Designs, Codes and Cryptography (2019) 87:2321–2333
https://doi.org/10.1007/s10623-019-00620-1

Hadamard matrices, d-linearly independent sets and correlation-immune Boolean functions with minimum Hamming weights

Qichun Wang[1]

Received: 25 September 2018 / Revised: 22 December 2018 / Accepted: 6 February 2019 /
Published online: 20 February 2019

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 this paper, we study minimum Hamming weights of 3-CI Boolean functions, and prove that the Carlet-Chen conjecture is equivalent to the famous Hadamard conjecture. Moreover, we propose a 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 $n \leq 13$.

Keywords Boolean functions · Correlation-immune · Minimum-weight · Hadamard matrices · d-Linearly independent sets

Mathematics Subject Classification 94C10, 05B20, 11T71, 03E75

1 Introduction

Side-channel analysis is a very powerful technique which target implementations of block ciphers [12,13,16,17]. 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 [6,14,15,20]. 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 [2,6].

Very recently, 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 $8\lceil \frac{n}{4} \rceil$ [5].

Communicated by K. T. Arasu.

✉ Qichun Wang
qcwang@fudan.edu.cn

[1] School of Computer Science and Technology, Nanjing Normal University, Nanjing 210046, People's Republic of China

In this paper, we study minimum Hamming weights of 3-CI Boolean functions, and prove that the Carlet-Chen conjecture is equivalent to the famous Hadamard conjecture. Moreover, we propose a 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 $n \leq 13$.

The paper is organized as follows. In Sect. 2, the necessary background is established. We then study the relationship between Hadamard matrices and minimum-weight d-CI functions in Sect. 3. In Sect. 4, we study the relationship between d-linearly independent sets and low-weight d-CI functions. We end in Sect. 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 [4,7,19,22].

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 [10].

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 [5], 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 [5]) *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 $w_{n,3} \geq 8\lceil \frac{n}{4} \rceil$.*

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

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 $1 \le i \le 4k-1$. Then $w_H(\mathbf{p}_i) = 2k$ and $w_H(\mathbf{p}_{i_1} \oplus \mathbf{p}_{i_2}) = 2k$, where $1 \le i \le 4k-1$ and $1 \le i_1 < i_2 \le 4k-1$. 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. □

It is noted that we can construct a 3-CI n-variable Boolean function with the minimum Hamming weight easily from a 2-CI $(n-1)$-variable Boolean function with the minimum Hamming weight.

Corollary 3.4 *If there exists a Hadamard matrix H of order $4k$, then $w_{4k,3} = 8k$.*

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. [1,8,9,11,18,21]). The smallest order for which no Hadamard matrix has been known is 668.

In [5], based on the numerical results, Carlet and Chen proposed the following conjecture.

Conjecture 3.6 (Carlet-Chen Conjecture) *Let $n \ge 3$ 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 $1 \le i \le 4k$. 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, $w_{4k-1,2} \le 4k$. By Lemma 3.1 and Theorem 3.2, we have $w_{4k,3} = 8k$. For $1 \le t \le 3$, we have $w_{4k+t,3} \le w_{4k+4,3} = 8(k+1)$. Then by Theorem 3.2, $8(k+1) \ge w_{4k+t,3} \ge 8\lceil \frac{4k+t}{4} \rceil = 8(k+1)$, 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. That is, for any different vectors $\alpha_1, \alpha_2, \ldots, \alpha_d$ of this set, there do not exist $c_1, \ldots, c_d \in \mathbb{F}_2$ such that $\sum_{i=1}^{d} c_i \alpha_i = 0$.

Definition 4.2 A subset S of $\mathbb{F}_2^m$ with k vectors is said 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 said 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 $v_{m,d_1} \ge v_{m,d_2}$ 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

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

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, $v_{m,3} \le 2^{m-1}$. Clearly, the set

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

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

Proposition 4.5 *For $m \ge 5$ and $d \ge \frac{2m+2}{3}$, 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 $d \ge \frac{2m+2}{3}$.*

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

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

where $(c_{i,1}, c_{i,2}, \ldots, c_{i,m}) \in \mathbb{F}_2^m$, for $m+1 \le i \le t$. 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 $d \ge \frac{2m+2}{3}$, there is no vector $\mathbf{q} \in T$ with $1 < w_H(\mathbf{q}) < \frac{2m+2}{3}$. Moreover, there do not exist two different vectors $\mathbf{q}_1, \mathbf{q}_2 \in T$ such that $w_H(\mathbf{q}_1) \ge \frac{2m+2}{3}$ and $w_H(\mathbf{q}_2) \ge \frac{2m+2}{3}$. Otherwise, $\mathbf{q}_1 \oplus \mathbf{q}_2$ is of the Hamming weight

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

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 $m \le 9$.

4.2 An algorithm for finding relative maximum *d*-linearly independent sets

Let $S \subset \mathbb{F}_2^m$ be any relative maximum d-linearly independent set. Then S is of rank m, and there is a linear transformation over $\mathbb{F}_2^m$ which maps S onto a set T containing m unit vectors. Clearly, T is also a relative maximum d-linearly independent set. Moreover, the

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	11
7					8	9	10

inverse transformation maps T onto S. Hence, without loss of generality, we only need to study how to find relative maximum d-linearly independent sets from the set of unit vectors $U = \{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$, where $\mathbf{u}_i$ is the unit vector whose i-th coordinate is 1, for $1 \leq i \leq m$.

Let $\mathbf{u} = (u_1, u_2, \ldots, u_m) \in \mathbb{F}_2^m$. We use $|\mathbf{u}|$ to denote the number $u_1+2u_2+\ldots+2^{m-1}u_m$, and provide an algorithm as follows.

An algorithm for finding relative maximum d-linearly independent sets:

1. Start with the set of unit vectors $U = \{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ and $i = d$.
2. Consider $\mathbf{u} \in \mathbb{F}_2^m$ satisfying $wt(\mathbf{u}) = i$ which are sorted by $|\mathbf{u}|$ in ascending size.
   a. If $\mathbf{u}$ cannot be written as a linear combination of $d-1$ vectors in U, update U to $U \cup \{\mathbf{u}\}$;
   b. If $|\mathbf{u}| = 2^m - 2^{m-i}$, update i to $i+1$.
   c. If $i > m$, goto step 3.
3. Output the set U.

In the algorithm, we sort $\mathbf{u}$ with the same weight by $|\mathbf{u}|$ in ascending size, and the last $\mathbf{u}$ satisfying $wt(\mathbf{u}) = i$ is $(0, \ldots, 0, 1, \ldots, 1)$ with $|\mathbf{u}| = 2^m - 2^{m-i}$. The algorithm is simple and even can be done by hand, which can be seen from the following example.

Example 1 Let $m = 7$ and $d = 4$. Then the set of unit vectors is

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

Consider vectors of weight 4. We can find the following four vectors one by one:

$$(1,1,1,1,0,0,0), (1,1,0,0,1,1,0), (1,0,1,0,1,0,1), (0,0,0,1,1,1,1),$$

and U is updated to the set with eleven vectors. Clearly, any vector of weight greater than 4 can be written as a linear combination of three vectors in U. Therefore, a relative maximum 4-linearly independent set with 11 vectors has been found (it is in fact an absolute maximum 4-linearly independent set).

Remark 1 It seems that the above algorithm always generates an absolute maximum d-linearly independent set, but we cannot prove it, which we leave as an open problem.

4.3 Constructing *d*-CI Boolean functions with low weights through relative maximum *d*-linearly independent sets

We now give a method to construct low-weight d-CI n-variable functions through relative maximum d-linearly independent sets (a similar method was used in Sect. V of [3]).

Construction 2 Let $S = \{\mathbf{u}_1, \ldots, \mathbf{u}_k\} \subset \mathbb{F}_2^m$ be a relative maximum 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 $m = 10$ and $d = 6$. Using the above algorithm, we can generate the following relative maximum 6-linearly independent set by hand quite easily.

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

In fact, S is an absolute maximum 6-linearly independent set. We have

$$\begin{aligned} &l_1 = x_1,\ l_2 = x_2,\ l_3 = x_3,\ l_4 = x_4,\ l_5 = x_5,\ l_6 = x_6,\ l_7 = x_7,\ l_8 = x_8 \\ &l_9 = x_9, l_{10} = x_{10},\ l_{11} = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6, \\ &l_{12} = x_1 \oplus x_2 \oplus x_3 \oplus x_7 \oplus x_8 \oplus x_9,\ l_{13} = x_1 \oplus x_4 \oplus x_5 \oplus x_7 \oplus x_8 \oplus x_{10}. \end{aligned}$$

Then we can get the function $f \in \mathcal{B}_{13}$ by Construction 2 with the support

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

It is easy to check that f is a 6-CI Boolean function with the Hamming weight 1024. Therefore, $w_{13,6} \le 1024$. Since $w_{13,6} \ge 1024$ (the lower bound was obtained by the Delsarte LP algorithm, see TABLE I of [5]), we have $w_{13,6} = 1024$. This is a previously unknown value, thus a triple question mark ??? in Table II of [5] 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 Since S is a relative maximum d-linearly independent set, it is of rank m and $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_{2^m}$ are different vectors. Therefore, f is a well-defined Boolean function with the Hamming weight 2^m. Clearly, f is d-CI if and only if

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	$\leq$**256**	**256**	$\leq$**1024**	1024	2048
13	2	16	32	$\leq$**256**	$\leq$**512**	**1024**	$\leq$**2048**	4096

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

for any $\mathbf{v} = (v_1, \ldots, v_k) \in \mathbb{F}_2^k$ satisfying $1 \leq w_H(\mathbf{v}) \leq d$. 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 $1 \leq w_H(\mathbf{v}) \leq d$. Since S is d-linearly independent, for any $\mathbf{v} \in \mathbb{F}_2^k$ with $1 \leq w_H(\mathbf{v}) \leq d$, we have $v_1\mathbf{u}_1 + \ldots + v_k\mathbf{u}_k \neq \mathbf{0}$. 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. □

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 [5]). By Theorem 4.7 and Table 1, we can determine the exact values for three of them. That is, $w_{11,4} = 128$, $w_{12,5} = 256$ and $w_{13,6} = 1024$. For other 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 [2,5]. Those entries in **bold** are new values obtained by us.

The number of rows of an orthogonal array can be lower bounded by the Delsarte LP bound, and the bounds were given in Table 1 of [2]. In Appendix 1, we deduce exact values for some orthogonal arrays and give some results on the maximum number of orthogonal vectors in $\mathbb{F}_2^n$. Based on the result of Appendix 1 and Theorem 4.7, we have $w_{11,4} = 128$. Then in Appendix 1, we give an 11-variable 4-CI Boolean function with the minimum Hamming weight. □

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. The field is still open and there are many problems deserved to be studied. We hope that our work would attract more researchers to be interested in this interesting topic.

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

Appendix A: Some results on the maximum number of orthogonal vectors in $\mathbb{F}_2^n$

A group of vectors in $\mathbb{F}_2^n$ are said to be d-orthogonal if any m vectors of them are orthogonal, for $1 \le m \le d$. We use $OA_{n,d}$ to denote the maximum number of d-orthogonal vectors in $\mathbb{F}_2^n$. Let $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_m$ be d-orthogonal row vectors and M be the matrix $[\mathbf{p}_1^T, \mathbf{p}_2^T, \ldots, \mathbf{p}_m^T]$. Clearly, if we negate any columns or exchange any rows of M, then the columns of the induced matrix are still d-orthogonal.

Let $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_m$ be 4-orthogonal column vectors and $M = [\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_m]$. Clearly, by exchanging rows, the first four columns of M can be transformed to the following vectors one by one:

$$\mathbf{q}_1 = \left(\mathbf{0}_{\frac{n}{2}}, \mathbf{1}_{\frac{n}{2}}\right)^T,$$

$$\mathbf{q}_2 = \left(\mathbf{0}_{\frac{n}{4}}, \mathbf{1}_{\frac{n}{4}}, \mathbf{0}_{\frac{n}{4}}, \mathbf{1}_{\frac{n}{4}}\right)^T,$$

$$\mathbf{q}_3 = \left(\mathbf{0}_{\frac{n}{8}}, \mathbf{1}_{\frac{n}{8}}, \mathbf{0}_{\frac{n}{8}}, \mathbf{1}_{\frac{n}{8}}, \mathbf{0}_{\frac{n}{8}}, \mathbf{1}_{\frac{n}{8}}, \mathbf{0}_{\frac{n}{8}}, \mathbf{1}_{\frac{n}{8}}\right)^T,$$

$$\mathbf{q}_4 = \left(\mathbf{0}_{\frac{n}{16}}, \mathbf{1}_{\frac{n}{16}}, \mathbf{0}_{\frac{n}{16}}, \mathbf{1}_{\frac{n}{16}}, \mathbf{0}_{\frac{n}{16}}, \mathbf{1}_{\frac{n}{16}}, \mathbf{0}_{\frac{n}{16}}, \mathbf{1}_{\frac{n}{16}}, \mathbf{0}_{\frac{n}{16}}, \mathbf{1}_{\frac{n}{16}}, \mathbf{0}_{\frac{n}{16}}, \mathbf{1}_{\frac{n}{16}}, \mathbf{0}_{\frac{n}{16}}, \mathbf{1}_{\frac{n}{16}}, \mathbf{0}_{\frac{n}{16}}, \mathbf{1}_{\frac{n}{16}}\right)^T,$$

where $\mathbf{0}_i = (0, \ldots, 0)$ and $\mathbf{1}_i = (1, \ldots, 1) \in \mathbb{F}_2^i$. Let $\mathbf{q}_5 = [\alpha_1, \ldots, \alpha_8]^T$, where $\alpha_j \in \mathbb{F}_2^{n/8}$. Suppose $\mathbf{q}_1, \mathbf{q}_2, \mathbf{q}_3, \mathbf{q}_4$ and $\mathbf{q}_5$ are 4-orthogonal. Clearly, $\alpha_1, \ldots, \alpha_8$ must be balanced vectors, since $\mathbf{q}_1, \mathbf{q}_2, \mathbf{q}_3$ and $\mathbf{q}_5$ are 4-orthogonal. Let $\mathbf{q}_4 = [\beta_1, \ldots, \beta_8]^T$ and x_i be the Hamming weight of $\alpha_i \oplus \beta_i$, where $1 \le i \le 8$. Since $\mathbf{q}_5 \oplus \mathbf{q}_4 \oplus c_1\mathbf{q}_1 \oplus c_2\mathbf{q}_2 \oplus c_3\mathbf{q}_3$ is balanced for $(c_1, c_2, c_3) \in \mathbb{F}_2^3$ and $wt(c_1, c_2, c_3) \le 2$, we have

$$\begin{cases} x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 = \frac{n}{2} \\ x_1 + x_2 + x_3 + x_4 - x_5 - x_6 - x_7 - x_8 = 0 \\ x_1 + x_2 - x_3 - x_4 + x_5 + x_6 - x_7 - x_8 = 0 \\ x_1 - x_2 + x_3 - x_4 + x_5 - x_6 + x_7 - x_8 = 0 \\ x_1 + x_2 - x_3 - x_4 - x_5 - x_6 + x_7 + x_8 = 0 \\ x_1 - x_2 + x_3 - x_4 - x_5 + x_6 - x_7 + x_8 = 0 \\ x_1 - x_2 - x_3 + x_4 + x_5 - x_6 - x_7 + x_8 = 0. \end{cases}$$

Therefore,

$$(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) = \left(C, \frac{n}{8} - C, \frac{n}{8} - C, C, \frac{n}{8} - C, C, C, \frac{n}{8} - C\right), \quad (1)$$

where $0 \le C \le \frac{n}{8}$.

Take $n = 48$. Then by exchanging rows or negating the column, $\mathbf{q}_5$ can be transformed to $(\gamma_1, \gamma_2, \gamma_2, \gamma_1, \gamma_2, \gamma_1, \gamma_1, \gamma_2)$, where (γ_1, γ_2) is

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

If $(\gamma_1, \gamma_2) = (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$, then there is no $\mathbf{q}_6 = (\theta_1, \ldots, \theta_8)$ such that $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_6$ are 4-orthogonal. Otherwise, $\theta_1, \ldots, \theta_8$ must be balanced vectors and

$$wt(\theta_1 \oplus \beta_1) + wt(\theta_2 \oplus \beta_2) + wt(\theta_1 \oplus \gamma_1) + wt(\theta_2 \oplus \gamma_2) = 6 + 6 = 2wt(\theta_1 \oplus \beta_1) + 6.$$

That is, $wt(\theta_1 \oplus \beta_1) = 3$, which is contradictory to the fact that θ_1 and β_1 are balanced vectors.

Now consider the case $(\gamma_1, \gamma_2) = (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$. Suppose $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_6$ are 4-orthogonal. Then $\mathbf{q}_6$ can be transformed to $(\theta_1, \ldots, \theta_8)$, where

$$\theta_1, \theta_4, \theta_6, \theta_7 \in \{(0, 0, 1, 1, 0, 1), (0, 1, 0, 0, 1, 1)\}, \theta_2 = \theta_3 = \theta_5 = \theta_8 = (1, 1, 0, 0, 1, 0),$$

or

$$\theta_2, \theta_3, \theta_5, \theta_8 \in \{(0, 0, 1, 1, 1, 0), (1, 0, 0, 0, 1, 1)\}, \theta_1 = \theta_4 = \theta_6 = \theta_7 = (1, 0, 1, 0, 1, 0).$$

It is easy to verify that all these 32 vectors are not 4-orthogonal with $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_5$. Therefore, $OA_{48,4} = 5$, which seems to be a previously unknown value. Hence, the minimum number of rows w of an orthogonal array $OA(w, 7, 2, 4)$ is 64, which was known to be ≥ 48 (see Table 1 of [2]).

Now consider $n = 80$. Suppose $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_6$ are 4-orthogonal. Then $\mathbf{q}_5$ can be transformed to $(\alpha_1, \alpha_2, \alpha_2, \alpha_1, \alpha_2, \alpha_1, \alpha_1, \alpha_2)$, where

$$\alpha_1 = (0, 0, 0, 1, 1, 0, 0, 1, 1, 1), \alpha_2 = (0, 0, 1, 1, 1, 0, 0, 0, 1, 1).$$

Moreover, $\mathbf{q}_6$ can be transformed to $(\theta_1, \ldots, \theta_8)$, where

$$\theta_1, \theta_4, \theta_6, \theta_7 \in \{(0, 1, 1, 0, 1, 0, 0, 0, 1, 1), (0, 0, 1, 1, 1, 0, 1, 0, 0, 1)\},$$

and

$$\theta_2, \theta_3, \theta_5, \theta_8 \in \{(1, 1, 0, 0, 0, 0, 0, 1, 1, 1), (0, 1, 0, 0, 1, 0, 1, 1, 0, 1), (0, 0, 0, 1, 1, 1, 1, 1, 0, 0)\}.$$

It is easy to check by computer that only 8 such vectors are 4-orthogonal with $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_5$. We then consider $\mathbf{q}_7$ for these 8 cases. Using the Eq. (1) for $\mathbf{q}_7 \oplus \mathbf{q}_i$, wherer $i = 4, 5, 6$, it is easy to verify by computer that there is no $\mathbf{q}_7$ 4-orthogonal with $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_6$. Therefore, $OA_{80,4} = 6$.

Now consider $n = 96$. We have the following facts:

(1) Suppose $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_6$ are 4-orthogonal. Then one of $\mathbf{q}_5$ and $\mathbf{q}_6$ can be transformed to $(\alpha, \alpha, \alpha, \alpha, \alpha, \alpha, \alpha, \alpha)$, where $\alpha = (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$.
(2) If there exists a $\mathbf{q}_7$ which is 4-orthogonal with $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_6$, then the constant C in the Eq. (1) for $\mathbf{q}_7 \oplus \mathbf{q}_i$ or $\mathbf{q}_6 \oplus \mathbf{q}_i$ is $\frac{n}{16}$, wherer $i = 4, 5$.

So, we can take $\mathbf{q}_5 = (\alpha, \alpha, \alpha, \alpha, \alpha, \alpha, \alpha, \alpha)$ and there are 48 cases for $\mathbf{q}_6$. Suppose there exists a $\mathbf{q}_8$ which is 4-orthogonal with $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_7$. Then only four cases for $\mathbf{q}_6$ are remained. For these four cases, it is easy to verify by computer that the vectors can be extended to a group of seven vectors 4-orthogonal with each other, but no $\mathbf{q}_8$ exists. Therefore, $OA_{96,4} = 7$, which is a previously unknown value. Hence, the minimum number of rows w of an orthogonal

Table 3 Maximum number of 4-orthogonal vectors in $\mathbb{F}_2^n$

n	32	48	64	80	96	112
$OA_{n,4}$	6	5	8	6	7	6

array $OA(w, 9, 2, 4)$ is 128 (it cannot be 112 from the next paragraph), which was known to be ≥ 96 [2].

Now consider $n = 112$. Suppose $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_6$ are 4-orthogonal. Then one of $\mathbf{q}_5$ and $\mathbf{q}_6$ can be transformed to $(\alpha_1, \alpha_2, \alpha_2, \alpha_1, \alpha_2, \alpha_1, \alpha_1, \alpha_2)$, where

$$\alpha_1 = (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1), \alpha_2 = (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1).$$

So, we can take $\mathbf{q}_5$ to be this vector. Suppose $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_7$ are 4-orthogonal. Then $\mathbf{q}_6$ can be reduced to eight cases, and it is easy to verify by computer that no $\mathbf{q}_7$ exists. Therefore, $OA_{112,4} = 6$, which is a previously unknown value. Hence, the minimum number of rows w of an orthogonal array $OA(w, 12, 2, 4)$ is 128, which was known to be ≥ 112 [2].

We summarize the results in Table 3. It is noted that by Table 3 the minimum number of rows w of an orthogonal array $OA(w, n, 2, 4)$ can be determined, for $n \leq 13$.

Appendix B: An 11-variable 4-CI Boolean function with the minimum Hamming weight

Take $m = 7$ and S be the absolute maximum 4-linearly independent set with 11 vectors given in Example 2. We have

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

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

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

It is easy to check that f is a 4-CI Boolean function with the Hamming weight 128. Therefore, $w_{11,4} \leq 128$. From Table 3 of Appendix 1, we have $w_{11,4} \geq 128$. Hence, $w_{11,4} = 128$. This is a previously unknown value, thus a triple question mark ??? in Table II of [5] can be taken place by it.

References

1. Baumert L., Golomb S.W., Hall M.J.: Discovery of an Hadamard matrix of order 92. Bull. Am. Math. Soc. **68**(3), 237–238 (1962).
2. Bhasin S., Carlet C., Guilley S.: Theory of masking with codewords in hardware: low-weight dth-order correlation-immune Boolean functions. IACR Cryptology ePrint Archive. Report 2013/303 (2013).
3. Borissov Y., Braeken A., Nikova S., Preneel B.: On the covering radii of binary reed-muller codes in the set of resilient Boolean functions. IEEE Trans. Inf. Theory **51**(3), 1182–1189 (2005).
4. Carlet C.: Boolean Functions for Cryptography and Error Correcting Codes. Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering", pp. 257–397. Cambridge University Press, Cambridge (2010) . http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.

5. Carlet C., Chen X.: Constructing low-weight *d*th-order correlation-immune Boolean functions through the Fourier-Hadamard transform. IEEE Trans. Inf. Theory **64**(4), 2969–2978 (2018).
6. Carlet C., Guilley S.: Side-channel indistinguishability. In: Proceedings of HASP–13. 2nd International Workshop on Hardware and Architectural Support for Security and Privacy, pp. 9:1–9:8 (2013).
7. Cusick T.W., Stănică P.: Cryptographic Boolean Functions and Applications, 2nd edn. Elsevier-Academic Press, Cambridge (2017).
8. Djokovic D.Z.: Hadamard matrices of order 764 exist. Combinatorica **28**(4), 487–489 (2008).
9. Georgiou S., Koukouvinos C., Seberry J.: Hadamard matrices, orthogonal designs and construction algorithms. Designs **563**, 133–205 (2003).
10. Hadamard J.: Résolution d'une question relative aux déterminants. Bull. Sci. Math. **17**, 240–246 (1893).
11. Kharaghani H., Tayfeh-Rezaie B.: A Hadamard matrix of order 428. J. Comb. Des. **13**(6), 435–440 (2005).
12. Kocher P.: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. Advances in Cryptology—CRYPTO'96 . LNCS 1109, pp. 104–113. Springer, Berlin (1996).
13. Kocher P., Jaffe J., Jun B.: Differential power analysis. Advances in Cryptology–CRYPTO '99. LNCS 1666, pp. 388–397. Springer, Berlin (1999).
14. Mangard S., Pramstaller N., Oswald E.: "Successfully attacking masked AES hardware implementations," Cryptographic Hardware and Embedded Systems—CHES 2005. LNCS 3659, pp. 157–171. Springer, Berlin (2005).
15. Mangard S., Oswald E., Popp T.: Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security). Springer, New York (2007).
16. Mazumdar B., Mukhopadhyay D., Sengupta I.: Constrained search for a class of good bijective s-boxes with improved DPA resistivity. IEEE Trans. Inf. Forensics Secur. **8**(12), 2154–2163 (2013).
17. Picek S., Papagiannopoulos K., Ege B., Batina L., Jakobovic D: Confused by Confusion: Systematic Evaluation of DPA Resistance of Various S-boxes. Progress in Cryptology—INDOCRYPT 2014. LNCS 8885, pp. 374–390. Springer, Berlin (2014)
18. Schmidt B.: Cyclotomic integers and finite geometry. J. Am. Math. Soc. **12**(4), 929–952 (1999).
19. Siegenthaler T.: Correlation immunity of nonlinear combining functions for cryptographic applications. IEEE Trans. Inf. Theory **30**(5), 776–780 (1984).
20. Trichina E., Seta D.D., Germani L.: Simplified adaptive multiplicative masking for AES. Cryptographic Hardware and Embedded Systems—CHES 2002. LNCS 2523, pp. 187–197. Springer, Berlin (2002).
21. Wallis J.S.: On the existence of Hadamard matrices. J. Comb. Theory A. **21**(2), 188–195 (1976).
22. Xiao G.Z., Massey J.L.: A spectral characterization of correlation-immune combining functions. IEEE Trans. Inf. Theory **34**(3), 569–571 (1988).