Constructing low-weight dth-order correlation-immune Boolean functions through the Fourier-Hadamard transform

Claude Carlet and Xi Chen*

Abstract

The correlation immunity of Boolean functions is a property related to cryptography, to error correcting codes, to orthogonal arrays (in combinatorics, which was also a domain of interest of S. Golomb) and in a slightly looser way to sequences. Correlation-immune Boolean functions (in short, CI functions) have the property of keeping the same output distribution when some input variables are fixed. They have been widely used as combiners in stream ciphers to allow resistance to the Siegenthaler correlation attack. Very recently, a new use of CI functions has appeared in the framework of side channel attacks (SCA). To reduce the cost overhead of counter-measures to SCA, CI functions need to have low Hamming weights. This actually poses new challenges since the known constructions which are based on properties of the Walsh-Hadamard transform, do not allow to build unbalanced CI functions.

In this paper, we propose constructions of low-weight dth-order CI functions based on the Fourier-Hadamard transform, while the known constructions of resilient functions are based on the Walsh-Hadamard transform. We first prove a simple but powerful result, which makes that one only need to consider the case where d is odd in further research. Then we investigate how constructing low Hamming weight CI functions through the Fourier-Hadamard transform (which behaves well with respect to the multiplication of Boolean functions). We use the characterization of CI functions by the Fourier-Hadamard transform and introduce a related general construction of CI functions by multiplication. By using the Kronecker product of vectors, we obtain more constructions of low-weight d-CI Boolean functions. Furthermore, we present a method to construct low-weight d-CI Boolean functions by making additional restrictions on the supports built from the Kronecker product.

Index Terms

Correlation-immune, Fourier-Hadamard transform, Low Hamming weight, Stream ciphers, Sequences.

I. INTRODUCTION

The role of Boolean functions, which was a domain of interest of S. Golomb [12], is prominent in cryptography, error correcting codes and sequences. Correlation-immune Boolean functions (in short, CI functions) have the property to keep the same output distribution if some input variables are fixed (at most d of them, where d is the so-called correlation immunity order of the function). They allow resisting the Siegenthaler correlation attack when they are used as combiners in stream ciphers, which were also related to the interest of S. Golomb [13]–[15]. They are nicely characterized by their Walsh-Hadamard transform [22].

*Corresponding author: Xi Chen.

Claude Carlet is with LAGA, UMR 7539, CNRS, Department of Mathematics, University of Paris 8 and Paris 13, France and with the University of Bergen, Norway. E-mail: claude.carlet@univ-paris8.fr. Xi Chen is with the College of Science, National University of Defense Technology, Changsha 410073, China, and with LAGA and the University of Paris 8. E-mail: 1138470214@qq.com.

This work is supported by the National Basic Research Program of China (Grant No. 2013CB338002), the Outstanding Youth Science Foundation (No. 11531002) and the Nature Science Foundation of China (NSFC) (No. 61572026,61722213).

Their study (more precisely, the study of balanced CI functions, called resilient, since combiner functions need to have uniformly distributed output) was very active at the end of the last century.

Their interest had decreased recently because the algebraic degree of correlation immune functions is bounded above by the Siegenthaler bound (see e.g. [4]) and new attacks (algebraic attacks [9], fast algebraic attacks [8], Rønjom-Helleseth attacks [20]) oblige now to use functions of very large algebraic degrees (while the Berlekamp-Massey attack [18] only obliged previously to use functions of reasonably large algebraic degrees). Nevertheless, CI functions are directly related to the notions of orthogonal arrays and of dual distance of unrestricted codes (see [10]). They play then a role in combinatorics and coding theory. Moreover, very recently, a new use of CI functions has appeared in the framework of side channel attacks (SCA), renewing their interest. These attacks on the implementations of block ciphers in embedded systems like smart cards, FPGA or ASIC assume an attacker model different from classical attacks, and are in practice extremely powerful. These implementations need then to include counter-measures, which slow down the cryptosystems and require additional memory. CI functions allow reducing the cost overhead of counter-measures to SCA. They need either to have low Hamming weights [6] or to be the indicators of so-called CIS codes, equal to the graphs of permutations [5]. In both cases, the CI functions are unbalanced and this actually poses new challenges since the known constructions (primary constructions like the Maiorana-McFarland construction and secondary constructions like the indirect sum, see a survey in [4]), which are based on (or at least related to) properties of the Walsh-Hadamard transform, do not allow to build CI functions with such constraints.

In this paper, we first prove a simple but powerful result through the Fourier-Hadamard transform, which makes that one only need to consider the case where d is odd to determine all the values $\omega_{n,d}$ of the minimum weight of CI functions of order d. References [1], [7] have studied $\omega_{n,d}$ and have given tables for small values of n (precisely, for $n \leq 13$). Several entries of this table were kept open. In the present paper, we propose several new constructions of CI functions, which are fitted for obtaining low Hamming weight functions, and we deduce new values in the table. The idea of our main constructions is to use the Fourier-Hadamard transform instead of the Walsh-Hadamard transform of Boolean functions. These two transformations are closely related, but the former behaves well with respect to the multiplication of Boolean functions (which leads to constructions by multiplying proper functions and allows to build low Hamming weight functions) while the latter behaves well with respect to their addition (which leads to constructions by adding proper functions, and allows in fine to build functions of larger weights only for instance balanced).

The rest of this paper is organized as follows. In Section II-A, we introduce some necessary definitions and useful lemmas. Then we recall some known results about low-weight d-CI Boolean functions in Section II-B. In Section II-C, we introduce an elementary construction, which shows that the upper inequality in Lemma 2.3 is in fact an equality when d is even. In Section III, we use the characterization of CI functions by the Fourier-Hadamard transform and introduce a related general construction of CI functions by multiplication. More constructions of low-weight d-CI Boolean functions are given by using the Kronecker product of vectors in Section VI. In Section V, we present a method to construct low-weight d-CI Boolean functions by making additional restrictions on the supports built from the Kronecker product.

II. Preliminaries

A. *Necessary definitions and useful lemmas*

In this section, we give the definitions and lemmas which will be used in the paper.

Let a_i be the i-th element of the row vector $a \in \mathbb{F}_2^n$. The Hamming weight of a is denoted by

$$w_H(a) = \#\{1 \leq i \leq n | a_i = 1\}$$

where for a set S, its cardinality is denoted by $\#S$. The Hamming distance between two vectors a, a' is $d_H(a, a') = w_H(a + a')$. For any integer n, we write 0_n for the all-0 column vector and 1_n for the all-1 column vector. We denote by the same symbol "$\cdot$" any inner product in $\mathbb{F}_2^n$, whatever is n.

An n-variable Boolean function, also called a Boolean function in n variables, is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$; it will be written as $f(x) : \mathbb{F}_2^n \to \mathbb{F}_2$, where $x = (x_1, x_2, \dots, x_n)$.

The support of n-variable Boolean function f is defined as

$$\mathrm{Supp}(f) = \{\xi \in \mathbb{F}_2^n | f(\xi) = 1\}.$$

Clearly, n-variable Boolean function f is determined uniquely by its support. The Hamming weight of f, denoted by $w_H(f)$, is the cardinality of $\mathrm{Supp}(f)$. It is an *affine invariant* in the sense that composing a Boolean function on the right by an affine permutation (that is, replacing it by an *affine equivalent* function; in fact, more generally, we could multiply by any permutation but we shall not need it) keeps its Hamming weight unchanged. Function f is called balanced if its output distribution is uniform, that is, if $w_H(f) = 2^{n-1}$.

Definition 2.1: [21] An n-variable Boolean function f is called correlation-immune of order d (in brief, d-CI) if the output distribution of f does not change when at most d input variables are fixed.

Equivalently, the support of the function must be a *simple binary orthogonal array* of strength d [17], i.e. the dual distance of this support is strictly larger than d.

Xiao and Massey give a characterization of d-CI Boolean functions by means of the Fourier-Hadamard transform.

Theorem 2.2: [22] An n-variable Boolean function f is a d-CI Boolean function if and only if for any $v \in \mathbb{F}_2^n$ satisfying $1 \leq w_H(v) \leq d$, we have:

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

where "$\cdot$" is the usual inner product in $\mathbb{F}_2^n$.

Of course, $\widehat{f}(v)$ can also be written as $\widehat{f}(v) = \sum\limits_{x \in \mathrm{Supp}(f)} (-1)^{v \cdot x}$. Hence, f is d-CI if and only if its support, viewed as an unrestricted (i.e. non necessarily linear) code, has dual distance at least $d+1$. Recall that the dual distance of a code $C \subseteq \mathbb{F}_{2^n}$ is the minimum nonzero value of $w_H(v)$ such that $\sum\limits_{x \in C} (-1)^{v \cdot x} \neq 0$; equivalently, it is the minimum nonzero value of i such that the coefficient of $X^{n-i}Y^i$ in the polynomial $D_C(X+Y, X-Y)$ is nonzero, where $D_C(X,Y) = \frac{1}{|C|} \sum_{(x,y) \in C^2} X^{n-d_H(x,y)} Y^{d_H(x,y)}$ is the distance enumerator of C. This coefficient indeed equals $\frac{1}{|C|} \sum_{w_H(v)=i} \left(\sum\limits_{x \in C} (-1)^{v \cdot x} \right)^2$ (see [10]).

The Walsh-Hadamard transform $\mathcal{W}_f(v) : \mathbb{F}_2^n \to \mathbb{C}$ of f is defined by:

$$\mathcal{W}_f(v) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + v \cdot x},$$

and the relationship between the Fourier-Hadamard transform and the Walsh-Hadamard transform is

$$\mathcal{W}_f(v) = \begin{cases} -2\widehat{f}(v), & \text{when} \quad v \neq 0; \\ 2^n - 2\widehat{f}(v), & \text{when} \quad v = 0. \end{cases} \tag{2}$$

So the Fourier-Hadamard and Walsh-Hadamard transforms are close to each other; however, they have slighly different properties (the addition of functions plays the same role with respect to the Walsh-Hadamard transform as the multiplication of functions with respect to the Fourier-Hadamard transform) and we shall see that, while the Walsh-Hadamard transform is useful (and has been much used) for studying balanced correlation immune functions (called resilient), the Fourier-Hadamard transform is more adapted to the study of low-weight correlation immune functions.

B. Known results about low-weight d-CI Boolean functions

Let $\mathcal{D}_{n,d}$ be the set of d-CI Boolean functions in n variables. The minimal Hamming weight (i.e. cardinality of the support) of n-variable d-CI non-zero Boolean functions is denoted by $\omega_{n,d}$.

For the convenience of the reader, we list some known results on $\omega_{n,d}$ and recall some of their proofs.

According to Sarkar-Maitra's divisibility property, the Hamming weight of a d-CI function is divisible by 2^d, and according to the first author's result, it is divisible by $2^{d+\left\lfloor \frac{n-d-1}{deg(f)} \right\rfloor}$, where $deg(f)$ is the algebraic degree of function f [3].

The only n-variable n-CI Boolean functions are the two constant function. The only $(n-1)$-CI non-constant Boolean functions are the resilient functions $\sum\limits_{i=1}^{n} x_i$ and $\sum\limits_{i=1}^{n} x_i + 1$. Then

$$\omega_{n,n} = 2^n \text{ and } \omega_{n,n-1} = 2^{n-1}. \tag{3}$$

We give the proof of the following lemma since it will be important in Remark 2.7.

Lemma 2.3: [1], [7] Let $n \geq d \geq 1$ be integers. Then

$$\omega_{n+1,d} \leq 2\omega_{n,d} \leq \omega_{n+1,d+1}.$$

Proof: Given $f(x) \in \mathcal{D}_{n,d}$, the function $g(x, x_{n+1}) = f(x)$ belongs to $\mathcal{D}_{n+1,d}$, since, for every a, we have $\widehat{g}(a,0) = 2\widehat{f}(a)$ and $\widehat{g}(a,1) = 0$, and has weight twice that of $f(x)$. Thus $\omega_{n+1,d} \leq 2\omega_{n,d}$. Assume that $g'(x, x_{n+1}) \in \mathcal{D}_{n+1,d+1}$ is given. Notice that any $d+1$-CI Boolean functions restricted to the hyperplane of equation $x_{n+1} = 0$ is a d-CI Boolean function with half weight. We have $f'(x) = g'(x,0) \in \mathcal{D}_{n,d}$. Thus $2\omega_{n,d} \leq \omega_{n+1,d+1}$. □

Theorem 2.4: [11] Let f be an unbalanced non-constant d-CI Boolean function. Then $d \leq \frac{2}{3}n - 1$.

The following result shows the relationship between CI Boolean functions and codes.

Lemma 2.5: [17] Let n be an integer and $1 \leq d < n$. Let $k_{\max}(n,d)$ be the largest dimension of a binary linear code $[n,k,d+1]$. We have $\omega_{n,d} \leq 2^{n-k_{\max}(n,d)}$.

Notice that binary MDS code $[n, n-1, 2]$ exists, then $\omega_{n,1} = 2$. The constructions of binary codes can be regarded as an upper bound on $\omega_{n,d}$ and more results on binary codes are available in [16].

Note that the minimal weight of a d-CI functions is larger than or equal to the minimal number of rows in an orthogonal array (OA), not necessarily simple, that is in turn larger than or equal to the optimal solution of Delsarte linear programming (LP) problem. A lower bound on $\omega_{n,d}$ can then be found in Table I below, given in [17].

TABLE I

LOWER BOUNDS ON $\omega_{n,d}$ OBTAINED BY THE DELSARTE LP ALGORITHM

d n	1	2	3	4	5	6	7	8	9	10	11	12	13
1	2												
2	2	4											
3	2	4	8										
4	2	6	8	16									
5	2	8	12	16	32								
6	2	8	16	32	32	64							
7	2	8	16	48	64	64	128						
8	2	10	16	64	88	112	128	256					
9	2	12	20	96	128	192	224	256	512				
10	2	12	24	96	192	320	384	512	512	1024			
11	2	12	24	96	192	512	640	1024	1024	1024	2048		
12	2	14	24	112	176	768	1024	1536	1792	2048	2048	4096	
13	2	16	28	128	224	1024	1536	2560	3072	3584	4096	4096	8192

Satisfiability Modulo Theory (SMT) tool is used to search for CI Boolean functions in [1].

We also give Table II from [1], [7] displaying the known values of $\omega_{n,d}$ for $n \leq 13$. A triple question mark ??? indicates that the value is unknown.

TABLE II
MINIMUM HAMMING WEIGHT OF d-CI NONZERO BOOLEAN FUNCTIONS IN n VARIABLES

d n	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

The method to calculate a values of $\omega_{n,d}$ is to prove a lower bound and by a construction to show an upper bound. If the lower bound equals the upper bound, then the value of $\omega_{n,d}$ is decided. If not, it is possible to obtain the values with the help of a computer when n is not very large. More precisely:

- The entries on light gray background follow from $\omega_{n,1} = 2$ and $\omega_{n,n} = 2^n$.
- The entries on dark gray background:
  Upper bound: Notice that $\omega_{n,n-1} = 2^{n-1}$, then $\omega_{n,d} \leq \omega_{n,n-1} = 2^{n-1}$ according to Lemma 2.3.
  Lower bound: According to Theorem 2.4, then for any $\lceil \frac{2n-2}{3} \rceil \leq d \leq n-1$, $2^{n-1} \leq \omega_{n,d}$.

In both areas above, the values of $\omega_{n,d}$ are already decided for any n.

- The entries on write background:
  Upper bound: The known constructions of binary codes provide an upper bound on $\omega_{n,d}$.
  Lower bound: A lower bound on $\omega_{n,d}$ can then be found in Table I according to the Delsarte Linear Programming bound. The fact that $\omega_{n,d}$ is divisible by 2^d is also used.
  Searching: Those entries in **bold** have been obtained by SMT tool.

C. *A first simple construction giving more information on $\omega_{n,d}$*

In this subsection, we introduce an elementary construction, which shows that the upper inequality in Lemma 2.3 is in fact an equality when d is even.

Proposition 2.6: Let d be an even integer such that $n \geq d \geq 2$. Then:

$$\omega_{n+1,d+1} = 2\omega_{n,d}.$$

Proof: Assume that $f(x) \in \mathcal{D}_{n,d}$ is given. Let

$$g(x, x_{n+1}) = \begin{cases} f(x), & \text{when} \quad x_{n+1} = 0; \\ f(x + 1_n), & \text{when} \quad x_{n+1} = 1. \end{cases} \tag{4}$$

It is clear that $g(x, x_{n+1})$ is an $n+1$-variable Boolean function with Hamming weight $2w_H(f)$. Now we prove that $g(x, x_{n+1})$ is a $d+1$-CI Boolean function, that is, for any $u \in \mathbb{F}_2^n, u_{n+1} \in \mathbb{F}_2$ satisfying $1 \leq w_H(u, u_{n+1}) \leq d+1$,

$$\widehat{g}(u, u_{n+1}) = \sum_{(x,x_{n+1}) \in \mathbb{F}_2^{n+1}} g(x, x_{n+1})(-1)^{(u,u_{n+1})\cdot(x,x_{n+1})} = 0.$$

Indeed, we have for any $(u, u_{n+1}) \in \mathbb{F}_2^{n+1}$:

$$\begin{aligned} \widehat{g}(u, u_{n+1}) &= \sum_{(x,x_{n+1}) \in \mathbb{F}_2^{n+1}} g(x, x_{n+1})(-1)^{(u,u_{n+1})\cdot(x,x_{n+1})} \\ &= \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{u\cdot x} + \sum_{x \in \mathbb{F}_2^n} f(x+1_n)(-1)^{(u,u_{n+1})\cdot(x,1)} \\ &= \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{u\cdot x} + \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{(u,u_{n+1})\cdot(x+1_n,1)} \\ &= (1 + (-1)^{w_H(u,u_{n+1})}) \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{u\cdot x} \\ &= (1 + (-1)^{w_H(u,u_{n+1})})\widehat{f}(u). \end{aligned}$$

If $w_H(u, u_{n+1}) = d+1$, then since d is an even integer, we have $1 + (-1)^{w_H(u,u_{n+1})} = 1 + (-1)^{d+1} = 0$, thus $\widehat{g}(u, u_{n+1}) = 0$.

If $u = 0_n$ and $w_H(u, u_{n+1}) \geq 1$, then $u_{n+1} = 1$. Thus $1 + (-1)^{w_H(u,u_{n+1})} = 1 + (-1) = 0$, which means $\widehat{g}(u, u_{n+1}) = 0$.

If $1 \leq w_H(u, u_{n+1}) \leq d$ and $u \neq 0_n$, we deduce that $1 \leq w_H(u) \leq w_H(u, u_{n+1}) \leq d$. Since $f(x) \in \mathcal{D}_{n,d}$, we have $\widehat{f}(u) = 0$, then $\widehat{g}(u, u_{n+1})$ is null.

Summarizing, for any $(u, u_{n+1}) \in \mathbb{F}_2^n$ such that $1 \leq w_H(u, u_{n+1}) \leq d+1$, the value $\widehat{g}(u, u_{n+1})$ is null, that is, $g(x, x_{n+1})$ is a $d+1$-CI Boolean function. Thus $g(x, x_{n+1}) \in \mathcal{D}_{n+1,d+1}$ and $\omega_{n+1,d+1} \leq 2\omega_{n,d}$ when d is even. But $2\omega_{n,d} \leq \omega_{n+1,d+1}$ for any $n \geq d \geq 1$ according to Lemma 2.3. Thus

$$\omega_{n+1,d+1} = 2\omega_{n,d}$$

for any even d satisfying $n \geq d \geq 2$. □

Remark 2.7: According to the proof of Lemma 2.3 and Proposition 2.6, for any even integer d, d-CI Boolean functions in n variables with weight ω_H exist if and only if $d+1$-CI Boolean functions in $n+1$ variables with weight $2\omega_H$ exist. This makes that one only need to consider the case where d is odd in further research, then the cases which need to be considered are twice less numerous.

Notice that $\omega_{10,4} = 128$, we directly obtain a new value of Table II according to Proposition 2.6, that is, $\omega_{11,5} = 256$.

On the basis of Table II, we propose the following conjecture.

Conjecture 2.8: Let $n \geq 3$ be any integer. The minimum Hamming weight of 3-CI nonzero Boolean functions in n variables equals

$$\omega_{n,3} = 8\lceil \frac{n}{4} \rceil. \tag{5}$$

We say that an n-variable Boolean function achieves the *3-CI conjectured value* if (5) holds. In the following, we will derive general bounds on $\omega_{n,d}$ with odd d. Particularly, we will deduce more values of $\omega_{n,3}$, which agree with our conjecture.

III. A construction of low-weight d-CI Boolean functions through the Fourier-Hadamard transform and a related inequality on $\omega_{n,d}$

In this section, we use the characterization of CI functions by the Fourier-Hadamard transform (rather than by the Walsh-Hadamard transform) and we introduce a related general construction of CI functions by multiplication (instead of by addition as used in classical constructions of resilient functions).

In the next proposition, given a matrix $M \in \mathbb{F}_2^{nt \times nt}$ and given $i, j = 1, \ldots, t$, we denote by $M^{(i,j)}$ the $n \times n$ matrix (called a block of M) obtained from M by erasing its rows whose indices do not belong to the interval $[n(i-1)+1; n(i-1)+n]$ and its columns whose indices do not belong to the interval $[n(j-1)+1; n(j-1)+n]$. Assuming that M is non-singular, denoting the inverse matrix of M by M^{-1} and the transposed matrix of M^{-1} by M', we denote by $M^{-1^{(i,j)}}$ and $M'^{(i,j)}$ the matrices obtained similarly from M^{-1} and M'. We define the symbol "$\cdot$" as the usual inner product in $\mathbb{F}_2^n$ and the symbol "$\times$" as the normal matrix multiplication (row vector can also be regarded as a matrix with one row). Notice that $M'^{(j,i)}$ is the transposed matrix of $M^{-1^{(i,j)}}$, according to the definition, then for any $x, y \in \mathbb{F}_2^n$ and $n \times n$ matrix $M^{(i,j)}$, we have

$$x \cdot (y \times M^{-1^{(i,j)}}) = y \cdot (x \times M'^{(j,i)}). \tag{6}$$

Proposition 3.1: Let t be a positive integer and M be a $nt \times nt$ nonsingular matrix over $\mathbb{F}_2$. Let $f_j \in \mathcal{D}_{n,d_j}$ for any $1 \leq j \leq t$. Define the following nt-variable function h, whose input is written in the form $(x^{(1)}, x^{(2)}, \ldots, x^{(t)})$, where $x^{(1)}, x^{(2)}, \ldots, x^{(t)} \in \mathbb{F}_2^n$:

$$h(x^{(1)}, x^{(2)}, \ldots, x^{(t)}) = \prod_{j=1}^{t} f_j\bigg(\sum_{i=1}^{t} x^{(i)} \times M^{(i,j)}\bigg).$$

Assume that for any $(u^{(1)}, u^{(2)}, \ldots, u^{(t)}) \in (\mathbb{F}_2^n)^t$ satisfying $1 \leq w_H(u^{(1)}, u^{(2)}, \ldots, u^{(t)}) \leq d$, there exists $1 \leq j \leq t$ such that

$$1 \leq w_H\bigg(\sum_{i=1}^{t} u^{(i)} \times M'^{(i,j)}\bigg) \leq d_j.$$

Then h belongs to $\mathcal{D}_{nt,d}$ and has Hamming weight $\prod_{j=1}^{t} w_H(f_j)$.

Proof: Notice that for any $(u^{(1)}, u^{(2)}, \ldots, u^{(t)}) \in (\mathbb{F}_2^n)^t$,

$$\begin{aligned}\widehat{h}(u^{(1)}, u^{(2)}, \ldots, u^{(t)}) &= \sum_{x^{(1)}, x^{(2)}, \ldots, x^{(t)} \in \mathbb{F}_2^n} h(x^{(1)}, x^{(2)}, \ldots, x^{(t)})(-1)^{(u^{(1)}, u^{(2)}, \ldots, u^{(t)}) \cdot (x^{(1)}, x^{(2)}, \ldots, x^{(t)})} \\ &= \sum_{x^{(1)}, x^{(2)}, \ldots, x^{(t)} \in \mathbb{F}_2^n} \Bigg(\prod_{j=1}^{t} f_j\bigg(\sum_{i=1}^{t} x^{(i)} \times M^{(i,j)}\bigg)\Bigg)(-1)^{\sum_{j=1}^{t} u^{(j)} \cdot x^{(j)}}.\end{aligned}$$

Replace $\sum_{i=1}^{t} x^{(i)} \times M^{(i,j)}$ by $y^{(j)}$ for $1 \leq j \leq t$, then $(y^{(1)}, y^{(2)}, \ldots, y^{(t)}) = (x^{(1)}, x^{(2)}, \ldots, x^{(t)}) \times M$, according to the well-known method of multiplication of matrices by blocks. Thus

$$(x^{(1)}, x^{(2)}, \ldots, x^{(t)}) = (y^{(1)}, y^{(2)}, \ldots, y^{(t)}) \times M^{-1},$$

which means $x^{(j)} = \sum_{i=1}^{t} y^{(i)} \times {M^{-1}}^{(i,j)}$ for $1 \leq j \leq t$. According to (6), then

$$\begin{aligned}
& \widehat{h}(u^{(1)}, u^{(2)}, \ldots, u^{(t)}) \\
= & \sum_{y^{(1)}, y^{(2)}, \ldots, y^{(t)} \in \mathbb{F}_2^n} \left(\prod_{j=1}^{t} f_j(y^{(j)}) \right) (-1)^{\sum_{j=1}^{t} u^{(j)} \cdot \left(\sum_{i=1}^{t} y^{(i)} \times {M^{-1}}^{(i,j)} \right)} \\
= & \sum_{y^{(1)}, y^{(2)}, \ldots, y^{(t)} \in \mathbb{F}_2^n} \left(\prod_{j=1}^{t} f_j(y^{(j)}) \right) (-1)^{\sum_{j=1}^{t} \sum_{i=1}^{t} y^{(i)} \cdot (u^{(j)} \times M'^{(j,i)})} \\
= & \sum_{y^{(1)}, y^{(2)}, \ldots, y^{(t)} \in \mathbb{F}_2^n} \left(\prod_{j=1}^{t} f_j(y^{(j)}) \right) (-1)^{\sum_{i=1}^{t} y^{(i)} \cdot \left(\sum_{j=1}^{t} u^{(j)} \times M'^{(j,i)} \right)} \\
= & \sum_{y^{(1)}, y^{(2)}, \ldots, y^{(t)} \in \mathbb{F}_2^n} \left(\prod_{j=1}^{t} f_j(y^{(j)}) \right) (-1)^{\sum_{j=1}^{t} y^{(j)} \cdot \left(\sum_{i=1}^{t} u^{(i)} \times M'^{(i,j)} \right)} \\
= & \prod_{j=1}^{t} \left(\sum_{y^{(j)} \in \mathbb{F}_2^n} f_j(y^{(j)}) (-1)^{y^{(j)} \cdot \left(\sum_{i=1}^{t} u^{(i)} \times M'^{(i,j)} \right)} \right) \\
= & \prod_{j=1}^{t} \widehat{f_j} \left(\sum_{i=1}^{t} u^{(i)} \times M'^{(i,j)} \right).
\end{aligned}$$

According to the hypothesis, for any $(u^{(1)}, u^{(2)}, \ldots, u^{(t)}) \in (\mathbb{F}_2^n)^t$ satisfying $1 \leq w_H(u^{(1)}, u^{(2)}, \ldots, u^{(t)}) \leq d$, there exists $1 \leq j \leq t$ such that

$$1 \leq w_H \left(\sum_{i=1}^{t} u^{(i)} \times M'^{(i,j)} \right) \leq d_j.$$

Since f_j is a d_j-CI Boolean function for any $1 \leq j \leq t$, we have for any $1 \leq w_H(u^{(1)}, u^{(2)}, \ldots, u^{(t)}) \leq d$ that

$$\widehat{h}(u^{(1)}, u^{(2)}, \ldots, u^{(t)}) = \prod_{j=1}^{t} \widehat{f_j} \left(\sum_{i=1}^{t} u^{(i)} \times M'^{(i,j)} \right) = 0,$$

which means h is a d-CI Boolean function.

By definition, h is affine equivalent to the direct product of f_j and then $w_H(h) = \prod_{j=1}^{t} w_H(f_j)$. Thus h belongs to $\mathcal{D}_{nt,d}$ and has Hamming weight $\prod_{j=1}^{t} w_H(f_j)$. □

As an application of Proposition 3.1, we have the following results.

Corollary 3.2: Let n, d, t be positive integers satisfying $d \leq n$ and $t \geq 2$. Assume that $f_1 \in \mathcal{D}_{n,d}$ and $f_j \in \mathcal{D}_{n,\lfloor \frac{d}{2} \rfloor}$ for any $2 \leq j \leq t$. Define

$$h(x^{(1)}, x^{(2)}, \ldots, x^{(t)}) = f_1(x^{(1)}) \prod_{j=2}^{t} f_j(x^{(j)} + x^{(1)});\ x^{(1)}, x^{(2)}, \ldots, x^{(t)} \in \mathbb{F}_2^n.$$

Then h belongs to $\mathcal{D}_{nt,d}$ and has Hamming weight $\prod_{j=1}^{t} w_H(f_j)$.

Proof: Let the $nt \times nt$ nonsingular matrix whose representation by $n \times n$ blocks equals

$$M = \begin{bmatrix} I & I & I & \cdots & I \\ 0 & I & 0 & \cdots & 0 \\ 0 & 0 & I & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & I \end{bmatrix},$$

where I is the identity $n \times n$ matrix and 0 is the all-0 $n \times n$ matrix. Then

$$M' = \begin{bmatrix} I & 0 & 0 & \cdots & 0 \\ I & I & 0 & \cdots & 0 \\ I & 0 & I & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ I & 0 & 0 & \cdots & I \end{bmatrix}.$$

Notice that

$$\begin{aligned} h(x^{(1)}, x^{(2)}, \ldots, x^{(t)}) &= f_1(x^{(1)}) \prod_{j=2}^{t} f_j(x^{(j)} + x^{(1)}) \\ &= f_1(x^{(1)} \times I) \prod_{j=2}^{t} f_j(x^{(j)} \times I + x^{(1)} \times I) = \prod_{j=1}^{t} f_j\Big(\sum_{i=1}^{t} x^{(i)} \times M^{(i,j)}\Big), \end{aligned}$$

where $f_1 \in \mathcal{D}_{n,d}$ and $f_j \in \mathcal{D}_{n,\lfloor \frac{d}{2} \rfloor}$ for any $2 \leq j \leq t$. According to Proposition 3.1, we only need to prove that for any $(u^{(1)}, u^{(2)}, \ldots, u^{(t)}) \in (\mathbb{F}_2^n)^t$ satisfying $1 \leq w_H(u^{(1)}, u^{(2)}, \ldots, u^{(t)}) \leq d$, either

$$1 \leq w_H\Big(\sum_{i=1}^{t} u^{(i)} \times M'^{(i,1)}\Big) = w_H\Big(\sum_{i=1}^{t} u^{(i)}\Big) \leq d,$$

or there exists $2 \leq j \leq t$ such that

$$1 \leq w_H\Big(\sum_{i=1}^{t} u^{(i)} \times M'^{(i,j)}\Big) = w_H(u^{(j)}) \leq \left\lfloor \frac{d}{2} \right\rfloor.$$

For any $(u^{(1)}, u^{(2)}, \ldots, u^{(t)}) \in (\mathbb{F}_2^n)^t$ satisfying $1 \leq w_H(u^{(1)}, u^{(2)}, \ldots, u^{(t)}) \leq d$, it is clear that

$$w_H\Big(\sum_{i=1}^{t} u^{(i)}\Big) \leq \sum_{i=1}^{t} w_H(u^{(i)}) = w_H(u^{(1)}, u^{(2)}, \ldots, u^{(t)}) \leq d.$$

If $\sum\limits_{i=1}^{t} u^{(i)} \neq 0_n$, then $1 \leq w_H\left(\sum\limits_{i=1}^{t} u^{(i)}\right) \leq d$. Otherwise $\sum\limits_{i=1}^{t} u^{(i)} = 0_n$. Notice that $(u^{(1)}, u^{(2)}, \dots, u^{(t)}) = 0_{nt}$ if and only if $u^{(j)} = 0_n$ for any $2 \leq j \leq t$ and $\sum\limits_{i=1}^{t} u^{(i)} = 0_n$. Then there exists $2 \leq j \leq t$ such that $u^{(j)} \neq 0_n$ since $w_H(u^{(1)}, u^{(2)}, \dots, u^{(t)}) \geq 1$. We have $u^{(j)} = \sum\limits_{i=1, i\neq j}^{t} u^{(i)} \neq 0_n$. Then

$$w_H(u^{(j)}) = w_H\left(\sum_{i=1, i\neq j}^{t} u^{(i)}\right) = \frac{w_H(u^{(j)}) + w_H\left(\sum\limits_{i=1,i\neq j}^{t} u^{(i)}\right)}{2} \leq \frac{\sum\limits_{i=1}^{t} w_H(u^{(i)})}{2} \leq \frac{d}{2}.$$

Since $w_H(u^{(j)})$ is an integer, there exists $2 \leq j \leq t$ such that $1 \leq w_H(u^{(j)}) \leq \lfloor \frac{d}{2} \rfloor$. The proof is complete. □

Remark 3.3: Given a code C_1 of dual distance d_1, a code C_2 of dual distance d_2 and codes $C_3, \dots, C_t$ of dual distances at least d_2, the dual distance of the code $\{(x^{(1)}, x^{(2)}, \dots, x^{(t)}) \in (\mathbb{F}_2^n)^t; x^{(1)} \in C_1, x^{(1)} + x^{(2)} \in C_2, \dots, x^{(1)} + x^{(t)} \in C_t\}$ equals $\min(d_1, 2\,d_2)$, according to the proof above.

One can construct nt-variable d-CI Boolean functions with Hamming weight $(\omega_{n,\lfloor \frac{d}{2} \rfloor})^{t-1}\,\omega_{n,d}$ according to Corollary 3.2. Then the following corollary is clear.

Corollary 3.4: Let n, d, t be positive integers satisfying $d \leq n$ and $t \geq 2$. We have

$$\omega_{nt,d} \leq (\omega_{n,\lfloor \frac{d}{2} \rfloor})^{t-1}\,\omega_{n,d}.$$

In the case of $d = 3, t = 2$, we have $\omega_{n,1} = 2$, then $2n$-variable 3-CI Boolean functions with Hamming weight $2\omega_{n,3}$ exist. Further, notice that $\omega_{4,3} = 8$ and $\omega_{12,3} = 24$, we can deduce that n-variable Boolean functions which achieve *3-CI conjectured value* exist when $n = 2^k$ or $3 \cdot 2^k$ for any $k \geq 2$.

IV. A construction of low-weight d-CI Boolean functions through Kronecker product

In this section, we deduce more values of $\omega_{n,d}$ by using the Kronecker product of vectors, which agree with our conjecture when $d = 3$. Another general construction by using Kronecker product directly is given in Proposition 4.5, which is a more general construction.

The Kronecker product of two vectors is defined as

$$(x^{(1)}, x^{(2)}) = ((x_1^{(1)}, \dots, x_{n_2}^{(1)}), (x_1^{(2)}, \dots, x_{n_1}^{(2)})) \in \mathbb{F}_2^{n_2} \times \mathbb{F}_2^{n_1} \to (x_{i_2}^{(1)} + x_{i_1}^{(2)})_{1 \leq i_1 \leq n_1, 1 \leq i_2 \leq n_2} \in \mathbb{F}_2^{n_1 n_2}.$$

Its generalization to t variables can be stated as follows:
for any $1 \leq r \leq t$, let $x^{(r)} = (x_{1,\dots,1,1,\dots,1}^{(r)}, \cdots, x_{n_1,\cdots,n_{r-1},n_{r+1},\cdots,n_t}^{(r)}) \in \mathbb{F}_2^{n_1 \cdots n_{r-1} n_{r+1} \cdots n_t}$, then we have $(x^{(1)}, x^{(2)}, \dots, x^{(t)}) \in \mathbb{F}_2^{n_2 n_3 \cdots n_t} \times \mathbb{F}_2^{n_1 n_3 \cdots n_t} \times \cdots \times \mathbb{F}_2^{n_1 n_2 \cdots n_{t-1}}$. The generalized Kronecker product of t vectors is then defined as:

$$(x^{(1)}, x^{(2)}, \dots, x^{(t)}) \to \big(\sum_{r=1}^{t} x_{i_1,\dots,i_{r-1},i_{r+1},\dots,i_t}^{(r)}\big)_{1 \leq i_1 \leq n_1, 1 \leq i_2 \leq n_2, \dots, 1 \leq i_t \leq n_t} \in \mathbb{F}_2^{n_1 n_2 \cdots n_t}.$$

In the following proposition, we use this generalized Kronecker product to define a construction of CI functions; in fact, we also append the first vector $x^{(1)} \in \mathbb{F}_2^{n_2 \cdots n_t}$ to the product, in order to construct low-weight d-CI Boolean functions.

Proposition 4.1: Let d, t be positive integers such that $2^t > d$. Assume that $f_1(x^{(1)})$ is a d-CI Boolean function with $n_2 \cdots n_t$ variables and $f_2(x^{(2)})$ is a $2\lfloor \frac{d}{2} \rfloor$-CI Boolean function with $n_1 n_3 \cdots n_t$ variables. For any $r = 3, 4, \dots, t$, assume that $f_r(x^{(r)})$ is a Boolean function whose number of variables equals

$n_1 \cdots n_{r-1} n_{r+1} \cdots n_t$ and which is such that, for every $v^{(r)} \in \mathbb{F}_2^{n_r}$ satisfying $1 \leq w_H(v^{(r)}) \leq d$ with $w_H(v^{(r)})$ even, we have $\widehat{f}_r(v^{(r)}) = 0$. We define the $\big((n_1+1)n_2n_3 \cdots n_t\big)$-variable function h by its support as follows:

$$\mathrm{Supp}(h) =$$
$$\left\{ \left(\left(\sum_{r=1}^{t} x^{(r)}_{i_1,\dots,i_{r-1},i_{r+1},\dots,i_t} \right)_{1 \leq i_1 \leq n_1, 1 \leq i_2 \leq n_2, \dots, 1 \leq i_t \leq n_t} , x^{(1)} \right) ; \begin{array}{l} x^{(1)} \in \mathrm{Supp}(f_1) \\ x^{(2)} \in \mathrm{Supp}(f_2) \\ \dots \\ x^{(t)} \in \mathrm{Supp}(f_t) \end{array} \right\},$$

then h is a d-CI Boolean function of Hamming weight $\prod\limits_{r=1}^{t} w_H(f_r)$.

In particular, if f_1 is a d-CI Boolean function and if each function f_r is $2\lfloor \frac{d}{2} \rfloor$-CI for $r = 2, \dots, t$, then h is a d-CI Boolean function of Hamming weight $\prod\limits_{r=1}^{t} w_H(f_r)$.

Proof: It is clear that h is an $\big((n_1+1)n_2n_3 \cdots n_t\big)$-variable Boolean function and has Hamming weight $\prod\limits_{r=1}^{t} w_H(f_r)$. For any $u = (u_{i_1,i_2,\dots,i_t})_{i_1,i_2,\dots,i_t} \in \mathbb{F}_2^{n_1n_2\cdots n_t}, v = (v_{i_2,\dots,i_t})_{i_2,\dots,i_t} \in \mathbb{F}_2^{n_2 \cdots n_t}$ (to simplify the notation, let us define $u_{0,i_2,\dots,i_t} := v_{i_2,\dots,i_t}$ for any $i_2, \dots, i_t$), we have:

$$\begin{aligned}
\widehat{h}(u,v) &= \sum_{\substack{x^{(1)} \in \mathrm{Supp}(f_1), x^{(2)} \in \mathrm{Supp}(f_2) \\ \dots, x^{(t)} \in \mathrm{Supp}(f_t)}} (-1)^{v \cdot x^{(1)} + \sum\limits_{1 \leq i_1 \leq n_1, 1 \leq i_2 \leq n_2, \dots, 1 \leq i_t \leq n_t} u_{i_1,i_2,\dots,i_t} (\sum\limits_{r=1}^{t} x^{(r)}_{i_1,\dots,i_{r-1},i_{r+1},\dots,i_t})} \\
&= \left(\sum_{x^{(1)} \in \mathrm{Supp}(f_1)} (-1)^{v \cdot x^{(1)} + \sum\limits_{1 \leq i_1 \leq n_1, 1 \leq i_2 \leq n_2, \dots, 1 \leq i_t \leq n_t} u_{i_1,i_2,\dots,i_t} x^{(1)}_{i_2,\dots,i_t}} \right) \\
&\quad \times \prod_{r=2}^{t} \left(\sum_{x^{(r)} \in \mathrm{Supp}(f_r)} (-1)^{\sum\limits_{1 \leq i_1 \leq n_1, 1 \leq i_2 \leq n_2, \dots, 1 \leq i_t \leq n_t} u_{i_1,i_2,\dots,i_t} x^{(r)}_{i_1,\dots,i_{r-1},i_{r+1},\dots,i_t}} \right) \\
&= \left(\sum_{x^{(1)} \in \mathrm{Supp}(f_1)} (-1)^{\sum\limits_{1 \leq i_2 \leq n_2, \dots, 1 \leq i_t \leq n_t} u_{0,i_2,\dots,i_t} x^{(1)}_{i_2,\dots,i_t} + \sum\limits_{1 \leq i_2 \leq n_2, \dots, 1 \leq i_t \leq n_t} x^{(1)}_{i_2,\dots,i_t} \big(\sum\limits_{i_1=1}^{n_1} u_{i_1,i_2,\dots,i_t} \big)} \right) \\
&\quad \times \prod_{r=2}^{t} \left(\sum_{x^{(r)} \in \mathrm{Supp}(f_r)} (-1)^{\sum\limits_{\substack{1 \leq i_1 \leq n_1, \dots, 1 \leq i_{r-1} \leq n_{r-1} \\ 1 \leq i_{r+1} \leq n_{r+1}, \dots, 1 \leq i_t \leq n_t}} x^{(r)}_{i_1,\dots,i_{r-1},i_{r+1},\dots,i_t} \big(\sum\limits_{i_r=1}^{n_r} u_{i_1,i_2,\dots,i_t} \big)} \right) \\
&= \left(\sum_{x^{(1)} \in \mathrm{Supp}(f_1)} (-1)^{\big(\sum\limits_{i_1=0}^{n_1} u_{i_1,1,\dots,1}, \cdots, \sum\limits_{i_1=0}^{n_1} u_{i_1,n_2,\dots,n_t} \big) \cdot x^{(1)}} \right) \\
&\quad \times \prod_{r=2}^{t} \left(\sum_{x^{(r)} \in \mathrm{Supp}(f_r)} (-1)^{\big(\sum\limits_{i_r=1}^{n_r} u_{1,\dots,1,i_r,1,\dots,1}, \cdots, \sum\limits_{i_r=1}^{n_r} u_{n_1,\dots,n_{r-1},i_r,n_{r+1},\dots,n_t} \big) \cdot x^{(r)}} \right) \\
&= \widehat{f}_1 \big(\sum_{i_1=0}^{n_1} u_{i_1,1,\dots,1}, \cdots, \sum_{i_1=0}^{n_1} u_{i_1,n_2,\dots,n_t} \big) \prod_{r=2}^{t} \widehat{f}_r \big(\sum_{i_r=1}^{n_r} u_{1,\dots,1,i_r,1,\dots,1}, \cdots, \sum_{i_r=1}^{n_r} u_{n_1,\dots,n_{r-1},i_r,n_{r+1},\dots,n_t} \big).
\end{aligned}$$

Let $u = (u_{i_1,i_2,\dots,i_t})_{i_1,i_2,\dots,i_t} \in \mathbb{F}_2^{n_1 n_2 \cdots n_t}, v = (v_{i_2,\dots,i_t})_{i_2,\dots,i_t} \in \mathbb{F}_2^{n_2 \cdots n_t}$ satisfying $1 \leq w_H(u,v) \leq d$, it is clear that:

$$w_H(\overrightarrow{u_1}) \leq w_H(u,v) \leq d,$$

where $\overrightarrow{u_1}$ is defined as the vector $\big(\sum_{i_1=0}^{n_1} u_{i_1,1,\dots,1}, \cdots, \sum_{i_1=0}^{n_1} u_{i_1,n_2,\dots,n_t}\big) \in \mathbb{F}_2^{n_2 n_3 \cdots n_t}$. For any $2 \leq r \leq t$, we define the vector $\big(\sum_{i_r=1}^{n_r} u_{1,\dots,1,i_r,1,\dots,1}, \cdots, \sum_{i_r=1}^{n_r} u_{n_1,\dots,n_{r-1},i_r,n_{r+1},\dots,n_t}\big) \in \mathbb{F}_2^{n_1 \cdots n_{r-1} n_{r+1} \cdots n_t}$ as $\overrightarrow{u_r}$ for convenience.

Assume that $w_H(\overrightarrow{u_1}) \neq 0$, then since f_1 is a d-CI Boolean function, we have $\widehat{f}_1(\overrightarrow{u_1}) = 0$ and $\widehat{h}(u,v)$ is null.

Assume that $w_H(\overrightarrow{u_1}) = 0$ but $w_H(\overrightarrow{u_2}) \neq 0$. Notice that

$$w_H(u,v) \pmod 2 \;=\; \sum_{1 \leq i_2 \leq n_2, \dots, 1 \leq i_t \leq n_t} \big(\sum_{i_1=0}^{n_1} u_{i_1,i_2,\dots,i_t}\big) = 0,$$

hence, $w_H(u,v)$ is even then the weight is no more than $2\lfloor \frac{d}{2} \rfloor$. Since $w_H(\overrightarrow{u_2}) \neq 0$, we have:

$$1 \leq w_H(\overrightarrow{u_2}) \leq w_H(u) \leq w_H(u,v) \leq 2\lfloor \frac{d}{2} \rfloor.$$

Then since f_2 is a $2\lfloor \frac{d}{2} \rfloor$-CI Boolean function, we have $\widehat{f}_2(\overrightarrow{u_2}) = 0$ and $\widehat{h}(u,v)$ is null.

Assume that $w_H(\overrightarrow{u_1}) = w_H(\overrightarrow{u_2}) = \ldots = w_H(\overrightarrow{u_{s-1}}) = 0$ but $w_H(\overrightarrow{u_s}) \neq 0$, where $3 \leq s \leq t$. Notice that

$$\begin{aligned} w_H(u) \pmod 2 \;&=\; \sum_{1 \leq i_1 \leq n_1, 1 \leq i_3 \leq n_3, \dots, 1 \leq i_t \leq n_t} \big(\sum_{i_2=1}^{n_2} u_{i_1,i_2,\dots,i_t}\big) = 0 \\ &=\; \sum_{1 \leq i_1 \leq n_1, \dots, 1 \leq i_{s-1} \leq n_{s-1}, 1 \leq i_{s+1} \leq n_{s+1}, \dots, 1 \leq i_t \leq n_t} \big(\sum_{i_s=1}^{n_s} u_{i_1,i_2,\dots,i_t}\big). \end{aligned}$$

Hence, $w_H(u)$ is even. The second equality shows then that $w_H(\overrightarrow{u_s})$ is even. Since $w_H(\overrightarrow{u_s}) \neq 0$, we have:

$$2 \leq w_H(\overrightarrow{u_s}) \leq w_H(u) \leq w_H(u,v) \leq d.$$

The hypothesis implies therefore that $\widehat{f}_s(\overrightarrow{u_s}) = 0$ and thus $\widehat{h}(u)$ is null.

Suppose that $w_H(\overrightarrow{u_1}) = w_H(\overrightarrow{u_2}) = \ldots = w_H(\overrightarrow{u_t}) = 0$. Since $w_H(u,v) \neq 0$ and $w_H(\overrightarrow{u_1}) = 0$, there exist $0 \leq i_1'' < i_1' \leq n_1, 1 \leq i_2 \leq n_2, \dots, 1 \leq i_t \leq n_t$ such that $u_{i_1',i_2,\dots,i_t} = u_{i_1'',i_2,\dots,i_t} = 1$. Note that i_1'' may be null but not i_1'. Thus there exists $u_{i_1',i_2,\dots,i_t} = 1$, where $1 \leq i_1' \leq n_1, 1 \leq i_2 \leq n_2, \dots, 1 \leq i_t \leq n_t$. Since $w_H(\overrightarrow{u_t}) = 0$, there exist $i_1', \dots, i_{t-1}$ and at least 2 values of i_t such that $u_{i_1',i_2,\dots,i_t} = 1$. Since $w_H(\overrightarrow{u_{t-1}}) = 0$, there exist then $i_1', \dots, i_{t-2}$ and at least 4 values of (i_{t-1}, i_t) such that $u_{i_1',i_2,\dots,i_t} = 1$. By induction, we have then $w_H(u,v) \geq 2^t$. But we have $1 \leq w_H(u,v) \leq d < 2^t$ by hypothesis, a contradiction. Hence, $w_H(\overrightarrow{u_1}) = w_H(\overrightarrow{u_2}) = \ldots = w_H(\overrightarrow{u_t}) = 0$ can not happen.

This completes the proof. □

Let $d = 3, t = 2$, we have the following corollary.

Corollary 4.2: Let $n_1 \geq 2, n_2 \geq 3$ be integers. Assume that f_1 is a 3-CI Boolean function in n_2 variables and f_2 is a 2-CI Boolean function in n_1 variables. Define the Boolean function h in $(n_1+1)n_2$ variables such that:

$$\mathrm{Supp}(h) = \{\big((x_{i_2}^{(1)} + x_{i_1}^{(2)})_{1 \leq i_1 \leq n_1, 1 \leq i_2 \leq n_2}, x^{(1)}\big) | x^{(1)} \in \mathrm{Supp}(f_1), x^{(2)} \in \mathrm{Supp}(f_2)\}.$$

Then h is a 3-CI Boolean function of Hamming weight $w_H(f_1)w_H(f_2)$.

Remark 4.3: Corollary 4.2 may provide more values of $\omega_{n,3}$ which agree with our conjecture. For example, since $\omega_{12,3} = 24$ and $\omega_{11,2} = 12$, a 144-variable Boolean function which achieves *3-CI conjectured value* exists according to Corollary 4.2, which means $\omega_{144,3} \leq 288$. Notice that $144 = 3^2 \cdot 2^4$, $\omega_{144,3}$ can not be obtained by Corollary 3.4.

Remark 4.4: According to Corollary 2.7, f_2 is a 2-CI Boolean function in n_1 variables with weight $w_H(f_2)$ if and only if there exists a 3-CI Boolean function f_2' in n_1+1 variables with $w_H(f_2') = 2w_H(f_2)$. Thus we can construct the 3-CI Boolean function h in $(n_1+1)n_2$ variables of Hamming weight $w_H(f_1)w_H(f_2')/2$ from two 3-CI Boolean function f_1, f_2'.

The following functions are constructed by the Kronecker product directly and the conditions on f_2 is weaker, but the number of variables of h is less than Proposition 4.1. Proposition 4.1 is more efficient for working on the table and the following proposition gives a more general construction. The proof is similar but easier than Proposition 4.1, we omit the details here.

Proposition 4.5: Let d, t be positive integers such that $2^t > d$. Assume that $f_1(x^{(1)})$ is a d-CI Boolean function whose number of variables equals the product $n_2 \cdots n_t$. For any $r = 2, 3, \ldots, t$, assume that $f_r(x^{(r)})$ is a Boolean function whose number of variables equals $n_1 \cdots n_{r-1} n_{r+1} \cdots n_t$ and which is such that, for every $v^{(r)} \in \mathbb{F}_2^{n_r}$ satisfying $1 \leq w_H(v^{(r)}) \leq d$ with $w_H(v^{(r)})$ even, we have $\widehat{f_r}(v^{(r)}) = 0$. We denote by h the $(n_1 n_2 \cdots n_t)$-variable function whose support equals the Kronecker product of the supports of $f_1, f_2, \ldots, f_t$:

$$\begin{aligned}&\mathrm{Supp}(h) = \\ &\{(\sum_{r=1}^{t} x^{(r)}_{i_1,\ldots,i_{r-1},i_{r+1},\ldots,i_t})_{1\leq i_1\leq n_1, 1\leq i_2\leq n_2,\ldots,1\leq i_t\leq n_t} | x^{(1)} \in \mathrm{Supp}(f_1), x^{(2)} \in \mathrm{Supp}(f_2), \ldots, x^{(t)} \in \mathrm{Supp}(f_t)\},\end{aligned}$$

then h is a d-CI Boolean function of Hamming weight $\prod_{r=1}^{t} w_H(f_r)$.

In particular, if f_1 is a d-CI Boolean function and if each function f_r is $2\lfloor\frac{d}{2}\rfloor$-CI for $r = 2, \ldots, t$, then h is a d-CI Boolean function of Hamming weight $\prod_{r=1}^{t} w_H(f_r)$.

V. MORE CONSTRUCTIONS

In this section, we construct low-weight d-CI Boolean functions by making additional restrictions on the supports built from the Kronecker product. In the next proposition, given a vector $v \in \mathbb{F}_2^m$, we denote by v^0 the vector $(v_1, \ldots, v_{m-1}, 0)$ and by v^1 the vector $(v_1, \ldots, v_{m-1}, 1)$.

Proposition 5.1: Let $n, m \geq 3$ be integers. Given an n-variable function f and an m-variable function g, we denote by h the nm-variable function whose support equals the Kronecker product of the supports of f and g:

$$\mathrm{Supp}(h) = \{((x_i + y_j)_{1\leq i\leq n, 1\leq j\leq m}) | x \in \mathrm{Supp}(f), y \in \mathrm{Supp}(g)\},$$

and by h', h'' the nm-variable functions whose supports equal respectively:

$$\mathrm{Supp}(h') = \{((x_i + y_j)_{1\leq i\leq n, 1\leq j\leq m}) | x \in \mathrm{Supp}(f), y \in \mathrm{Supp}(g) \text{ satisfying } y_m = 0\},$$

$$\mathrm{Supp}(h'') = \{((x_i + y_j)_{1\leq i\leq n, 1\leq j\leq m}) | x \in \mathrm{Supp}(f), y \in \mathrm{Supp}(g) \text{ satisfying } y_m = 1\}.$$

We have then, for any $u = (u_{i,j})_{1\leq i\leq n; 1\leq j\leq m} \in \mathbb{F}_2^{nm}$ that:

$$\widehat{h}(u) = \widehat{f}(\sum_{j=1}^{m} u_{1,j}, \cdots, \sum_{j=1}^{m} u_{n,j})\, \widehat{g}(\sum_{i=1}^{n} u_{i,1}, \cdots, \sum_{i=1}^{n} u_{i,m}),$$

$$\widehat{h'}(u) = \frac{1}{2}\widehat{f}(\sum_{j=1}^{m} u_{1,j}, \cdots, \sum_{j=1}^{m} u_{n,j}) \left(\widehat{g}(\sum_{i=1}^{n} u_{i,1}, \cdots, \sum_{i=1}^{n} u_{i,m-1}, 0) + \widehat{g}(\sum_{i=1}^{n} u_{i,1}, \cdots, \sum_{i=1}^{n} u_{i,m-1}, 1)\right),$$

$$\widehat{h''}(u) = \frac{1}{2}\widehat{f}(\sum_{j=1}^{m} u_{1,j}, \cdots, \sum_{j=1}^{m} u_{n,j}) \left(\widehat{g}(\sum_{i=1}^{n} u_{i,1}, \cdots, \sum_{i=1}^{n} u_{i,m-1}, 0) - \widehat{g}(\sum_{i=1}^{n} u_{i,1}, \cdots, \sum_{i=1}^{n} u_{i,m-1}, 1)\right).$$

Assume that $f(x)$ is a 3-CI Boolean function and that $g(y)$ is such that, for every $v \in \mathbb{F}_2^m$ of Hamming weight 2, we have $\widehat{g}(v) = 0$ (respectively, we have $\widehat{g}(v^0) + \widehat{g}(v^1) = 0$, $\widehat{g}(v^0) - \widehat{g}(v^1) = 0$), then h is a 3-CI Boolean function of Hamming weight $w_H(f)w_H(g)$ (respectively, h' is a 3-CI Boolean function, h'' is a 3-CI Boolean function). Moreover, if g is 1-CI then h' and h'' have Hamming weight $w_H(f)w_H(g)/2$. In particular, if f and g are 3-CI Boolean functions, then h is a 3-CI Boolean function of Hamming weight $w_H(f)w_H(g)$ and both h' and h'' are 3-CI Boolean functions of Hamming weight $w_H(f)w_H(g)/2$.

Proof: It is clear that h, h', h'' are nm-variable Boolean functions and that h has Hamming weight $w_H(f)w_H(g)$. If g is 1-CI, then the restriction of g to the hyperplane of equation $y_m = 0$ (resp. $y_m = 1$) has Hamming weight $w_H(g)/2$ and h', h'' have then Hamming weight $w_H(f)w_H(g)/2$.

For any $u \in \mathbb{F}_2^{nm}$, we have:

$$\begin{aligned}
\widehat{h}(u) &= \sum_{x\in \mathrm{Supp}(f), y\in \mathrm{Supp}(g)} (-1)^{\sum_{1\le i\le n, 1\le j\le m} u_{i,j}(x_i+y_j)} \\
&= \sum_{x\in \mathrm{Supp}(f)} (-1)^{\sum_{i=1}^{n}(\sum_{j=1}^{m} u_{i,j})x_i} \sum_{y\in \mathrm{Supp}(g)} (-1)^{\sum_{j=1}^{m}(\sum_{i=1}^{n} u_{i,j})y_j} \\
&= \sum_{x\in \mathrm{Supp}(f)} (-1)^{(\sum_{j=1}^{m} u_{1,j}, \cdots, \sum_{j=1}^{m} u_{n,j})\cdot x} \sum_{y\in \mathrm{Supp}(g)} (-1)^{(\sum_{i=1}^{n} u_{i,1}, \cdots, \sum_{i=1}^{n} u_{i,m})\cdot y} \\
&= \widehat{f}(\sum_{j=1}^{m} u_{1,j}, \cdots, \sum_{j=1}^{m} u_{n,j})\, \widehat{g}(\sum_{i=1}^{n} u_{i,1}, \cdots, \sum_{i=1}^{n} u_{i,m}),
\end{aligned}$$

$$\begin{aligned}
\widehat{h'}(u) &= \sum_{x\in \mathrm{Supp}(f)} (-1)^{(\sum_{j=1}^{m} u_{1,j}, \cdots, \sum_{j=1}^{m} u_{n,j})\cdot x} \sum_{y\in \mathrm{Supp}(g), y_m=0} (-1)^{(\sum_{i=1}^{n} u_{i,1}, \cdots, \sum_{i=1}^{n} u_{i,m})\cdot y} \\
&= \widehat{f}(\sum_{j=1}^{m} u_{1,j}, \cdots, \sum_{j=1}^{m} u_{n,j}) \left(\frac{\sum_{y\in \mathrm{Supp}(g)} (-1)^{(\sum_{i=1}^{n} u_{i,1}, \cdots, \sum_{i=1}^{n} u_{i,m-1}, 0)\cdot y} + \sum_{y\in \mathrm{Supp}(g)} (-1)^{(\sum_{i=1}^{n} u_{i,1}, \cdots, \sum_{i=1}^{n} u_{i,m-1}, 1)\cdot y}}{2} \right) \\
&= \frac{1}{2}\widehat{f}(\sum_{j=1}^{m} u_{1,j}, \cdots, \sum_{j=1}^{m} u_{n,j}) \left(\widehat{g}(\sum_{i=1}^{n} u_{i,1}, \cdots, \sum_{i=1}^{n} u_{i,m-1}, 0) + \widehat{g}(\sum_{i=1}^{n} u_{i,1}, \cdots, \sum_{i=1}^{n} u_{i,m-1}, 1)\right),
\end{aligned}$$

$$\begin{aligned}
\widehat{h''}(u) &= \sum_{x\in \mathrm{Supp}(f)} (-1)^{(\sum\limits_{j=1}^{m} u_{1,j},\cdots,\sum\limits_{j=1}^{m} u_{n,j})\cdot x} \sum_{y\in \mathrm{Supp}(g),y_m=0} (-1)^{(\sum\limits_{i=1}^{n} u_{i,1},\cdots,\sum\limits_{i=1}^{n} u_{i,m})\cdot y} \\
&= \widehat{f}\big(\sum_{j=1}^{m} u_{1,j},\cdots,\sum_{j=1}^{m} u_{n,j}\big)\Bigg(\frac{\sum\limits_{y\in \mathrm{Supp}(g)} (-1)^{(\sum\limits_{i=1}^{n} u_{i,1},\cdots,\sum\limits_{i=1}^{n} u_{i,m-1},0)\cdot y} - \sum\limits_{y\in \mathrm{Supp}(g)} (-1)^{(\sum\limits_{i=1}^{n} u_{i,1},\cdots,\sum\limits_{i=1}^{n} u_{i,m-1},1)\cdot y}}{2}\Bigg) \\
&= \frac{1}{2}\widehat{f}\big(\sum_{j=1}^{m} u_{1,j},\cdots,\sum_{j=1}^{m} u_{n,j}\big)\Big(\widehat{g}\big(\sum_{i=1}^{n} u_{i,1},\cdots,\sum_{i=1}^{n} u_{i,m-1},0\big) - \widehat{g}\big(\sum_{i=1}^{n} u_{i,1},\cdots,\sum_{i=1}^{n} u_{i,m-1},1\big)\Big).
\end{aligned}$$

The second steps for h' and h'' hold since

$$\begin{aligned}
&\sum_{y\in \mathrm{Supp}(g)} (-1)^{(\sum\limits_{i=1}^{n} u_{i,1},\cdots,\sum\limits_{i=1}^{n} u_{i,m-1},0)\cdot y} \\
= &\sum_{y\in \mathrm{Supp}(g),y_m=0} (-1)^{(\sum\limits_{i=1}^{n} u_{i,1},\cdots,\sum\limits_{i=1}^{n} u_{i,m-1})\cdot y'} + \sum_{y\in \mathrm{Supp}(g),y_m=1} (-1)^{(\sum\limits_{i=1}^{n} u_{i,1},\cdots,\sum\limits_{i=1}^{n} u_{i,m-1})\cdot y'},
\end{aligned}$$

and

$$\begin{aligned}
&\sum_{y\in \mathrm{Supp}(g)} (-1)^{(\sum\limits_{i=1}^{n} u_{i,1},\cdots,\sum\limits_{i=1}^{n} u_{i,m-1},1)\cdot y} \\
= &\sum_{y\in \mathrm{Supp}(g),y_m=0} (-1)^{(\sum\limits_{i=1}^{n} u_{i,1},\cdots,\sum\limits_{i=1}^{n} u_{i,m-1})\cdot y'} - \sum_{y\in \mathrm{Supp}(g),y_m=1} (-1)^{(\sum\limits_{i=1}^{n} u_{i,1},\cdots,\sum\limits_{i=1}^{n} u_{i,m-1})\cdot y'},
\end{aligned}$$

where $y = (y', y_m)$.

Let $u \in \mathbb{F}_2^{nm}$ satisfying $1 \le w_H(u) \le 3$, it is clear that

$$w_H\big(\sum_{j=1}^{m} u_{1,j},\cdots,\sum_{j=1}^{m} u_{n,j}\big) \le w_H(u) \le 3.$$

If $(\sum\limits_{j=1}^{m} u_{1,j},\cdots,\sum\limits_{j=1}^{m} u_{n,j}) \ne 0_n$, then since f is a 3-CI Boolean function, we have $\widehat{f}\big(\sum\limits_{j=1}^{m} u_{1,j},\cdots,\sum\limits_{j=1}^{m} u_{n,j}\big) = 0$ and $\widehat{h}(u), \widehat{h'}(u), \widehat{h''}(u)$ are null.

If $(\sum\limits_{j=1}^{m} u_{1,j},\cdots,\sum\limits_{j=1}^{m} u_{n,j}) = 0_n$ and $u \ne 0$, then $w_H(u) = \sum\limits_{i=1}^{n}\sum\limits_{j=1}^{m} w_H(u_{i,j})$ is even and $1 \le w_H(u) \le 3$ implies $w_H(u) = 2$. There exist then $1 \le i_1 \le n, 1 \le j_1 < j_2 \le m$ such that $u_{i_1,j_1} = u_{i_1,j_2} = 1$ and others are 0. Thus $\sum\limits_{i=1}^{n} u_{i,j_1} = \sum\limits_{i=1}^{n} u_{i,j_2} = 1$ and others are 0, which means $w_H(\sum\limits_{i=1}^{n} u_{i,1},\cdots,\sum\limits_{i=1}^{n} u_{i,m}) = 2$. According to the hypothesis, we have $\widehat{g}(\sum\limits_{i=1}^{n} u_{i,1},\cdots,\sum\limits_{i=1}^{n} u_{i,m}) = 0$ (respectively, we have $\widehat{g}(\sum\limits_{i=1}^{n} u_{i,1},\cdots,\sum\limits_{i=1}^{n} u_{i,m-1},0)+\widehat{g}(\sum\limits_{i=1}^{n} u_{i,1},\cdots,\sum\limits_{i=1}^{n} u_{i,m-1},1) = 0$, $\widehat{g}(\sum\limits_{i=1}^{n} u_{i,1},\cdots,\sum\limits_{i=1}^{n} u_{i,m-1},0) - \widehat{g}(\sum\limits_{i=1}^{n} u_{i,1},\cdots,\sum\limits_{i=1}^{n} u_{i,m-1},1) = 0$), then $\widehat{h}(u)$ is null (respectively, $\widehat{h'}(u) = 0$,$\widehat{h''}(u) = 0$).

This completes the proof. □

VI. Concluding Remarks

In this paper, we first proved a simple but powerful result, which makes that one only need to consider the case where d is odd for investigating the minimum Hamming weight of CI-functions of order d. Then we used the characterization of CI functions by the Fourier-Hadamard transform and introduced a related general construction of CI functions by multiplication. By using the Kronecker product of vectors, we obtained more constructions of low Hamming weight d-CI Boolean functions. Furthermore, we present a method to construct low-weight d-CI Boolean functions by making additional restrictions on the supports built from the Kronecker product. For further research, it is interesting to construct more low Hamming weight d-CI Boolean functions, especially new values in the table which lists the minimum Hamming weights of d-CI nonzero Boolean functions in n variables.

References

[1] S. Bhasin, C. Carlet, 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.

[2] J. Bierbrauer, K. Gopalakrishnan, D. R. Stinson. Orthogonal arrays, resilient functions, error-correcting codes, and linear programming bounds. SIAM Journal on Discrete Mathematics, vol. 9(3), pp. 424-452, 1996.

[3] C. Carlet. On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions. Sequences and their Applications. Springer London, pp. 131-144, 2002.

[4] C. Carlet. Boolean Functions for Cryptography and Error Correcting Codes. Chapter of the monography *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer eds, Cambridge University Press, pp. 257-397 2010. Preliminary version available at www.math.univ-paris13.fr/~carlet/english.html

[5] C. Carlet, J.-L. Danger, S. Guilley and H. Maghrebi. Leakage Squeezing of Order Two. *Proceedings of INDOCRYPT 2012, LNCS* 7668, pp. 120-139, 2012.

[6] C. Carlet and S. Guilley. Side-channel indistinguishability. *Proceedings of HASP '13, 2nd International Workshop on Hardware and Architectural Support for Security and Privacy*, pp. 9:1-9:8. Tel Aviv, Israel, june 2013. ACM, New York, 2013.

[7] C. Carlet and S. Guilley, Correlation-immune Boolean functions for easing counter-measures to side channel attacks. Proceedings of the Workshop "Emerging Applications of Finite Fields", Algebraic Curves and Finite Fields, Radon Series on Computational and Applied Mathematics, published by de Gruyter, pp. 41-70, 2014.

[8] N. Courtois. Fast Algebraic Attacks on Stream Ciphers with Linear Feedback. *Proceedings of CRYPTO 2003, Lecture Notes in Computer Science* 2729, pp. 177-194, 2003.

[9] N. Courtois and W. Meier. Algebraic Attacks on Stream Ciphers with Linear Feedback. *Proceedings of EUROCRYPT 2003, Lecture Notes in Computer Science* 2656, pp. 346-359, 2003.

[10] P. Delsarte. Four fundamental parameters of a code and their combinatorial significance. *Information and Control*, vol. 23(5), pp. 407-438, 1973.

[11] D.G. Fon-Der-Flaass. A bound on correlation immunity. Sib. Elektron. Mat. Izv. 4, pp. 133-135, 2007. http://semr.math.nsc.ru/v4/p133-135.pdf.

[12] S.W. Golomb. On the classification of Boolean functions. IEEE Transactions on Information Theory, vol. 5(5), pp. 176-186, 1959.

[13] S.W. Golomb. Shift Register Sequences. Aegean Park Press, 1982.

[14] S.W. Golomb. Shift Register Sequences - A Retrospective Account. SETA 2006.

[15] S.W. Golomb, G. Gong. Signal design for good correlation. Cambridge University Press, Cambridge 2005.

[16] M. Grassl. Code Tables: Bounds on the parameters of various types of codes. Available at http://www.codetables.de/, Universitat Karlsruhe.

[17] A.S. Hedayat, N.J.A. Sloane and J. Stufken. Orthogonal arrays, theory and applications. Springer series in statistics, New York, Springer-Verlag press, 1999.

[18] J.L. Massey. Shift-register analysis and BCH decoding. *IEEE Transactions on Information Theory*, vol. 15, pp. 122-127, 1969.

[19] S. Picek, C. Carlet, S.Guilley, et al. Evolutionary Algorithms for Boolean Functions in Diverse Domains of Cryptography. Evolutionary Computation, 2016.

[20] S. Rønjom and T. Helleseth. A new attack on the filter generator. IEEE Transactions on Information Theory, vol. 53(5), pp. 1752-1758, 2007.

[21] T. Siegenthaler, Correlation immunity of Nonlinear Combining Functions for Cryptographic Applications[J]. IEEE Transactions on Information Theory, vol. 30(5), pp. 776-780, 1984.

[22] G.Z. Xiao and J.L. Massey, A spectral characterization of correlation-immune combining functions. IEEE Transactions on Information Theory, vol. 34(3), pp. 569-571, 1988.

Claude Carlet received the Ph.D. degree from the University of Paris 6, Paris, France, in 1990 and the Habilitation to Direct theses from the University of Amiens, France, in 1994. He was Associate Professor with the Department of Computer Science at the University of Amiens from 1990 to 1994, and Professor with the Department of Computer Science at the University of Caen, France, from 1994 to 2000 and with the Department of mathematics, University of Paris 8, Saint-Denis, France since then. His research interests include Boolean functions, cryptology and coding theory. Prof. Carlet was Associate Editor for Coding Theory of IEEE Transactions on Information Theory from March 2002 until February 2005. He is the Editor in Chief of the journal "Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences" (CCDS) published by SPRINGER. He is in the editorial boards of the journals "Designs, Codes and Cryptography" (SPRINGER), "Advances in Mathematics of Communications" (AIMS),"International Journal of Computer Mathematics" (Taylor & Francis) and "International Journal of Information and Coding Theory" (Inderscience publishers).

Xi Chen received his B.S. degree in 2013 in mathematics from the National University of Defense Technology, Changsha, China. He is now a Ph.D. Candidate in mathematics in the College of Science, National University of Defense Technology of China. His research interests are cryptography and Boolean functions.