} & \cdots & (-1)^{a_{1,4k}} \\ (-1)^{a_{2,1}} & (-1)^{a_{2,2}} & \cdots & (-1)^{a_{2,4k}} \\ \cdots & \cdots & \cdots & \\ (-1)^{a_{4k-1,1}} & (-1)^{a_{4k-1,2}} & \cdots & (-1)^{a_{4k-1,4k}} \end{bmatrix},$$

where $a_{i,j} \in \mathbb{F}_2$, $1 \leq i \leq 4k-1$ and $1 \leq j \leq 4k$. Let $\mathbf{q}_j = (a_{1,j}, \ldots, a_{4k-1,j})$, where $1 \leq j \leq 4k$. Then we construct a function $f \in \mathcal{B}_{4k-1}$ whose support is $\{\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_{4k}\}$.

We give an example to illustrate the construction.

Example 1: Take the Hadamard matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{bmatrix}.$$

Negate the last column and then delete the first row, we have

$$H \to \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 \end{bmatrix}.$$

That is,

$$\widetilde{H} = \begin{bmatrix} (-1)^0 & (-1)^0 & (-1)^1 & (-1)^1 \\ (-1)^0 & (-1)^1 & (-1)^0 & (-1)^1 \\ (-1)^1 & (-1)^0 & (-1)^0 & (-1)^1 \end{bmatrix}.$$

Then the support of $f \in \mathcal{B}_3$ defined in Construction 1 is

$$\{(0,0,1), (0,1,0), (1,0,0), (1,1,1)\}.$$

Proposition 3.3. *Let H be any $4k \times 4k$ Hadamard matrix, and $f \in \mathcal{B}_{4k-1}$ be the function defined in Construction 1. Then f is a 2-CI Boolean function with the minimum Hamming weight.*

Proof. Since H is a Hadamard matrix, the rows of the induced matrix $\widetilde{H} = [(-1)^{a_{i,j}}]$ in Construction 1 are mutually orthogonal and they are all orthogonal to the vector $(1, 1, \ldots, 1)$. Let $\mathbf{p}_i = (a_{i,1}, a_{i,2}, \ldots, a_{i,4k})$, where

$1 \leq i \leq 4k-1$. Then $w_H(\mathbf{p}_i) = 2k$ and $w_H(\mathbf{p}_{i_1} \oplus \mathbf{p}_{i_2}) = 2k$, where $1 \leq i \leq 4k-1$ and $1 \leq i_1 < i_2 \leq 4k-1$. Therefore, f is 2-CI. Since $w_H(f) = 4k = 4\lceil \frac{4k-1+1}{4} \rceil$, by Theorem 3.2, f is a 2-CI Boolean function with the minimum Hamming weight. □

Corollary 3.4. *If there exists a Hadamard matrix H of order $4k$, then $w_{4k,3} = 2k$.*

In [2], Bhasin et al. presented an open problem: the minimal weight of a d-CI function in n variables might not increase with n. By Corollary 3.4, we can give a negative answer to this problem, since there are infinitely many Hadamard matrices.

3.2 Equivalence of the Hadamard and Carlet-Chen conjectures

Hadamard conjectured that there exists a Hadamard matrix of order $4k$ for every positive integer k. After more than one hundred years, this conjecture still remains open.

Conjecture 3.5 (Hadamard Conjecture)**.** *A Hadamard matrix of order $4k$ exists for every positive integer k.*

There are many results on this conjecture (see e.g. [1, 7, 8, 10, 17, 20]). The smallest order for which no Hadamard matrix has been known is 668.

In [4], based on the numerical results, Carlet and Chen proposed the following conjecture.

Conjecture 3.6 (Carlet-Chen Conjecture)**.** *Let $n \geq 3$ be any integer. Then $w_{n,3} = 8\lceil \frac{n}{4} \rceil$.*

We now prove that the above two conjectures are equivalent.

Theorem 3.7. *The Carlet-Chen conjecture is equivalent to the Hadamard conjecture.*

Proof. If the Carlet-Chen conjecture holds, then for any positive integer k, we have $w_{4k,3} = 8k$. Hence, $w_{4k-1,2} = 4k$. That is, there exists a 2-CI $f \in \mathcal{B}_{4k-1}$ with the Hamming weight $4k$. Let the support of f be $\{(a_{i,1}, a_{i,2}, \ldots, a_{i,4k-1})\}$, where $1 \leq i \leq 4k$. We construct a $4k \times 4k$ matrix

H as follows.

$$H = \begin{bmatrix} 1 & (-1)^{a_{1,1}} & (-1)^{a_{1,2}} & \cdots & (-1)^{a_{1,4k-1}} \\ 1 & (-1)^{a_{2,1}} & (-1)^{a_{2,2}} & \cdots & (-1)^{a_{2,4k-1}} \\ \cdots & \cdots & \cdots & \cdots & \\ 1 & (-1)^{a_{4k,1}} & (-1)^{a_{4k,2}} & \cdots & (-1)^{a_{4k,4k-1}} \end{bmatrix}.$$

Then $H^T H = 4kI$, where I is the identity $4k \times 4k$ matrix. That is, H^T is a Hadamard matrix of order $4k$.
Now suppose the Hadamard conjecture is correct. Then for any positive integer k, there exists a Hadamard matrix H of order $4k$. By Proposition 3.3, the function defined in Construction 1 is a 2-CI Boolean function with the Hamming weight $4k$. Therefore, $w_{4k-1,2} \leq 4k$. By Lemma 3.1 and Theorem 3.2, we have $w_{4k,3} = 8k$. For $1 \leq t \leq 3$, we have $w_{4k+t,3} \leq w_{4k+4,3} = 8(k+1)$. Then by Theorem 3.2, $8(k+1) \geq w_{4k+t,3} \geq 8\lceil \frac{4k+t}{4} \rceil = 8(k+1)$, and the result follows. □

From the proof of Theorem 3.7, for any minimum-weight 2-CI function $f \in \mathcal{B}_{4k-1}$, there always exists a Hadamard matrix of order $4k$ such that the function defined in Construction 1 is the same as f. In other words, our construction can provide all minimum-weight 2-CI Boolean functions in $4k-1$ variables.

4 d-linearly independent sets and d-CI Boolean functions with low Hamming weights

4.1 d-linearly independent sets

We now introduce the notion, d-linearly independent set, which will be used in our construction of d-CI Boolean functions with low Hamming weights.

Definition 4.1. *A subset of $\mathbb{F}_2^m$ is said to be d-linearly independent if no vector in the set can be written as a linear combination of any other $d-1$ vectors in the set.*

Definition 4.2. *A subset S of $\mathbb{F}_2^m$ with k vectors is set to be a relative maximum d-linearly independent set if S is not a subset of any d-linearly independent set of $\mathbb{F}_2^m$ with $k+1$ vectors.*

Clearly, any d-linearly independent set can be extended to a relative maximum d-linearly independent set, and the rank of a relative maximum d-linearly independent set is m.

Definition 4.3. *A subset of $\mathbb{F}_2^m$ with k vectors is set to be an absolute maximum d-linearly independent set if there is no d-linearly independent set of $\mathbb{F}_2^m$ with $k+1$ vectors. We denote this maximum value k as $v_{m,d}$.*

It is easy to see that $v_{m,2} = 2^m - 1$ and $v_{m,d_1} \geq v_{m,d_2}$ for $d_1 < d_2$. We now determine other values of $v_{m,d}$.

Proposition 4.4. *The cardinality of an absolute maximum 3-linearly independent set of $\mathbb{F}_2^m$ is 2^{m-1}. That is, $v_{m,3} = 2^{m-1}$.*

Proof. Suppose there exists a 3-linearly independent set $\{\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_{2^{m-1}+1}\} \subset \mathbb{F}_2^m$. Then we construct a set

$$T = \{\mathbf{p}_i,\ 1 \leq i \leq 2^{m-1}+1\} \bigcup \{\mathbf{p}_1 + \mathbf{p}_j,\ 2 \leq j \leq 2^{m-1}+1\}.$$

Clearly, the cardinality of the set T is $2^{m-1} + 1 + 2^{m-1} > 2^m$, which is contradictory to the fact that T is a subset of $\mathbb{F}_2^m$. Therefore, $v_{m,3} \leq 2^{m-1}$. Clearly, the set

$$S = \{\mathbf{p} \in \mathbb{F}_2^m | w_H(\mathbf{p}) \textit{ is odd}\}$$

is a 3-linearly independent set with 2^{m-1} vectors, and the result follows. □

Proposition 4.5. *For $m \geq 5$ and $d \geq \frac{2m+2}{3}$, the cardinality of an absolute maximum d-linearly independent set of $\mathbb{F}_2^m$ is $m+1$. That is, $v_{m,d} = m+1$, for $d \geq \frac{2m+2}{3}$.*

Proof. Let $S = \{\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_t\} \subset \mathbb{F}_2^m$ be any absolute maximum d-linearly independent set. Take a basis of S, say $\{\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_m\}$. Then any vector in S can be written as a linear combination of the basis vectors. We have

$$\begin{bmatrix} \mathbf{p}_1 \\ \mathbf{p}_2 \\ \cdots \\ \mathbf{p}_m \\ \mathbf{p}_{m+1} \\ \cdots \\ \mathbf{p}_t \end{bmatrix} = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \ldots & 1 \\ c_{m+1,1} & c_{m+1,2} & \ldots & c_{m+1,m} \\ \cdots & \cdots & \cdots & \cdots \\ c_{t,1} & c_{t,2} & \ldots & c_{t,m} \end{bmatrix} \begin{bmatrix} \mathbf{p}_1 \\ \mathbf{p}_2 \\ \cdots \\ \mathbf{p}_m \end{bmatrix},$$

where $(c_{i,1}, c_{i,2}, \ldots, c_{i,m}) \in \mathbb{F}_2^m$, for $m+1 \leq i \leq t$. Therefore,

$$T = \{(1,0,\ldots,0), \ldots, (0,0,\ldots,1), (c_{m+1,1}, \ldots, c_{m+1,m}), \ldots, (c_{t,1}, \ldots, c_{t,m})\}$$

is an absolute maximum d-linearly independent set. Since $d \geq \frac{2m+2}{3}$, there is no vector $\mathbf{q} \in T$ with $1 < w_H(\mathbf{q}) < \frac{2m+2}{3}$. Moreover, there do not exist two

Table 1: The values of $v_{m,d}$

d \ m	3	4	5	6	7	8	9
2	7	15	31	63	127	255	511
3	4	8	16	32	64	128	256
4		5	6	8	11	13	15
5			6	7	9	12	14
6				7	8	9	12
7					8	9	10

different vectors $\mathbf{q}_1, \mathbf{q}_2 \in T$ such that $w_H(\mathbf{q}_1) \geq \frac{2m+2}{3}$ and $w_H(\mathbf{q}_2) \geq \frac{2m+2}{3}$. Otherwise, $\mathbf{q}_1 \oplus \mathbf{q}_2$ is of the Hamming weight

$$\leq \frac{2m-4}{3} = \frac{2m+2}{3} - 2$$

and it can be written as a linear combination of other $\frac{2m+2}{3} - 2$ vectors in T. Therefore, the cardinality of T is at most $m+1$. Clearly, the set

$$S = \{\mathbf{p} \in \mathbb{F}_2^m | w_H(\mathbf{p}) = 1 \ or \ m\}$$

is a d-linearly independent set with $m+1$ vectors, and the result follows. □

If m is small, it is quite easy to determine the values of $v_{m,d}$. In Table 1, we list all the values of $v_{m,d}$, for $m \leq 9$.

4.2 An efficient method to construct d-CI Boolean functions with low Hamming weights

We now give a method to construct low-weight d-CI n-variable functions through d-linearly independent sets.

Construction 2: Let $S = \{\mathbf{u}_1, \ldots, \mathbf{u}_k\} \subset \mathbb{F}_2^m$ be a d-linearly independent set. Let $l_j \in \mathcal{B}_m$ be the linear function $\mathbf{u}_j \cdot \mathbf{x}$, where $\mathbf{x} \in \mathbb{F}_2^m$ and "$\cdot$" is the usual inner product. The truth table of l_j is denoted by the column vector $\mathbf{p}_j = (a_{1,j}, a_{2,j}, \ldots, a_{2^m,j})^T$. Let

$$M = [\mathbf{p_1}, \ldots, \mathbf{p}_k] = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,k} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,k} \\ \cdots & \cdots & \cdots & \cdots \\ a_{2^m,1} & a_{2^m,2} & \cdots & a_{2^m,k} \end{bmatrix} = \begin{bmatrix} \mathbf{q}_1 \\ \mathbf{q}_2 \\ \cdots \\ \mathbf{q}_{2^m} \end{bmatrix},$$

where $\mathbf{q}_i \in \mathbb{F}_2^k$ and $1 \le i \le 2^m$. Then we construct a function $f \in \mathcal{B}_k$ whose support is $\{\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_{2^m}\}$.

We give an example to illustrate the construction.

Example 2: Take $m = 7$ and

$$\begin{aligned} S = &\{(1,0,0,0,0,0,0),(0,1,0,0,0,0,0),(0,0,1,0,0,0,0),(0,0,0,1,0,0,0),\\ &(0,0,0,0,1,0,0),(0,0,0,0,0,1,0),(0,0,0,0,0,0,1),(1,1,1,1,0,0,0),\\ &(1,1,0,0,1,1,0),(1,0,1,0,1,0,1),(1,1,1,1,1,1,1)\}. \end{aligned}$$

Clearly, S is a 4-linearly independent set with 11 vectors. We have

$$\begin{aligned} &l_1 = x_1,\ l_2 = x_2,\ l_3 = x_3,\ l_4 = x_4,\ l_5 = x_5,\ l_6 = x_6,\ l_7 = x_7,\\ &l_8 = x_1 \oplus x_2 \oplus x_3 \oplus x_4,\ l_9 = x_1 \oplus x_2 \oplus x_5 \oplus x_6,\\ &l_{10} = x_1 \oplus x_3 \oplus x_5 \oplus x_7,\ l_{11} = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7. \end{aligned}$$

Then we can get the function $f \in \mathcal{B}_{11}$ by Construction 2 with the support

$$\begin{aligned} &\{(0,0,0,0,0,0,0,0,0,0,0),(1,0,0,0,0,0,0,0,0,0,0),(0,1,0,0,0,0,0,0,0,0,0),\\ &(1,1,0,0,0,0,0,0,0,0,0),\ldots,(0,1,1,1,1,1,1,1,1,1,0),(1,1,1,1,1,1,1,0,0,0,0)\} \end{aligned}$$

It is easy to check that f is a 4-CI Boolean function with the Hamming weight 128. Therefore, $w_{11,4} \le 128$. Since $w_{11,4} \ge w_{10,4} = 128$, we have $w_{11,4} = 128$. This is a previously unknown value, thus a triple question mark ??? in Table II of [4] can be taken place by it.

Proposition 4.6. *Let $f \in \mathcal{B}_k$ be the function defined in Construction 2. Then f is a d-CI Boolean function with the Hamming weight 2^m.*

Proof. Clearly, f is d-CI if and only if

$$\sum_{\mathbf{x} \in Supp(f)} (-1)^{\mathbf{v}\cdot\mathbf{x}} = 0,$$

for any $\mathbf{v} = (v_1, \ldots, v_k) \in \mathbb{F}_2^k$ satisfying $1 \le w_H(\mathbf{v}) \le d$. That is, $w_H(v_1\mathbf{p_1} \oplus \ldots \oplus v_k\mathbf{p_k}) = 2^{m-1}$, for any $\mathbf{v} \in \mathbb{F}_2^k$ with $1 \le w_H(\mathbf{v}) \le d$. Since S is a d-linearly independent set, for any $\mathbf{v} \in \mathbb{F}_2^k$ with $1 \le w_H(\mathbf{v}) \le d$, we have $v_1\mathbf{u}_1 + \ldots + v_k\mathbf{u}_k \ne \mathbf{0}$. Therefore,

$$v_1 l_1 \oplus \ldots \oplus v_k l_k = (v_1\mathbf{u}_1 + \ldots + v_k\mathbf{u}_k) \cdot \mathbf{x}$$

is a balanced function, and the result follows. □

Table 2: The values of $w_{n,d}$

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

Theorem 4.7. *Let $v_{m,d}$ be the cardinality of the absolute maximum d-linearly independent set of $\mathbb{F}_2^m$. Then*

$$w_{v_{m,d},d} \leq 2^m.$$

Proof. Let $S = \{\mathbf{u}_1, \ldots, \mathbf{u}_k\} \subset \mathbb{F}_2^m$ be an absolute maximum d-linearly independent set. Then $k = v_{m,d}$. By Construction 2, we can generate a function $f \in \mathcal{B}_{v_{m,d}}$. By Proposition 4.6, f is a d-CI Boolean function with the Hamming weight 2^m. Therefore,

$$w_{v_{m,d},d} \leq 2^m.$$

□

For $n \leq 13$, there are 8 unknown values of $w_{n,d}$ (see Table II of [4]). By Theorem 4.7 and Table 1, we can determine the exact values for half of them. That is, $w_{11,4} = 128$, $w_{12,5} = 256$, $w_{12,6} = 512$ and $w_{13,7} = 1024$. For other four unknown values, Theorem 4.7 provides an upper bound. In Table 2, we list the values of $w_{n,d}$ for $n \leq 13$. All values for $n \leq 10$ can be determined by the SMT tool [2], and those entries in *italic* are new values obtained by [2, 4]. Those entries in **bold** are new values obtained by us. A question mark ? indicates that the value is the upper bound deduced from

Theorem 4.7. In Appendix A, we give an example of the 12-variable 6-CI Boolean function with the minimum Hamming weight.

By computing $v_{m,d}$ and $w_{v_{m,d},d}$, for small m and d, we find that $w_{v_{m,d},d} = 2^m$ always holds. So we propose the following conjecture.

Conjecture 4.8. *Let $v_{m,d}$ be the cardinality of the absolute maximum d-linearly independent set of $\mathbb{F}_2^m$. Then*

$$w_{v_{m,d},d} = 2^m.$$

It is noted that if Conjecture 4.8 holds, then all the values of $w_{n,d}$ for $n \leq 13$ and most values for general n are determined. Moreover, the functions generated by Construction 2 using absolute maximum d-linearly independent sets are minimum-weight d-CI Boolean functions. Anyway, given an absolute maximum d-linearly independent set S, Construction 2 can provide a d-CI Boolean function with low weight. That is, we have transformed the problem of finding low-weight correlation-immune Boolean functions to the problem of finding absolute maximum d-linearly independent sets, which can be done very efficient.

5 Conclusion

In this paper, we studied the relationships between Hadamard matrices, d-linearly independent sets and correlation-immune Boolean functions with minimum Hamming weights. We proposed two constructions of minimum-weight d-CI Boolean functions, and deduced some quite interesting results. The field is still open and there are many problems deserved to be studied.

Acknowledgment

The author would like to thank the financial support from the National Natural Science Foundation of China (Grant 61572189).

References

[1] L. Baumert, S. W. Golomb and M. J. Hall, "Discovery of an Hadamard Matrix of Order 92," *Bulletin of the American Mathematical Society* 68:3 (1962), 237–238.

[2] S. Bhasin, C. Carlet and S. Guilley, "Theory of masking with codewords in hardware: low-weight dth-order correlation-immune Boolean functions," IACR Cryptology ePrint Archive, Report 2013/303, 2013.

[3] C. Carlet, "Boolean Functions for Cryptography and Error Correcting Codes," Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering", Cambridge University Press, pp. 257–397, 2010. Available: http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.

[4] C. Carlet and X. Chen, "Constructing low-weight dth-order correlation-immune Boolean functions through the Fourier-Hadamard transform," to appear in *IEEE Trans. Inform. Theory.*

[5] C. Carlet and S. Guilley, "Side-channel indistinguishability," *Proceedings of HASP 13*, 2nd International Workshop on Hardware and Architectural Support for Security and Privacy, 2013, pp. 9:1–9:8.

[6] T. W. Cusick and P. Stănică, *Cryptographic Boolean Functions and Applications* (2nd ed.), Elsevier–Academic Press, 2017.

[7] D. Z. Djokovic, "Hadamard matrices of order 764 exist," *Combinatorica* 28:4 (2008), 487–489.

[8] S. Georgiou, C. Koukouvinos and J. Seberry, "Hadamard matrices, orthogonal designs and construction algorithms," *Designs* 563 (2003), 133–205.

[9] J. Hadamard, "Résolution d'une question relative aux déterminants," *Bull. Sci. Math.* 17 (1893), 240–246.

[10] H. Kharaghani and B. Tayfeh-Rezaie, "A Hadamard matrix of order 428," *Journal of Combinatorial Designs* 13:6 (2005), 435–440.

[11] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," *Advances in Cryptology–CRYPTO 96* , LNCS 1109, Springer–Verlag, 1996, pp. 104–113.

[12] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," *Advances in Cryptology–CRYPTO 99* , LNCS 1666, Springer–Verlag, 1999, pp. 388–397.

[13] S. Mangard, N. Pramstaller and E. Oswald, "Successfully attacking masked AES hardware implementations," *Cryptographic Hardware*

and Embedded Systems C CHES 2005, LNCS 3659, Springer–Verlag, 2005, pp. 157–171.

[14] S. Mangard, E. Oswald and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)*, Springer-Verlag New York, 2007.

[15] B. Mazumdar, D. Mukhopadhyay and I. Sengupta, "Constrained Search for a Class of Good Bijective S-Boxes with Improved DPA Resistivity," *IEEE Trans. Inform. Forensics and Security* 8:12 (2013), 2154–2163.

[16] S. Picek, K. Papagiannopoulos, B. Ege, L. Batina and D. Jakobovic, "Confused by Confusion: Systematic Evaluation of DPA Resistance of Various S-boxes," *Progress in Cryptology – INDOCRYPT* 2014, LNCS 8885, Springer–Verlag, 2014, pp. 374–390.

[17] B. Schmidt, "Cyclotomic integers and finite geometry," *Journal of the American Mathematical Society* 12:4 (1999), 929–952.

[18] T. Siegenthaler, "Correlation immunity of Nonlinear Combining Functions for Cryptographic Applications," *IEEE Trans. Inform. Theory* 30:5 (1984), pp. 776–780.

[19] E. Trichina, D. D. Seta and L. Germani, "Simplified adaptive multiplicative masking for AES," *Cryptographic Hardware and Embedded Systems C CHES 2002*, LNCS 2523, Springer–Verlag, 2002, pp. 187–197.

[20] J. S. Wallis, "On the existence of Hadamard matrices," *J. Combinat. Theory A.* 21:2 (1976) 188–195.

[21] G. Z. Xiao and J. L. Massey, "A spectral characterization of correlation-immune combining functions," *IEEE Trans. Inform. Theory* 34:3 (1988), pp. 569–571.

A A 12-variable 6-CI Boolean function with the minimum Hamming weight

Take $m = 9$ and

$$\begin{aligned} S =\{&(1,0,0,0,0,0,0,0,0),(0,1,0,0,0,0,0,0,0),(0,0,1,0,0,0,0,0,0),\\ &(0,0,0,1,0,0,0,0,0),(0,0,0,0,1,0,0,0,0),(0,0,0,0,0,1,0,0,0),\\ &(0,0,0,0,0,0,1,0,0),(0,0,0,0,0,0,0,1,0),(0,0,0,0,0,0,0,0,1),\\ &(1,1,1,1,1,1,0,0,0),(1,1,1,0,0,0,1,1,1),(0,0,0,1,1,1,1,1,1)\}. \end{aligned}$$

Clearly, S is a 6-linearly independent set with 12 vectors. We have

$$\begin{aligned} &l_1 = x_1,\ l_2 = x_2,\ l_3 = x_3,\ l_4 = x_4,\ l_5 = x_5,\ l_6 = x_6,\ l_7 = x_7,\\ &l_8 = x_8,\ l_9 = x_9,\ l_{10} = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6,\\ &l_{11} = x_1 \oplus x_2 \oplus x_3 \oplus x_7 \oplus x_8 \oplus x_9,\ l_{12} = x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus x_9. \end{aligned}$$

Then a function $f \in \mathcal{B}_{12}$ is defined by Construction 2. It is easy to check that f is a 6-CI Boolean function with the minimum Hamming weight 512.