VOL. 10, NO 22, DECEMBER, 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

CORRELATION IMMUNITY AND RESILIENCY OF BOOLEAN FUNCTIONS FROM HAAR DOMAIN PERSPECTIVE

H. M. Rafiq and M. U. Siddiqi
ECE Department, Faculty of Engineering, IIUM, Jalan Gombak, Kuala Lumpur, Malaysia
E-Mail: umarsiddiqi@iium.edu.my

ABSTRACT

The strength of any conventional cipher system relies on the underlying cryptographic Boolean functions employed in the system. The design of such systems requires that the employed Boolean functions meet specific security criteria. Two of such criteria are the correlation immunity and resiliency of a given Boolean function. To determine whether such criteria are met, a designer needs the help of spectral transform tool and in this case the Walsh spectral transform. Most of the cryptographic criteria have been generalized in terms of the Walsh transform. In this paper, we present an alternative view of such criteria from the Haar spectral transform point of view. The Haar along with the Walsh are the two methods considered suitable for representing Boolean functions. The paper exploits the analogy between the two transforms to derive the Haar general representation of the correlation-immunity and the resiliency security criteria. The paper presents the Haar-based conditions on which a given Boolean function should meet to be considered correlation-immune of order k $(CI(k))$ or resilient of order k $(R(k))$. In addition, the paper presents a Haar-based algorithm for testing correlation-immunity of an arbitrary Boolean function including experimental results related to the algorithm. The results in this presentation are based on a simulation study of the Haar-based algorithm in comparison to its Walsh-counterpart. The results portray the computational advantage of the Haar method over the Walsh approach for the correlation-immunity measure. The paper includes as well, a discussion on the worst-case scenario with advantages and flexibility of the Haar method in conjunction with the lower order Walsh transform. A summary of the work is then presented in the conclusion of the paper.

Keywords: boolean functions, haar transform, haar spectrum, spectral coefficients, cryptographic security criteria, correlation-immunity, and resiliency.

INTRODUCTION

The design of strong conventional cipher systems requires that the employed cryptographic Boolean functions meet specific security criteria. Two of such criteria are the correlation immunity and resiliency of a given Boolean function. To determine whether such criteria are met, a designer needs the help of spectral transform tool and in this case the Walsh spectral transform. The Walsh spectral transform has been mostly employed for analysis and generalization of desired cryptographic Boolean functions [1, 2, 4, 5, 11, 12, 13].

The Haar spectral transform along with the Walsh transform, are the two transforms considered suitable for representations of Boolean functions [3, 7, 8]. The Haar method has gained wide spread usage in various fields of engineering and computer science [7]. In cryptography, only the Walsh transform has been employed for analysis of such systems. The motivation of this paper is based on the works of [3, 7]. The contribution of this work is towards cryptographic Boolean functions and their Haar-based characterization; specifically a Haar alternative view of two significant cryptographic criteria is presented. The Haar provide a local-based spectral view of functions satisfying such criteria. This view is significant especially when it comes to construction of such functions. The paper presents the correlation-immunity and resiliency security criteria from the Haar domain perspective. The paper answers the following significant questions; given an arbitrary Boolean function then what are the conditions on its Haar spectrum for it to satisfy the two security criteria? How can such a function be tested using the Haar transform to see if it satisfies the two criteria? How does the Haar-based method compared to the existing Walsh method? What are the advantages of employing the Haar transform in this context?

The paper is organized as follows. Section 2 presents an overview of Boolean functions including the spectral transforms and existing significant results. In section 3, the Haar spectral characterization of correlation-immunity and resiliency is derived and presented. The Haar-based algorithm for testing correlation-immunity of an arbitrary Boolean function is given in section 4. The section presents as well, simulation results of the conducted experiments in comparison between the Haar-based algorithm and its Walsh counterpart. Moreover, the section explores the significance of employing the Haar transform along with the Walsh transform as hybrid method. Finally, in section 5, we present the conclusion of the paper and discussion on future work.

PRELIMINARIES

In this section, we present a review on Boolean functions and results from earlier research works that relate to correlation immunity and resiliency.

An *n*-variable Boolean function $f(x_1, \dots, x_n)$, is a mapping of *n* binary inputs ($(x_1, \dots, x_n) \in \mathbb{F}_2^n$) to a single binary output ($f(x) \in \mathbb{F}_2$) [1, 2]. The input argument is an *n*-dimensional binary vector $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_2^n$ ($x_i \in \mathbb{F}_2$). The set of all Boolean functions is denoted by B_n. Any $f \in B_n$ has a unique representation in each of the following forms [2]:

- The ordered tuple $T_f = (f(x^{(0)}), f(x^{(1)}), \dots, f(x^{(2^n-1)}))$ is called the binary truth table of $f(f \in \mathbb{F}_2\})$. The truth table lists the outputs of the function for all the possible 2^n input combinations, where $x^{(0)} = (0, \dots, 0)$ (the all-zeroes vector), $x^{(2^n-1)} = (1, \dots, 1)$ (the all-ones vector), and generally $x^{(k)}$ as the binary vector representation of the integer k, for $0 \le k \le 2^n - 1$. The relationship between x and k is given by $x = \sum_{i=1}^{n} 2^{n-i} x_i$.
- Sometimes instead of T_f, it is more advantageous to use the real valued function of *f*, which is called the sign function ξ or the polarity truth table (ξ takes values from the set $\{-1,1\}$). It is defined as $\xi(x) = (-1)^{f(x)} \equiv 1 - 2f(x), \forall \alpha \in \mathbb{F}_2^n$. The truth table of the sign function is called the sequence of *f*. Some literature use $\hat{f}$ as equivalent notation of ξ.
- The polynomial representation (ANF); the algebraic normal form can be written uniquely as a sum (XOR) of products (AND)

$$f = a_0 \oplus a_1 x_1 \oplus \cdots \oplus a_{12} x_1 x_2 \oplus \cdots \oplus a_{12\cdots n} x_1 x_2 \cdots x_n$$

Where $a_i, x_i \in \mathbb{F}_2$

The highest number of variables in the product terms of the ANF gives the degree of f and is denoted by $\deg(f)$. Other representations for the Boolean function such as NNF can be found in [1, 2]. The weight of a function is defined as the number of nonzero entries in T_f and is denoted by $wt(f)$. If the weight of a function is $2^n - 1$, meaning that the number of zeroes and ones in the truth table are equal, then the function is balanced.

Linear and Affine Boolean functions: A linear Boolean function, selected by $\omega \in Z_2^n$ is denoted by L_ω with the general expression $L_\omega = \omega_1 x_1 \oplus \omega_2 x_2 \oplus \cdots \oplus \omega_n x_n$. Any function of the form $f = c \oplus L_\omega$ where $c \in F_2$ is called **Affine** function. The set of affine functions contain all the linear functions.

Walsh-hadamard transform: The Walsh transform (ξ_{WH}) of a function ξ on $\mathbb{F}_2^n$ is given by [1, 2]:

$$\xi_{WH}(u) = \sum_{x,u \in V_n} (-1)^{f(x) \oplus x \cdot u} \quad (1)$$

Haar functions: The set of Haar functions (H_l^q's or simply as H_j) forms a complete set of orthogonal rectangular basis functions [3,4]. They are defined on the interval $[0, 2^n)$ as un-normalized taking the values of 0 and ± 1 as follows:

$$H_0^{(0)}(x) = H_0(x) = 1, \forall x \in [0, 2^n)$$

$$H_j(x) = \begin{cases} 1, & (2q) \cdot 2^{n-l-1} \le x < (2q+1) \cdot 2^{n-l-1} \\ -1, & (2q+1) \cdot 2^{n-l-1} \le x < (2q+2) \cdot 2^{n-l-1} \\ 0, & else\ in\ [0, 2^n) \end{cases} \quad (2)$$

Where: l and q are degree (zone of the spectrum resp.) and order of the Haar functions respectively. With $j = 2^l + q$ and for each value of $l = 0, 1, \dots, n-1$, we have $q = 0, 1, \dots, 2^l - 1$.

Haar transform: the Haar transform (ξ_H) of ξ is defined by [3,4]:

$$\xi_H(j) = \sum_{x=0}^{x=2^n-1} H_l^q(x) \cdot \xi(x) \quad (3)$$

Another definition of the Haar functions was given in [3], where the Haar functions are expressed directly in terms of the input variables (based on the degrees and order of the functions). The definition is derived through the connection between the Haar, Rademacher, and the Walsh-Paley functions. In this sense, the Haar functions are sub-sets of the Walsh-Paley functions. The Haar functions $H_l^q(x)$ depending on the degrees $l \in [0, n)$, and orders $q \in [0, 2^l)$ are alternatively given by [3]:

$$H_l^q(x) = \begin{cases} (-1)^{x_{l+1}}, & x \in S_q^l \\ 0, & otherwise \end{cases}, \quad (4)$$

Where, $S_q^l = \{x | x \in [q \cdot 2^{n-l},\ (q+1) \cdot 2^{n-l})$ is the restriction of x to the respective sub-interval/subset defined by the corresponding degree and order. For each of the degrees and the respective orders, the spectral domain interval of $[0, 2^n)$ is partitioned into disjoint subintervals defined by S_q^l. In turn, an equivalent definition of the Haar spectrum $\hat{F}_{H_l}{}^q(x)$ is given as:

$$\hat{F}_{H_l}{}^q(x) = \sum_{x \in S_q^l} (-1)^{f(x) \oplus x_{l+1}}, \quad (5)$$

Correlation immunity (CI): Given an n-variable Boolean function ξ, then it is correlation immune of order k ($CI(k)$, $1 \le k \le n$) if and only if all of its Walsh spectral coefficients satisfy the following condition [1,2, 4,5].

$$\xi_{WH}(\omega) = \sum_{x \in V_n} (-1)^{f(x) \oplus x \cdot \omega} = 0, \quad \forall\, \omega \ni 1 \le wt(\omega) \le k \tag{6}$$

Resiliency: An n-variable Boolean function ξ is resilient of order k if and only if it satisfies $CI(k)$ and is balanced. That is, it is $CI(k)$ and $\xi_{WH}(0) = 0$ [1,2, 4,5,11-15].

The next results based on [9] are significant for distinguishing between resiliency and linearity within the Haar domain. The work has presented the Haar spectral characterization of linear and affine functions. In this work, the distribution of the Haar spectral coefficients for linear functions was derived and presented. Each zone (defined by the degree l) of the Haar spectral coefficient represents a correlation to a specific set of 2^l sub-linear functions ($L^l{}_\omega(q) = \omega_1 q_1 \oplus \omega_2 q_2 \oplus \cdots \oplus \omega_l q_l;\ \omega, q \in \mathbb{F}_2^l$) and their complements. Suppose that the Haar transform is applied to a given n-variable linear Boolean function $(L_\alpha(x) = \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \cdots \oplus \alpha_n x_n;\ \alpha, x \in \mathbb{F}_2^n)$, then the Haar nonzero spectral coefficients will be restricted to within a specific zone (depending on the transformed function). The general Haar representation of linear functions is defined as follows [9]:

Haar spectral definition of linear functions: For the sake of simplicity in notations, let the linear function be given as $L_\alpha(x) \equiv L(x) = \alpha_i x_i \oplus x_{l+1} \ni \alpha_i \in \mathbb{F}_2, i \in [1, l+1),\ l \in [1, n)$ and $x = (x_1, \dots, x_n) \in \mathbb{F}_2^n$ in Paley ordering (bit-reverse representation). The Haar spectrum ($\hat{L}_H(x)$) of the linear function in polarity form ($\hat{L}$) is given by:

$$\hat{L}_H(x) = \begin{cases} \pm 2^{n-l}, & x \in [2^l, 2^{l+1}) \\ 0, & otherwise \end{cases} \tag{7}$$

It was shown in [9] that, as the absolute Haar spectrum of the linear functions is flat within the respective zone (taking the maximum value of 2^{n-l}) then, the "2^{n-l}" term can be factored out. Once the factored term is out, the resulting spectral coefficients within the zone assume a unique linear distribution corresponding to the transformed function. The resulting coefficients represent a specific Walsh function in $\mathbb{F}_2^l$. In turn, the Equation. 7 can be written equivalently as:

$$\hat{L}_H(x) = 2^{n-l} \cdot \begin{cases} L^l{}_\omega(q), & \omega, q \in \mathbb{F}_2^l, x = 2^l + q \\ 0, & otherwise \end{cases} \tag{8}$$

The following section presents the Haar study on correlation immunity and resiliency.

CORRELATION IMMUNITY AND RESILIENCY FROM HAAR PERSPECTIVE

In this section, the Haar spectral characterization of Correlation-Immune (CI) functions is examined. The section presents a study on the general representation of correlation-immunity for a given Boolean function within the Haar spectral domain. The generalization is carried out for both cases; when the order is one ($CI(1)$) and when the general order is k ($CI(k)$). The work presents derivations for Haar based representation of this security criterion.

We introduce first a new data structure to be used in Haar generalization. Let $S\hat{F}_H(l)$ denote the sum of Haar spectral coefficients over the interval $2^l \le x < 2^{l+1}$, that is $S\hat{F}_H(l) = \sum_{x=2^l}^{2^{l+1}-1} \xi_H(x)$, $l = 0,1, \dots, n-1$. This sum represents the addition of spectral coefficients for a given zone within the Haar spectrum. And let $\overrightarrow{S\hat{F}_H}(u)$ be the vector containing all the sums ($S\hat{F}_H(l),\ l \in [0, n)$) for a given spectrum including the spectrum's global coefficient ($\xi_H(0)$). The vector containing all the sums will be referred to as the Haar-Sum-Vector (HSV) from now onwards. It is obvious from its definition the HSV is a $1 \times (n+1)$ vector consisting of the first two global Haar spectral coefficients, and the rest of its elements consist of the sums over the zones defining the local coefficients (see Example 3.1 below).

Example 3.1 Consider a Haar spectrum for a given four-variable Boolean function, then the HSV for the respective spectrum is given by $\overrightarrow{S\hat{F}_H}(u) = \left[\xi_H(0),\ S\hat{F}_H(0), S\hat{F}_H(1), S\hat{F}_H(2), S\hat{F}_H(3)\right]$.

Consider the variable $\vec{\omega} = \langle \omega_1, \omega_2, \dots, \omega_n \rangle \in \mathbb{F}_2^n$ then, the following will be taken into account:

Let $\vec{\omega}_{k_1} = \langle 0,0, \dots, 0, \omega_k = 1, 0, \dots, 0 \rangle$: An n-dimensional unit vector with one at the k^{th} position and zeroes elsewhere.

Let $\vec{\omega}_{k_0} = \langle \omega_1, \omega_2, \dots, \omega_{k-1}, \omega_k = 0, \omega_{k+1}, \dots, \omega_n \rangle$:
The vector $\vec{\omega}$ with zero at the k^{th} position.
Note that, the following properties hold

1. $\vec{\omega} = \vec{\omega}_{k_1} + \vec{\omega}_{k_0}$,
2. $wt(\omega) = 1 \Rightarrow \vec{\omega} = \vec{\omega}_{k_1}, for\ 1 \le k \le n$
3. $x \cdot \vec{\omega}_{k_1} = x_k \cdot 1 = x_k$

Now, the correlation-immunity can be characterized from the Haar spectral domain point of view. The following proposition gives the Haar general characterizations of the correlation-immunity of order one.

Proposition 3.1 A given *n*-variable Boolean function f (with sign function ξ), satisfies correlation-immunity of order one ($CI(1)$) provided that the following condition on its HSV ($\overrightarrow{S\hat{F}_H}(u)$) holds:

$$\overrightarrow{S\hat{F}_H}(u) = 0, \quad for\ 1 \le u \le n+1 \tag{9}$$

Proof: The proof follows by considering the L.H.S of Equation. 6

$\Rightarrow \xi_W(\vec{\omega}) = \xi_W(\vec{\omega}_{k_1}) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus x\cdot\vec{\omega}_{k_1}}$

$\Rightarrow \xi_W(\vec{\omega}_{k_1}) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus x_k}, \quad for\ 1\le k\le n$

$\equiv \sum_{x=0}^{2^n-1}(-1)^{f(x)\oplus x_k}$

$\equiv \sum_{x\in S_0^l}(-1)^{f(x)\oplus x_k} + \sum_{x\in S_1^l}(-1)^{f(x)\oplus x_k}$

$+\cdots+\sum_{x\in S_{2^l-1}^l}(-1)^{f(x)\oplus x_k}$

$\equiv \sum_q\sum_{x\in S_q^l}(-1)^{f(x)\oplus x_k}, \qquad l\in[0,n), q\in[0,2^l)$

$\equiv \sum_q\sum_{x\in S_q^l}(-1)^{f(x)\oplus x_{l+1}}, \qquad k=l+1$

$\equiv \sum_q \xi_{H_l}^q(x) = \overrightarrow{S\hat{F}_H}(u),\ 1\le u\le n$

$\Rightarrow \overrightarrow{S\hat{F}_H}(u) = 0,$ (LHS=RHS of Equation. 6)

This ends the proof.

For higher order correlation to be appropriately derived, a need arises for a restriction on variable space as follows.

Defining a restriction on $\mathbb{F}_2^n$: Let $\mathbb{F}_2^l$ be a restriction on $\mathbb{F}_2^n$ such that, given $(\omega_1,\omega_2,\dots,\omega_n)\in\mathbb{F}_2^n$, the following are true

$\mathbb{F}_2^l \subseteq \mathbb{F}_2^n,\ \forall\, l\in[0,n)$: disjoint Subsets

$\mathbb{F}_2^l \Rightarrow (\omega_1,\omega_2,\dots,\omega_l)\in\mathbb{F}_2^n \wedge \omega_{l+1}=1\ fixed$

$(\omega_1,\omega_2,\dots,\omega_l)\in\mathbb{F}_2^l \Rightarrow (\omega_1,\omega_2,\dots,\omega_l,\omega_{l+1}=1,0,\dots,0)\in\mathbb{F}_2^n$

$\forall\, l\in[0,n) \Rightarrow q\in\mathbb{F}_2^l$

Keeping this restriction in mind and rewriting the Walsh transform in terms of the Haar spectrum based on the respective degrees and orders then, the Haar based definition can be derived as according to the following proposition.

Proposition 3.2 An n-variable Boolean function f (with sign function ξ), satisfies correlation-immunity of order k $(CI(k))$ provided that the following condition on its Haar spectrum $(\xi_{H_l}^q)$ holds, $\forall q\ni 1<wt(q)\le k-1$

$$\sum_{q,\omega\in\mathbb{F}_2^l}\xi_H^l(q)\cdot(-1)^{\omega\cdot q}=0, \qquad (10)$$

Proof: The proof follows by considering the L.H.S of Equation. 6 and rewriting the Walsh function as:

$\Rightarrow \hat{F}_W(\vec{\omega}) = \hat{F}_W(\vec{\omega}_{l+1_1}\oplus\vec{\omega}_{l+1_0}),\quad for\ 0\le l\le n$

$= \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus x\cdot(\vec{\omega}_{l+1_1}\oplus\vec{\omega}_{l+1_0})}$

$= \sum_{x\in\mathbb{F}_2^n}(-1)^{(f(x)\oplus x\cdot\vec{\omega}_{l+1_1})\oplus(x\cdot\vec{\omega}_{l+1_0})}$

$= \sum_{x\in\mathbb{F}_2^n}(-1)^{(f(x)\oplus x_{l+1})\oplus(x\cdot\vec{\omega}_{l+1_0})}$

$= \sum_{x\in\mathbb{F}_2^n}(-1)^{(f(x)\oplus x_{l+1})}\cdot(-1)^{x\cdot\vec{\omega}_{l+1_0}}$

$\equiv \sum_{x\in S_0^l}(-1)^{(f(x)\oplus x_{l+1})}\cdot(-1)^{x\cdot\vec{\omega}_{l+1_0}}$

$+\sum_{x\in S_1^l}(-1)^{(f(x)\oplus x_{l+1})}\cdot(-1)^{x\cdot\vec{\omega}_{l+1_0}}+\cdots$

$+\sum_{x\in S_{2^l-1}^l}(-1)^{(f(x)\oplus x_{l+1})}\cdot(-1)^{x\cdot\vec{\omega}_{l+1_0}}$

$\equiv \sum_q\sum_{x\in S_q^l}(-1)^{(f(x)\oplus x_{l+1})}\cdot(-1)^{x\cdot\vec{\omega}_{l+1_0}}$

, $Note: wt(\vec{\omega}_{l+1_0}) = wt(\vec{\omega})-1$

$\equiv \sum_{q,\omega\in\mathbb{F}_2^l}\left(\sum_{x\in S_q^l}(-1)^{(f(x)\oplus x_{l+1})}\right)\cdot(-1)^{q\cdot\omega},$

$\equiv \sum_{q,\omega\in\mathbb{F}_2^l}\left(\xi_H^l(q)\right)\cdot(-1)^{q\cdot\omega},$

$\equiv \sum_{q,\omega\in\mathbb{F}_2^l}\xi_H^l(q)\cdot(-1)^{q\cdot\omega},\ \forall\, q\ni 1<wt(q)\le k-1$

$\Rightarrow \sum_{q,\omega\in\mathbb{F}_2^l}\xi_H^l(q)\cdot(-1)^{q\cdot\omega}=0$, (LHS=RHS of Equation. 6)

This ends the proof.

The following example demonstrates the order one $CI(1)$ for a given 3-variable Boolean function.

Example 3.2: Consider the 3-variable Boolean function with polarity truth table $\xi = [-1,-1,-1,1,1,-1,-1,-1]$. Its Haar spectrum (ξ_H), Walsh-Hadamard spectrum (ξ_{WH}), and the Haar representation of the correlation immunity $(\overrightarrow{S\hat{F}_H}(u))$, are given in the following table (see Table-1). It can be seen clearly from the table that, all the variables with weight one $(wt(x)=1)$ have the corresponding spectral coefficients equal to zero. This is true as well for the sum of the Haar spectral coefficients within the respective zones.

Table-1. Spectrums of the function in example 3.2.

x	$x_1x_2x_3$	q	$q_1q_2\dots q_l$	ξ	ξ_{WH}	ξ_H	$\overrightarrow{S\hat{F}_H}(u)$
0	000	-	-	-1	-4	-4	-4
1	001	0	0	-1	0	0	0
2	010	0	0	-1	0	-2	0
3	011	1	1	1	4	2	
4	100	0	00	1	0	0	
5	101	1	01	-1	-4	-2	0
6	110	2	10	-1	-4	2	
7	111	3	11	-1	0	0	

Note that the different colors in the table (Table-1) entail the different zones within the Haar spectral domain. The red color represents the zone defined by $l=0$, the blue represents the next zone $(l=1)$ within the spectrum, while the green represents the last zone $(l=2)$ of the spectrum. For resiliency then, in addition to the function being satisfying CI it must also be balanced. A function ξ is said to be balanced given then its Haar global spectral coefficient is zero [10]. That is, if its Haar spectrum satisfies Equation. 11 (see below). The next proposition summarizes the Haar spectral generalization for order one resiliency.

$$\xi_H(0) = 0 \quad (11)$$

Proposition 3.3 An *n*-variable Boolean function *f* (with sign function ξ), is said to be resilient of order 1 ($R(1)$) provided that the following conditions on its HSV ($\overrightarrow{S\hat{F}_H}(u)$) holds, $\forall u \ni 0 \leq u \leq n+1$

$$\overrightarrow{S\hat{F}_H}(u) = 0 \quad (12)$$

Proof: The proof of the proposition follows directly from proposition 3.1 and Equation. 11. This ends the proof.

On the other hand, the Haar generalization for higher order resiliency can be summarized based on the following proposition.

Proposition 3.4 An *n*-variable Boolean function *f* (with sign function ξ), is said to be resilient of order k ($R(k)$) provided that the following conditions on its Haar spectrum ($\xi_{H_l^q}$) holds, $\forall u \ni 0 \leq u \leq n+1$

$$\sum_{q,\omega \in \mathbb{F}_2^l} \xi_H^l(q) \cdot (-1)^{\omega \cdot q} = 0 \ \wedge \ \xi_H(0) = 0 \quad (13)$$

Proof: The proof of the proposition follows directly from proposition 3.2 and Equation. 11 by extending the correlation immune function to be balanced. *This ends the proof.*

The next question at this juncture is simply: How does one differentiate a resilient function from being a linear or affine function. This has to be considered due to the fact that, the nonzero values of the Haar spectrum of such functions are restricted to a specific zone of the spectrum where the rest of the zones are zeroes. The difference is based on the magnitude of the nonzero coefficients presented in the preliminary section through Equation. 7 and Equation. 8 respectively. The following Lemma guarantees the resilient function to be a nonlinear function. We give the lemma here without a proof as the Haar definition of linear functions is sufficient on its own.

Lemma 3.1 A Boolean function ξ is a nonlinear resilient function of order *k* if it satisfies Equation. 13 and the following is true for all its Haar spectral zones

$$\sum_q \left|\xi_{H_l^q}\right| \neq 2^n, \forall l \in [0,n) \quad (14)$$

The lemma simply guarantees a nonlinear function by restricting the transformed function from having maximum correlation with any given arbitrary *n*-variable linear or affine function.

The following section presents an algorithm for testing whether a given arbitrary Boolean function is correlation immune or not. The section also presents experimental results for the presented method.

EXPERIMENTAL RESULTS

In this section we give the results for an experiment conducted on the Haar-based method of measuring the correlation immunity of a given Boolean function. The results given here are related to the Haar-based algorithm (CI-test algorithm) for testing whether a given arbitrary Boolean function satisfies the correlation immunity or not.

The steps involved in the CI-test algorithm are given in the figure below (see Figure-1). The algorithm steps are direct as the first and second steps computes the Haar spectrum of the function and the corresponding sums over the zones respectively. The test for the CI criterion is performed in step 3 where the sums are tested. If all the zones' sums up to zero then, the function is correlation immune and the algorithm sets the logical *y* value to 1, otherwise the function does not satisfy the said criterion (*y* value set to 0). The last step outputs the value of *y*.

Experimental setup

The Haar-based algorithm together with the Walsh-Hadamard (Using MatLab built-in function) approach to testing the CI property, were simulated in a comparison experiment. The simulations were run for a number of iterations equal to 10, and the average execution time for each algorithm was recorded. The following table (see Table-2) presents a summary of the average execution times. The corresponding results are depicted in the figure below (see Figure-2). Note that, all the time measurements presented here are in "*seconds*" as a unit of measurements. All the algorithms were implemented using the MatLab software (MATLAB Version: 8.0.0.783 (R2012b)) on a laptop computer with the following specifications; Intel Core i5-2410M CPU @ 2.30GHz, 4.0GB RAM, 32-bit OS. The MatLab built-in function is the Fast-Walsh-Hadamard transform (FWHT), while our implemented Haar transform is the Fast-Haar-transform (FHT) based on the works of [3, 8].

Test Algorithm: CI Test
Input: An *n*-variable BF in polarity form, ξ
Output: 1 or 0
Steps:
Step 1: Compute the Haar spectrum of the function, ξ_H
Step 2: Compute the respective sum over the zones, $S\hat{F}_H(l), \quad l \in [0,n)$
Step 3: ***If*** $S\hat{F}_H(l) = 0 \ \forall l \in [0,n)$ ***then*** $y = 1$, ***Else*** $y = 0$
Step 4: Output y

Figure-1. Haar-based CI-test algorithm.

Table-2. CI-Test algorithm: Average execution times for $n = 3,4, \ldots ,10$.

n	$FWHT$	FHT
3	0.0009	0.0002
4	0.0010	0.0003
5	0.0012	0.0004
6	0.0016	0.0005
7	0.0024	0.0006
8	0.0044	0.0008
9	0.0083	0.0013
10	0.0119	0.0020

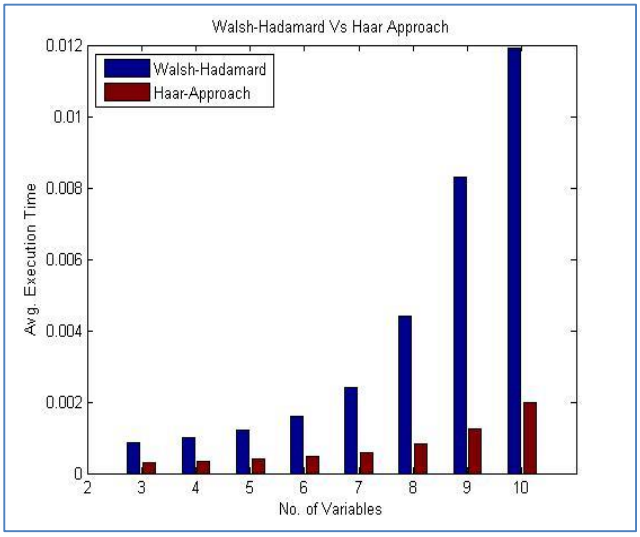

Figure-2. FWHT Vs FHT – Average execution time for CI test.

Results overview and discussion

It is clear from the experimental results that, the Haar-HSV approach has a better performance simply due to the fact that it has less number of operations involved. Still, the next obvious question then is, "What is the advantage of using the Haar method of approach here, and how is it advantageous?" In addition to better computational complexity compared to the Walsh approach, the Haar approach has another advantage as follows; the Haar local-based behavioural properties makes it possible for the algorithm to quit in the middle of the process if the condition has been violated. In other words, say for instance the algorithm was scanning down the spectrums with increasing number of zones. Now if at any moment in time the condition is violated before getting to the last zone then, the algorithm has the flexibility to quit the process at that exact point in time. In doing so, the algorithm does not need to check any further down the zones. On the other hand, the Walsh-based approach requires the complete Walsh spectrum to be computed first before checking whether the condition has been met or not. One thing to note as well is that, the worst case for the Haar approach is going through all the zones which is still advantageous in terms of performance and complexity. It should be noted for the higher order correlation immunity (proposition 3.2) that, in essence the equation given in the proposition reflects applying the Walsh-Hadamard transform to each of the Haar spectral zones independently. The order of transform depends on the degree defining the zone. An alternative view is that, instead of applying the Walsh-transform to the original Boolean function but rather applying it to the Haar spectrum of such function. In terms of complexity then, the worst case scenario will be that both the two methods have the same number of operations. The positive effect of the Haar method is that, each spectral zone can be processed independently. This is significant in the sense that, if each of the zones is treated independently as a separate vector then this allows the possibility of all of them to be processed at the same time in parallel rather than sequentially one after another. This flexibility arises out of the fact that, the processing of one zone does not require the outcome of another's and the zones can be considered through distributed arrays.

The following section presents the conclusion of the paper.

CONCLUSIONS

The strength of any conventional cipher system relies on the underlying cryptographic Boolean functions employed in the system. The design of such systems requires that the employed Boolean functions meet specific security criteria. Two of such criteria are the correlation immunity and resiliency of a given Boolean function. In this paper, we presented an alternative view of such criteria from the Haar spectral transform point of view. The Haar along with the Walsh are the two methods considered suitable for representing Boolean functions. The paper exploited the analogy between the two transforms to derive the Haar general representation of the correlation-immunity and the resiliency security criteria.

The paper presented the Haar-based conditions on which a given Boolean function should meet to be considered correlation-immune of order k $(CI(k))$ or resilient of order k $(R(k))$. In addition, the paper presented a Haar-based algorithm for testing correlation-immunity of an arbitrary Boolean function including experimental results related to the algorithm. The presented results were based on a simulation study of the Haar-based algorithm in comparison to its Walsh-counterpart. The results portrayed the computational advantage of the Haar method over the Walsh approach for the correlation-immunity measure. The paper included as well, a discussion on the worst-case scenario with advantages and flexibility of the Haar method in conjunction with the lower order Walsh transform. The Haar method provides the flexibility to view the transformed function from local behaviour

perspective in terms of its sub-functions. This property of the Haar makes it more convenient as the properties of the sub-functions of the transformed function can be viewed directly from the Haar spectrum of the original function.

Another flexibility of the Haar method as an advantage is that, it can be used along with the Walsh method as a hybrid method to analyse the respective Boolean functions. This property gives rise to the possibility of parallel processing of the Haar spectral zones in determining the presented cryptographic criteria. This hybrid approach is meant for further exploration in this research work. The work presented here is part of a research work conducted on analysis and synthesis of cryptographic Boolean functions.

ACKNOWLEDGEMENTS

The work presented here is partially funded by a grant from the IIUM Endowment Fund.

REFERENCES

[1] Thomas, C.W. and Pantelimon, S. 2009. Cryptographic Boolean Functions and Applications, Academic Press, Elseveir Inc.

[2] Carlet, C. 2010. Boolean Functions for Cryptography and Error Correcting Codes. In Crama, Y. and Hammer, P. L. (eds.) Chapter of the monograph Boolean Models and Methods in Mathematics, Computer Science and Engineering, published by Cambridge University Press, pp. 257-397.

[3] Karposky, M. G., Stanković, R. S. and Astola, J. T. 2008. Spectral Logic and Its Applications for the Design of Digital Devices, John Wiley and Sons, Inc.

[4] Kui, R., Jaemin, P. and Kwangjo, K. 2005. On the Construction of Cryptographically Strong Boolean Functions with Desirable Trade-Off, Journal of Zhejiang University Science, 6A (5): 358-364.

[5] Neiderreiter, H. (Ed.). 2002. Coding Theory and Cryptology, World Scientific Publishing Co. Inc., University Press Singapore.

[6] Read, M. 2007. Explicable Boolean Functions, Dissertation submitted in part fulfillment for the degree of MEng. In Computer Systems and Software Engineering, Department of Computer Science, The University of York.

[7] Stanković, R.S. and Falkowski, B.J. 2003. The Haar Wavelet Transform: Its Status and Achievement. Computers and Electrical Engineering, an International Journal. The Netherlands. vol. 29, pp. 25-44.

[8] Thornton, M.A., Miller, D.M. and Drechsler, R. 2001. Transformations amongst the Walsh, Haar, Arithmetic and Reed-Muller Spectral Domains. Proc 4th Intl. Workshop on Applications of Reed-Muller Expansion in Circuit Design. Victoria Canada. pp. 215-225.

[9] Rafiq, H. M. and Siddiqi, M. U. 2009. Haar Transformation of Linear Boolean functions. Proceeding of IEEE International Conference on Signal Processing Systems. Singapore. pp. 802-805.

[10] Rafiq, H.M. and Siddiqi, M.U. 3-5 July 20012. Analysis and Synthesis of Cryptographic Boolean Functions in Haar Domain: Initial Results. In Computer and Communication Engineering (ICCCE), 2012 International Conference on. Kuala Lumpur. pp. 566-569.

[11] S. Gao, Wenping M.A., Y. Zhao, and Z. Zhuo. 2011. Walsh Spectrum of Cryptographically Concatenating Functions and Its Applications in Constructing Resilient Boolean Functions. Journal of Computational Information Systems. 7(4), pp. 1074-1081.

[12] P. Charping and E. Pasalic. 2003. On Propagation Characteristics of Resilient Functions. *In:* NyBerg K, Heys H, eds. Selected Areas in Cryptography. LNCS 2595. Springer-Verlag, Berlin. pp. 175-195.

[13] Zhang W.G. and Xiao G.Z. 2009. Constructions of Almost Optimal Resilient Boolean Functions on Large Even Number of Variables. IEEE Trans. Inf. Theory, 55: 5822-5831.

[14] Zhang W.G. and Xiao G.Z. 2011. Construction of Almost Optimal Resilient Boolean Functions via Concatenating Maioran-McFarland Functions. Sci. China Inf. Sci, 54:909-912.

[15] Zhang W.G. and Pasalic E. 2014. Constructions of Resilient S-Boxes with Strictly Almost Optimal Nonlinearity through Disjoint Linear Codes. IEEE Trans. Inf. Theory, 60: 1638-1651.