Haar Spectrum based Construction of Resilient and Plateaued Boolean Functions

H. M. Rafiq
ECE Department
Faculty of Engineering, IIUM
Kuala Lumpur, Malaysia

M. U. Siddiqi
ECE Department
Faculty of Engineering, IIUM
Kuala Lumpur, Malaysia

ABSTRACT

Stream cipher systems are considered desirable and secure if composed of Boolean functions (B.Fs) that are characterized by high *resiliency*. Resiliency is one of the main cryptographic security criteria for a given Boolean function. One of the classes of functions satisfying high resiliency with desirable cryptographic properties include the Plateaued functions whose design construction is of significant interest. The main known methods for these functions' construction are based on the Walsh spectrum or the related truth table concatenations if not algebraic methods. This paper examines the Haar spectral transform as an alternative method for the design of such functions. As its contribution, the paper presents different methods utilizing the Haar spectral coefficients' distribution for the design of highly resilient functions including Plateaued functions. The paper presents two methods of approaches namely; design of resilient BFs within the current variable domain without considering lower variable domains and using the lower variable domains to construct resilient functions within the higher variable domain. In the process, a Haar based construction method of $(\boldsymbol{k+1})^{\boldsymbol{th}}$-order resilient functions from $\boldsymbol{k}^{\boldsymbol{th}}$-order resilient functions is derived and presented. The presentation shows the advantage of the Haar based method compared to the existing Walsh benchmark. The paper demonstrates that it is possible with the Haar based method of approach to see directly the local properties of a given $\boldsymbol{n}$-variable BF with respect to its sub-functions from $\boldsymbol{r}$-variable domains $(\boldsymbol{r < n})$ without considering the spectra of the respective sub-functions. On the other hand, the Haar local behavioral properties related to the transformed functions provide the possibility to enumerate different types of resilient functions including the Plateaued functions.

General Terms

Boolean Functions, Private Key Cryptography, Stream Ciphers, Spectral Analysis.

Keywords

Cryptographic Boolean Functions, Haar/Walsh Transforms, Haar Spectrum, Spectral Coefficients, Cryptographic Security Criteria, Construction Methods and Resiliency.

1. INTRODUCTION

A strong stream cipher requires that the employed Boolean function within the system does not lose the system's statistical information as well as being resistant to correlation attacks. For the system to reach such level of security, the designer of the system has to ensure that the BF deployed for the system satisfies the resiliency property [1,2,3,4,5]. The question of how such functions are constructed has been covered within literature and most of the existing works are either based on the Walsh transform or truth table concatenations if not algebraic approach. Majority of these approaches build up an n-variable resilient function by using lower variable resilient functions through mostly concatenation of such lower domain functions [1,2,3]. On the other hand, a lot is known on the characteristics of the Plateaued class of resilient functions and yet not much on their methods of construction [2].

This paper presents such construction of resilient functions based on the Haar spectral transform as an alternative method of approach. The Haar in this sense provides a better alternative view of such functions since it makes it possible to view both the current variable domain as well as the lower variable domain at the same time. This possibility is based on the fact that the Haar spectrum is characterized by the local behavioral view of the transformed function. The paper presents Haar based methods on which the resilient functions can be constructed. The methods are considered for different restrictions on the Haar spectral coefficients and their related zones. The derivations are based on absolute flat spectral zones as well as mixed zero and nonzero spectral coefficients within zones of the respective Haar spectrum. In the process, the paper examines the presented construction methods and derives their connection to Plateaued functions. Additionally, the Haar based construction method from lower order resiliency to higher order is presented. It is demonstrated in the presentation that, the Haar spectrum provides more ways on which the resilient functions can be considered and possibly opens a door for further enumeration of such functions.

The paper is organized as follows. Section 2 presents an overview of Boolean functions including the spectral transform methods and some of the known results to be employed in the later sections. Also covered are some Haar extensions on the existing Walsh construction methods. In section 3, the various Haar based methods of constructing resilient functions are presented in four different sub-sections. Each of the sub-section reflects on different aspects of Haar spectral characterization and distribution of resilient functions. The section derives construction methods by looking at Haar spectral zones' distribution and whether the zones are absolute flat or mixed between zero and nonzero coefficients. Included in the section as well are the Plateaued functions from Haar point of view and the construction of higher order resilient functions from lower order ones. Finally, section 4 presents the conclusion of the paper along with the related discussion on future work.

2. OVERVIEW

2.1 Boolean Functions

The mapping of n input bits $((x_1, \dots, x_n) \in \mathbb{F}_2^n)$ to a single output bit $(f(x) \in \mathbb{F}_2)$ defines what is called an n-variable Boolean function (BF) $f(x_1, \dots, x_n)$. Any given BF f in B_n

(B_n is the set of all BFs) can be represented uniquely in several ways including; the binary truth table, the polarity truth table, and the algebraic normal form [1, 2]. These are the main representations which are of interest to this work.

The ordered tuple defined by f ($f \in \mathbb{F}_2\}$): $f = \left(f\left(x^{(0)}\right), f\left(x^{(1)}\right), \dots, f\left(x^{(2^n-1)}\right)\right)$ and constitutes outputs of the function for all possible 2^n input combinations, is referred to as the *binary truth table* of *f*. Note that $x^{(0)} = (0, \dots, 0)$, $x^{(2^n-1)} = (1, \dots, 1)$, and $k = \sum_{i=1}^{n} 2^{n-i} x_i$, where the binary vector $x^{(k)}$ represents the integer k $(0 \le k \le 2^n - 1)$. Sometimes instead of using the binary form of the function, it is more convenient to employ its corresponding real valued form which is referred to as the *sign function*. The *sign function* is denoted by $\hat{f}$ and also called the *polarity truth table* (resp. *sequence* of *f*), takes values from the set $\{-1,1\}$ and is defined as $\hat{f}(x) = (-1)^{f(x)} \equiv 1 - 2f(x), \forall x \in \mathbb{F}_2^n$. On the other hand, the representation of the BF *f* defined by $f = a_0 \oplus a_1 x_1 \oplus \cdots \oplus a_{12} x_1 x_2 \oplus \cdots \oplus a_{12\cdots n} x_1 x_2 \cdots x_n$ $(a_i, x_i \in \mathbb{F}_2)$ is called the *Algebraic Normal Form* (*ANF*) where the expression of the function is uniquely given as a sum (XOR) of products (AND).

The number of variables in the product terms of the ANF defines the *degree* of f (denoted as $\deg(f)$) and the number of nonzero entries in a function's truth table defines the *weight* (denoted as $wt(f)$) of the function. A function is considered as *balanced* if it contains equal number of zeros and ones in its truth table (equivalently $wt(f) = 2^{n-1}$).

Affine and Linear Boolean Functions: An *n*-variable BF defined and denoted generally as $L_\omega = \omega_1 x_1 \oplus \omega_2 x_2 \oplus \cdots \oplus \omega_n x_n$ is called a *linear* BF, which is selected by $\omega \in \mathbb{F}_2^n$. *Affine* functions on the other hand, are complements of the linear functions and defined as $f = c \oplus L_\omega$ where $c \in \mathbb{F}_2$. Note that, all the linear functions are contained in the set of affine functions. For the purpose of the work presented here, the notation ${L^k}_\omega$ means a *k*-variable linear function.

2.2 Spectral Transforms

This section looks at the Haar and Walsh spectral transforms, which are the two main transforms considered suitable for representation of Boolean functions. The section also presents some of the existing results that will be employed in the subsequent sections of the paper.

Throughout this paper the following notations and abbreviations will be assumed: *WH*, *WP* are the Walsh-Hadamard and Walsh-Paley orderings respectively; $\vec{y}_j$ is the *j*-th row (*Y* function) in the respective transform matrix; $\vec{r}_{0_s}$ is a row-vector whose elements are all ones $(\vec{1})$ with size as 1×2^s; $\vec{r}_{1_s}$ is a balanced row-vector whose first half elements are all ones and the second half elements are all negative-ones with size 1×2^s;

Walsh-Hadamard Transform (WHT) of a function $\hat{f}$ on $\mathbb{F}_2^n$ is denoted by $\hat{F}_{WH}$ and given by [1, 2]:

$$\hat{F}_{WH}(u) = \textstyle\sum_{x,u \in \mathbb{F}_2^n} (-1)^{f(x) \oplus x \cdot u} \qquad (1)$$

The **Walsh-Paley** Matrices ($[WP_n]$): These matrices are just Walsh transform matrices in Paley ordering and are given by [7,8] ($\forall\, i \in [0, 2^{n-1})$)

$$[WP_n] = \left[\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \overrightarrow{rp}_{i_{n-1}}\right] \text{ And } \; [WP_0] = [1] \qquad (2)$$

Where, $\otimes$ is the Kronecker product and $\overrightarrow{rp}_{i_{n-1}}'s$ are the rows of the previous lower order matrix ($[WP_{n-1}]$). Consequently, the rows in the interval $[2^l, 2^{l+1})$ (in $(n-1)^{th}$-order) will produce the rows in the interval $[2^{l+1}, 2^{l+2})$ (in the $(n)^{th}$-order). Note that the rows $[2^l, 2^{l+1})$ defines the sub-matrices of the $[WP_n]$.

Haar Functions: The set of Haar functions H_l^q (resp. H_j) are defined as un-normalized over the input interval of $[0, 2^n)$ and taking values of 0 and ± 1. They form a complete set of orthogonal rectangular basis functions [5,6,10] and their definition is given as follows:

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

$$H_j(x) = \begin{cases} 1, & u_0 \cdot 2^{n-l-1} \le x < u_1 \cdot 2^{n-l-1} \\ -1, & u_1 \cdot 2^{n-l-1} \le x < u_2 \cdot 2^{n-l-1} \\ 0, & \quad else\ in\ [0, 2^n) \end{cases} \qquad (3)$$

Where $u_i = 2q + i$; l and q are degree and order of the Haar functions respectively. With $j = 2^l + q$ and for each value of $l = 0, 1, \dots, n-1$, the orders are $q = 0, 1, \dots, 2^l - 1$. The Haar spectral zones are defined by the respective degrees locally.

Haar Transform: the Haar transform ($\hat{F}_H$) of $\hat{f}$ is defined by [5,6,10]:

$$\hat{F}_H(j) \;= \textstyle\sum_{x=0}^{x=2^n-1} H_l^q(x) \cdot \hat{f}(x) \equiv \sum_x H_j \cdot \hat{f}(x) \qquad (4)$$

An important alternative and equivalent definition of the Haar functions was given in [5] and further utilized in [13] to define the Haar spectrum as:

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

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 [13]. It is very important to note that, every Haar spectral coefficient is a correlation between the transformed B.F f and the sub-linear function $\vec{r}_{1_{n-l}}$. The correlation is over dyadic sub-intervals of the BF.

2.3 Known Results and Some Extensions

Resiliency [1,2]: An *n*-variable Boolean function $\hat{f}$ is resilient of order *k* if and only if its Walsh ($\hat{F}_{WH}$) and Haar spectra satisfies the conditions given by (6) [1,2, 4,5,11-15] and (7) [13] respectively

$$\Rightarrow\; \hat{F}_{WH}(\omega) = \textstyle\sum_{x \in V_n} (-1)^{f(x) \,\oplus\, x \cdot \omega} = 0, \qquad (6)$$
$$\forall\, \omega \ni 1 \le wt(\omega) \le k \;\wedge\; \hat{F}_{WH}(0) = 0$$

$$\Rightarrow\; \textstyle\sum_{q,\omega \,\in\, \mathbb{F}_2^l} \hat{F}_H^l(q) \cdot (-1)^{\omega \cdot q} = 0, \qquad (7)$$
$$\forall q \ni 1 < wt(q) \le k - 1 \;\wedge\; \hat{F}_H(0) = 0$$

Note that, a function that is resilient of order *k* is indeed a balanced correlation-immune function of the same order. It was also stressed out in [13] that the Haar spectrum of a nonlinear resilient function should satisfy the following condition given by (8). The condition ensures that the transformed function does not have maximum correlation with a linear or affine function [13].

$$\textstyle\sum_q \left|\hat{F}_{H_l^q}\right| \ne 2^n, \forall l \in [0, n-1) \qquad (8)$$

The same representations and derivations given in [13] can be used to extend the following theorem (see Theorem 1) which was presented in [1]. The theorem deals with the concatenation (based on (9)) of two k-th order resilient functions to form a $(k+1)\text{-}th$ order resilient function. The extension is simply on the second condition of the theorem where the Haar spectral coefficients can be used in place of the Walsh coefficients as according to (10).

$$f(x, x_{n+1}) = x_{n+1} f_1(x) \oplus \bar{x}_{n+1} f_2(x) \qquad (9)$$

Theorem 1 [1]: Given that $x = (x_1, x_2, \ldots, x_n)$, and suppose that f_1, f_2 and f are related by equation (9) where the first two functions are *n*-variable functions while the third one (f) is $n+1$-variable function. Then, for $k < n-1$, f is $(k+1)$-resilient if and only if the following two conditions hold

i. The two functions f_1 *and* f_2 are k-resilient
ii. $\forall\, v \in \mathbb{F}_2^n \ni wt(v) = k+1$ then the Walsh transform satisfies $F_{1_{WH}}(v) + F_{2_{WH}}(v) = 0$

The condition ii of the theorem in Haar representation is then given simply as according to the following equation

$$\textstyle\sum_{q,v \in \mathbb{F}_2^l} \hat{F}_{1_H}^{\,l}(q) \cdot (-1)^{v \cdot q} + \sum_{q,v \in \mathbb{F}_2^l} \hat{F}_{2_H}^{\,l}(q) \cdot (-1)^{v \cdot q} = 0\,,$$
$$\forall\, q \in \mathbb{F}_2^l \ni wt(q) = k \qquad (10)$$

Additionally, the theorem gives the condition relating the degrees of the involved functions. If all the functions' degrees are equal, then *f* would have the maximum degree of *n*+1-(*k*+2) if and only if the other two source functions have their max degree of *n*-(*k*+1) [1].

The Haar transform of a given linear BF is defined by [11, 13]:

$$\hat{L}_H(x) = 2^{n-l} \cdot \begin{cases} L^l{}_\omega(q), & \omega, q \in \mathbb{F}_2^l, x = 2^l + q \\ 0, & otherwise \end{cases} \qquad (11)$$

The **Haar-Sum-Vector** (HSV) [13]: let the sum of Haar spectral coefficients over the zone defined by l ($l = 0,1,\ldots,n-1$) be given by $S\hat{F}_H(l) = \sum_{x=2^l}^{2^{l+1}-1} \hat{F}_H(x)$, then the HSV denoted by $\overrightarrow{S\hat{F}_H}$ is a $1 \times (n+1)$ vector containing all the zones' spectral sums including the Haar global spectral coefficient. In this sense the HSV is defined as:

$$\overrightarrow{S\hat{F}_H}(u) = \left[\hat{F}_H(0),\ S\hat{F}_H(0), S\hat{F}_H(1), S\hat{F}_H(2), \ldots, S\hat{F}_H(n-1)\right] \qquad (12)$$

The following section explores the Haar based construction of resilient functions

3. HAAR BASED CONSTRUCTION OF RESILIENT FUNCTIONS

This section derives different construction methods for resilient functions based on their Haar spectral characterization. Each of the following section considers various specific methods of approach.

3.1 The Last Haar Spectral Zone and the Absolute Nonzero Flat Spectrum

This section considers the last zone of the Haar spectrum for a given arbitrary function. But before proceeding, it is significant to introduce the following notions relating to any given BF.

Let a given *n*-variable BF f constitute a dyadic ($i = 2^t, t \geq 1$) concatenation of sub-functions $f^{(i)}$ and defined as $f = f^{(0)} \| f^{(1)} \| \ldots \| f^{(2^t-1)}$, then it is obvious that the lowest number of sub-functions is when $t = 1$ giving two sub-functions as $f^{(0)}$ and $f^{(1)}$. On the other hand, the highest number of sub-functions is when $t = n-1$ giving a total of 2^{n-1} sub-functions. The interest of this section is therefore when $t = n-1$ and in this sense the sub-functions are defined either by $\vec{r}_{1_1}$ or $\vec{r}_{0_1}$ as given by the equation (13). The following example (Example 1) demonstrates this for a *three* variable case:

$$f^{(i)} = \pm\vec{r}_{1_1} = \pm[1,-1] \quad or \quad f^{(i)} = \pm\vec{r}_{0_1} = \pm[1,1] \qquad (13)$$

Example 1: Consider the linear function $\hat{L} = [1,-1,1,-1,-1,1,-1,1]$ and the arbitrary function $\hat{f} = [1,1,1,-1,-1,1,-1,-1]$. The linear function can be written as a concatenation of $\vec{r}_{1_1}$ as $\hat{L} = [\vec{r}_{1_1} \| \vec{r}_{1_1} \| -\vec{r}_{1_1} \| -\vec{r}_{1_1}] \equiv [\vec{r}_{1_1}, \vec{r}_{1_1}, -\vec{r}_{1_1}, -\vec{r}_{1_1}]$. On the other hand, the second function is given by $\hat{f} = [\vec{r}_{0_1} \| \vec{r}_{1_1} \| -\vec{r}_{1_1} \| -\vec{r}_{0_1}] \equiv [\vec{r}_{0_1}, \vec{r}_{1_1}, -\vec{r}_{1_1}, -\vec{r}_{0_1}]$. The functions' respective Haar transforms are given in the following table (see Table 1 below) including the distribution for the linear function defined by (11):

Table 1. Spectra for Example 1

x	$\hat{f}(x)$	$\hat{F}_H(x)$	$\hat{L}(x)$	$\hat{L}_H(x)$	$L^2{}_\omega(q)$
0	1	0	1	0	
1	1	4	-1	0	
2	1	2	1	0	
3	-1	2	-1	0	
4	-1	0	-1	2	+
5	1	2	1	2	+
6	-1	-2	-1	-2	−
7	-1	0	-1	-2	+

It is clear from the table that, L^2 represent the distribution of the sub-functions $\vec{r}_{1_1}$ (when 2 is factored out) as concatenation forming up the original linear function. This point to the most important fact that whenever a given arbitrary BF constitutes a concatenation defined by the distribution of only $\pm\vec{r}_{1_1}$as sub-functions, then all the other spectral zones ($l \neq n-1$) will contain only zero spectral coefficients. This key idea is summarized in the following proposition for the conditions on the Haar spectral coefficients' distribution of a given resilient function.

Proposition 1: let f be an *n*-variable Boolean function with polarity representation given by $\hat{f}$, and the Haar spectrum of its polarity form as $\hat{F}_H$. If the Haar spectrum of the function satisfies the following conditions,

1. The corresponding HSV has only zero elements: $\overrightarrow{S\hat{F}_H}(u) = 0, \forall u \in [0, n+1)$
2. The nonzero Haar spectral coefficients are restricted within the last zone of the spectrum ($l = n-1$) with the following balanced distribution: $$\hat{F}_H(x) = \begin{cases} \pm 2, & 2^{n-1} \leq x < 2^n \\ 0, & otherwise \end{cases}$$
3. The spectral coefficients' distribution is nonlinear (does not satisfy the L_ω^{n-1} distribution)
4. The sum over the absolute spectral coefficients is given by $\sum_x |\hat{F}_H(x)| = 2 \cdot 2^{n-1} = 2^n$

Then, the function f is **a balanced nonlinear resilient** function

Proof: The proof of the proposition follows directly from the definition of resiliency. Assuming the conditions of the proposition have been satisfied, then the proof requires to show that the function is balanced and correlation immune. Using the Haar definition, the function is already balanced since the initial spectral coefficient is ($\hat{F}_H(0) = 0$) zero by the conditions 1 and 2 of the proposition. For the correlation immunity, all that needs to be done is to show that the sum of the spectral coefficients for each zone is zero. Now based on the elements of the HSV, all the sums are zeroes meaning that the transformed function is correlation immune by the Haar definition. At this point, the remaining question is whether the function is linear or not. Since the spectral distribution of the coefficients does not satisfy the L_ω^{n-1} distribution (conditions 3 and 4) then, the transformed function is not linear. Given that the function is not linear then the sum (sum_{n-1}) over the nonzero spectral coefficients is given by,

$$sum_{n-1} = \textstyle\sum_{x=2^{n-1}}^{2^n-1} \hat{F}_H(x) \equiv \sum_q \hat{F}_{H}{}_{n-1}^{q}(x)$$

$$\equiv 2\left(\textstyle\sum_{x\ni(\hat{F}_H=1)} \hat{F}_H(x) + \sum_{x\ni(\hat{F}_H=-1)} \hat{F}_H(x)\right)$$

$$\equiv 2\cdot 0 \equiv 0$$

Whereby, the balanced distribution (condition 2) guarantees the sum to be zero. Since the sum is zero and again by the definition of resiliency together with conditions 3 and 4, then f is a balanced nonlinear resilient function. □

The proposition 1 gives a method of approach to designing a balanced nonlinear resilient function by only ensuring conditions 2 and 3 of the proposition are satisfied. Once these two conditions are satisfied, the rest of the conditions follows suit. The question then is how to ensure that condition 3 is satisfied and the best way to do this is by exploiting on the linear distribution given by L_ω^{n-1}. The process then involves manipulating the linear distribution to transform it to nonlinear distribution. The simplest way of achieving this is by expressing the L_ω^{n-1} as a concatenation of lower variable distributions for instance $L_\omega^{n-1} = [L_\omega^{n-2}\|L_\omega^{n-2}]$. The summary of the steps involved in this construction algorithm (based on proposition 1) is given in the following figure (see Figure 1).

Algorithm 1: Construction Algorithm for Resilient Functions

Input: Number of variables, n

Output: Resilient function, $\hat{f}$

Steps:

Step 1: Pick two unique sub-matrices of the Paley matrix of order $n-1$

Step 2: Pick any two unique balanced L_ω^{n-2} distributions from the two sub-matrices.

Step 3: Concatenate the two L_ω^{n-2} distributions to form the spectral coefficients for the last zone of the Haar spectrum.

Step 4: Use the distribution for the sub-functions $\vec{r}_{1_1}$ to construct the respective resilient function, $\hat{f}$

Step 5: Output $\hat{f}$

Figure 1: Algorithm 1 – Proposition 1 Based Construction Algorithm for Resilient Functions

It should be noted that, the first step of the algorithm involves picking up the sub-matrices defined by degree greater than one. These sub-matrices contain rows whose distribution follows the L_ω^{n-1} linear distribution, and half of such rows contain elements of the balanced L_ω^{n-2} linear distribution. The unique L_ω^{n-2} linear distributions from the two choices of rows within the different sub-matrices (step 2 of the algorithm), are then employed for the construction of the resilient function (steps 3 and 4 of the algorithm). The last step outputs the constructed resilient function. The following example demonstrates the steps of the construction algorithm.

Example 2: Consider a 4-variable case, the Walsh-Paley matrix of order 3 and its sub-matrices are given in the Figure 2 below. In this case, there are only two unique sub-matrices (from the figure) that constitute L_ω^3 linear distributions which can be split into balanced L_ω^2 distributions (step 2 of Algorithm 1). Included in the figure as well, are the possible combinations (red and green colors) or concatenations of unique L_ω^{n-2} linear distributions (excluding their complements). Any such concatenation defines the step 3 process in the construction algorithm based on proposition 1. Then choosing the concatenation, $[+\ +\ -\ -\|+\ -\ +\ -]$ for step 3 of the Algorithm 1, gives the following spectral coefficients for the last zone of the Haar spectrum: $[2,2,-2,-2,2,-2,2,-2]$. The resulting distribution is then utilized over the sub-functions $\vec{r}_{1_1}$ to construct the respective resilient function as $\hat{f} = [\vec{r}_{1_1}, \vec{r}_{1_1}, -\vec{r}_{1_1}, -\vec{r}_{1_1}, \vec{r}_{1_1}, -\vec{r}_{1_1}, \vec{r}_{1_1}, -\vec{r}_{1_1}] = [1,-1,1,-1,-1, 1,-1,1,1,-1,-1,1,1,-1,-1,1]$. It can easily be verified that the Haar spectrum of the resulting function consist of nonzero spectral coefficients only within the last spectral zone and that the function is indeed resilient. *This Ends the Example*

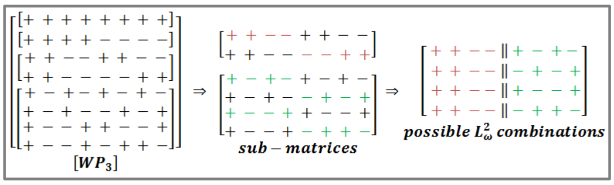

Figure 2: Walsh-Paley Matrix of Order 3 with its two Unique Sub-Matrices and their Possible Unique Combinations

Remark: An important point to make is that, the concatenation of the unique L_ω^{n-2} linear distributions under context can be viewed directly from the current variable domain of n. In other words, this process coincides with the construction of such resilient functions from the existing literature where the consideration is truth table concatenation of lower variable linear functions [1,2,14]. The Haar method gives this view from the current domain due to its local behavioral properties related to the transformed BF.

The following sub-section examines the mixture of zeroes and nonzero spectral coefficients within different zones.

3.2 Zones with Mixed Zeroes and Nonzero Spectral Coefficients

The consideration in this section is not the same as the previous construction (section 3.1) of resilient functions but rather on the last zone of the spectrum being not absolute flat. In this sense, the focus then shifts to the other zones of the spectrum defined by degrees $0 < l < n-1$. Specifically, when these zones are absolute flat taking values half the number of nonzero values of the corresponding transforming Haar functions. The following proposition summarizes the conditions on the Haar spectral coefficients within the zones for a given BF to be resilient.

Proposition 2 – Haar Based Resilient Construction: let f be an n-variable Boolean function with polarity representation given by $\hat{f}$, and the Haar spectrum of its polarity form as $\hat{F}_H$. If the Haar spectrum of the function satisfies the following conditions,

1. The spectral coefficients for $x < 2^{n-1}$ satisfy the following conditions

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

2. The flat spectral zones follow a balanced distribution that is linear in terms of the ± signs $(2^{n-l-1} \cdot L_\omega^l)$ $\sum_{\mathrm{x}=2^l}^{2^{l+1}-1} \hat{F}_H(x) = 0,\ \forall l \in [1, n-2)$
3. The last zone's spectral coefficients satisfy balanced distribution between zero and nonzero coefficients with $\sum_x \hat{F}_H(x) = 0,\ x \in [2^{n-1}, 2^n)$

Then, the function f is **a balanced nonlinear resilient** function

Proof: The proof of the proposition follows the same idea as the previous proposition. The transformed function is balanced since the initial spectral coefficient is $(\hat{F}_H(0) = 0)$ zero by the condition 1 of the proposition. Similarly for the correlation immunity, all that needs to be done is to show that the sum of the spectral coefficients for each zone is zero. The initial zone $(l = 0)$ and the last zone $(l = n - 1)$ both satisfy the Haar correlation definition as according to the conditions 1 and 3 respectively of the proposition. The only thing left for consideration is the flat spectral zones; now condition 2 guarantees that the zones satisfy the Haar correlation immunity property (defined by (7)). As all the spectral coefficients satisfy the Balanced and Correlation immunity conditions, the respective function f then is a balanced nonlinear resilient function. □

Example 3: Proposition 2 can help in constructing resilient functions with a distribution of more nonzero spectral coefficients over the Haar spectrum through different zones rather than within only one zone. The following table (see Table 2 below) gives example of functions created based on the proposition for 4-variable functions. Note that the different zones within the Haar spectra are color coded differently so as to clearly observe the related conditions.

Table 2. 4-Var Resilient Functions Based on Proposition 2

x	$\hat{f}_1(x)$	$\hat{f}_2(x)$	$\hat{f}_3(x)$	$\hat{F}_{1H}(x)$	$\hat{F}_{2H}(x)$	$\hat{F}_{3H}(x)$
0	1	-1	1	0	0	0
1	1	1	1	0	0	0
2	1	1	1	4	4	4
3	-1	1	-1	-4	-4	-4
4	-1	-1	-1	2	-2	2
5	-1	-1	1	-2	-2	2
6	-1	1	-1	-2	2	-2
7	1	-1	-1	2	2	-2
8	-1	-1	-1	0	-2	0
9	-1	1	-1	2	0	2
10	1	-1	1	0	0	-2
11	-1	-1	-1	-2	2	0
12	1	1	-1	0	-2	0
13	1	1	1	2	0	2
14	-1	1	1	0	0	-2
15	1	-1	1	-2	2	0

Remark: One key observation within the last spectral zones of these functions is that, there is a unique spectral coefficients' distribution that holds when the zone is split into two sub-intervals. The two consecutive sub-intervals in this sense contain the same balanced distribution of the spectral coefficients. This behavior reflect the Haar based local properties of a given function and hence the balanced property locally for correlation immunity.

The next section presents a review on Plateaued functions and how they are related here within the Haar spectral domain.

3.3 Plateaued Functions

The Plateaued functions [1,2,14] or three-valued functions [1,2,15,16] are considered as functions with desirable cryptographic properties and their Walsh spectral coefficients assume values of either 0 or $\pm 2^\lambda$. Looking back at Proposition 1 given in the previous section then it can be noted that the resulting resilient functions are in fact Plateaued functions in the sense that their corresponding Walsh spectra would contain only three values. The following proposition summarizes this relationship.

First, it should be noted that the Haar based definition of resilient given in (7) is nothing other than the use of the Haar transform in place of the Walsh-Hadamard transform. That is, the left-hand-side (LHS) of (7) represents a specific Walsh-spectral coefficient and this connection between the two transforms is through different zones [13].

Proposition 3: The resilient function f based on Proposition 1 is a *Plateaued* function.

Proof: The proof follows the definition of a Plateaued function that its Walsh spectrum consists of either zero values or $\pm 2^\lambda$. The starting point is with all spectral coefficients defined by $x < 2^{n-1}$ where the first two global coefficients $\hat{F}_H(0)$ and $\hat{F}_H(1)$ $(l = 0)$ are same as Walsh coefficients $(\hat{F}_{WP}(0)$ and $\hat{F}_{WP}(1)$ resp.) which are both zeroes. Now for the other zones defined by $0 < l < n - 1$, it can be clearly seen that their Walsh coefficients are all zeroes since $\sum_{q,\omega\, \in\, \mathbb{F}_2^l} \hat{F}_H^l(q) \cdot (-1)^{\omega \cdot q} = \sum_{q,\omega\, \in\, \mathbb{F}_2^l} 0 \cdot (-1)^{\omega \cdot q} = 0.$ The only remaining zone is the last zone defined by $l = n - 1$ and whose Walsh coefficients are given by

$$\sum_{q,\omega\, \in\, \mathbb{F}_2^{n-1}} \hat{F}_H^{n-1}(q) \cdot (-1)^{\omega \cdot q} = \sum_{q,\omega\, \in\, \mathbb{F}_2^{n-1}} (\pm 2) \cdot (-1)^{\omega \cdot q}$$

$$= \pm 2 \cdot \sum_{q,\omega\, \in\, \mathbb{F}_2^{n-1}} (L_\omega^{n-1}) \cdot (-1)^{\omega \cdot q}$$

$$= \pm 2 \cdot \Big[\sum_{q,\omega\, \in\, \mathbb{F}_2^{n-2}} (L_\omega^{n-2}) \cdot (-1)^{\omega \cdot q}$$

$$+ \sum_{q,v\, \in\, \mathbb{F}_2^{n-2}} (L_v^{n-2}) \cdot (-1)^{v \cdot q}\Big] = 0 \ or\ \pm 2^{n-1}$$

The respective Walsh coefficient is zero if $\omega, v \neq q$, otherwise it is 2^{n-1} when either $\omega = q$ or $v = q$ (both ω and v cannot be equal to q at the same time). When one of them equals q then the respective sum equals the length of the corresponding sub-linear function $(\|L_\omega^{n-2}\|\ or\ \|L_v^{n-2}\|)$ which is 2^{n-2}. When the length multiplied by the factored coefficient $(\pm 2 \cdot 2^{n-2})$ then the resulting Walsh coefficient becomes $\pm 2^{n-1}$. Where the negative is incase $(-1)^{\omega \cdot q}$ is a complement of L_ω^{n-2} (similar for $(-1)^{v \cdot q}$ and L_v^{n-2}). Since the Walsh coefficients can take only one of the three values $0\ or\ \pm 2^{n-1}$, the transformed function f is then a *Plateaued* function. □

For the resilient functions generated by proposition 2 on the other hand, there should be an extra condition with regards to the last spectral coefficients for the resulting function to be a *Plateaued* function. The following proposition summarizes this condition.

Proposition 4: A resilient function f generated based on proposition 2 can be a Plateaued function if its Haar spectrum satisfies the given 3 conditions (proposition 2's) and the following holds:

$$\sum_{q,\omega\, \in\, \mathbb{F}_2^{n-1}} \hat{F}_H^{n-1}(q) \cdot (-1)^{\omega \cdot q} = 0, \pm 2^{n-1} \qquad (14)$$

Proof: The proof of the proposition is straight forward as the first two global coefficients are zeroes (condition 1 of proposition 2). For the flat spectral zones ($1 < l < n - 1$) it can be easily verified that the corresponding Walsh coefficients ($\sum_{q,\omega \in \mathbb{F}_2^l} \hat{F}_H^l(q) \cdot (-1)^{\omega \cdot q}$) can only take either 0 or $\pm 2^{n-l-1} \cdot 2^l = \pm 2^{n-1}$. This is true since the 2^{n-l-1} value can be factored out and the resulting spectral coefficients are linear (L_ω^l) and whose Walsh transform is either 0 or $\pm 2^l$ depending on the linear distribution and by the Walsh definition of linear functions. The new condition introduced by the proposition ensures that the Walsh coefficients based on the last Haar spectral zone assume the same values ($0\ or \pm 2^{n-1}$) as the other Haar spectral zones. □

Remark: For Proposition 3, the resulting λ is equivalent to $2^{\frac{n}{2}+1}$ for the case of 4-variable functions. The construction methods presented here (Propositions 1 and 2) can be used on their own for any given number of variables of at least **four** (for resilient functions). These methods can as well be used in conjunction with the existing methods such as the one given in [1,2,17], through combination of lower variable functions satisfying the resilient criterion. The Haar approach can be integrated with the Walsh and used as hybrid (Haar-Walsh) as well with better results [13].

3.4 Higher Order Resiliency from Lower Order Ones

The following theorem generalizes the condition on which one may be able to use only one resilient function of order *k* in *n*-variables to obtain a function in *n*+1-variables that is resilient of order *k*+1.

Theorem 2: Suppose that $\hat{f}$ is a k resilient sign function in n-variables and suppose the following holds for some Haar spectrum $\hat{G}_H$ of an $n + 1$-variable sign function $\hat{g}$

$$\hat{G}_H(x) = \begin{cases} 0, & x < 2^{n-1} \\ 2\hat{f}, & 2^{n-1} \le x < 2^n \end{cases} \tag{15}$$

Then, $\hat{g}$ is resilient of order $k + 1$

Proof: The proof of this theorem follows directly from the Haar based definition of resilient function. Since the spectrum contains only zero values for higher spectral zones ($x < 2^{n-1}$), so the only thing left to do is just to see the last zone of the spectrum through the Haar definition of correlation given in (7) as follows

$$\sum_{q \in \mathbb{F}_2^{n-1}} \hat{G}_H^{n-1}(q) \cdot (-1)^{\omega \cdot q} = \sum_{q \in \mathbb{F}_2^{n-1}} \hat{f}(q) \cdot (-1)^{\omega \cdot q}$$

$$= \sum_{q \in \mathbb{F}_2^{n-1}} \hat{f}(q) \cdot (-1)^{\omega \cdot q}$$

$$= 0,\ \ni 0 \le wt(q) \le k \qquad (\hat{f} \text{ is a } k \text{ resilient})$$

$\Rightarrow \quad \hat{g}$ is $k + 1$-resilient (By Haar definition). □

The Haar design algorithm based on Theorem 2 is given in the figure below (Figure 3). The algorithm can be used in this case for designing resilient functions satisfying higher order given lower order functions. What the algorithm does in the figure is simply ensuring that the function has the Haar spectral distribution that will satisfy resiliency. This is one of the main advantages of the Haar transform as the spectral coefficients behave locally and therefore can be used to influence the function directly by a designer to reach specific target goals. The following example demonstrates the algorithm.

Example 4: Consider the 4-variable function $\hat{f}$ given in the following table (Table 3) along with its WP spectrum and the Haar spectrum. It can clearly be seen the function is resilient of order 1 since the last zone of the Haar spectrum is balanced while the rest of the zones are zeroes, or by just looking at the WP spectrum then it can be seen that all coefficients with index weight equals one are zeroes. If this function is utilized based on Theorem 2, then the resulting function $\hat{g}$ would be a 5-variable function of order 2. The resulting function in this case is given as $\hat{g} = 0\text{x}66996996$ in Hexadecimal format whose Haar spectral coefficients follow the distribution given by the Theorem 2. *End of Example*

```
Design Algorithm: Higher Order Resiliency
Input: An $n$-variables $k$-resilient BF in polarity form, $\hat{f}$
Output: An $(n+1)$-variables $(k+1)$-resilient BF in polarity form, $\hat{g}$
Steps:
  Step 1: Compute $temp_{vec} = 2 * \hat{f}$
  Step 2: Initialize parameter: $count = 0,\ V_{out}(x) = 0\ \forall x \in [0, 2^{n+1})$
  Step 3: Loop: while $count < 2^n$ do
      Step 3.1: $ind_{left} = 2 * count;\quad ind_{right} = 2 * count + 1;$
      Step 3.2: If $temp_{vec}(count) = -2$ then go to Step 3.3 else go
                to Step 3.4
      Step 3.3: $V_{out}(ind_{left}, ind_{right}) = [-1, 1]$; then go to Step 3.5
      Step 3.4: $V_{out}(ind_{left}, ind_{right}) = [1, -1]$; then go to Step 3.5
      Step 3.5: $count = count + 1$
  Step 4: Output $\hat{g} = V_{out}$
```

Figure 3: Haar Design Algorithm for Generating Higher Order (*k*) Resilient from Lower Order (*k*-1)

Table 3. A 4-Var Function from Example 4 and Its WP and Haar Spectra

x	$\hat{f}(x)$	$\hat{F}_{WP}(x)$	$\hat{F}_H(x)$
0	1	0	0
1	-1	0	0
2	1	0	0
3	-1	0	0
4	-1	0	0
5	1	0	0
6	-1	0	0
7	1	0	0
8	1	0	2
9	-1	0	2
10	-1	8	-2
11	1	8	-2
12	-1	0	2
13	1	0	-2
14	1	8	-2
15	-1	-8	2

Note on the evaluation of the Haar-based methods of approach: It is clear from the remarks given in the previous sections that, the Haar alternative methods of approach make it possible to look at a given function in the current variable domain (n) along with its related sub-functions from lower variable domains ($r < n$). This is done from the highest considered variable domain without leaving that domain. In effect, it is one of the Haar advantages that is not shared by the existing construction methods based on Walsh transform or truth table concatenation, where a designer has to consider first the lower variable domains ($r < n$) or the related sub-functions in order to build a higher variable function (n-variable function). In such cases, a function is designed by starting first with sub-functions and then utilizing them to construct a new one in higher variable domain [1,2,3,4,14,16]. On the other hand, the Haar based methods can be integrated well with the existing methods and give extra flexibility in terms of design constructions. This is in fact true as the Haar methods can provide added alternative from the perspective of a function’s local properties or by combination with the Walsh as hybrid methods of approach [13].

The following section presents the conclusion of the paper.

4. CONCLUSION

Stream ciphers are considered desirable and secure if composed of Boolean functions (B.Fs) that are characterized by high *resiliency*. Resiliency is one of the main cryptographic security criteria for a given Boolean function. One of the classes of functions satisfying high resiliency with desirable cryptographic properties are the Plateaued functions and whose design construction is of significant interest. This paper has examined the Haar spectral transform as an alternative method for the design of such functions. The paper presented different methods utilizing the Haar spectral coefficients’ distribution for the design of highly resilient functions including Plateaued functions. The paper presented two methods of approaches namely; design of resilient BFs within the current variable domain without considering lower variable domains and using the lower variable domains to construct resilient functions within higher variable domain. In the process, a Haar based construction method of $(k+1)^{th}$-order resilient functions from k^{th}-order resilient functions is derived and presented as well.

The Haar based construction methods for resilient functions have been considered for different restrictions on the Haar spectral coefficients and their related zones. The derivations were based on absolute flat spectral zones as well as mixed zero and nonzero spectral coefficients within zones of the respective Haar spectrum. In the process, the paper examined the presented construction methods and derived their connection to Plateaued functions. In addition, the Haar based construction method from lower order resiliency to higher order has been presented. It is demonstrated in the presentation that, the Haar spectrum provides more ways on which the resilient functions can be considered and possibly opens a door for further enumeration of such functions. The Haar flexibility and its local properties provide an advantage over the Walsh based methods since the Walsh is global in nature and it is difficult to view lower variable functions’ properties while in higher variable domains. The paper demonstrates that it is possible with the Haar based method of approach to see directly the local properties of a given n-variable BF with respect to its sub-functions from r-variable domains $(r < n)$ without considering the spectra of the respective sub-functions. On the other hand, the Haar local behaviors related to the transformed functions provide the possibility to enumerate different types of resilient functions including the Plateaued functions.

The work presented here dealt mainly with Haar spectral coefficients $(\hat{F}_H^l)$ having a distribution over absolute values of 2^{n-l-1} $(1 < l < n-1)$. It is highly recommended for further examination on Haar spectral coefficients having a balanced nonzero distribution over values that are less than 2^{n-l-1} for $1 < l < n-1$. Also of interest is the distribution of zero and nonzero values within the same spectral zones such that, their Walsh linear combination is either less than 2^{n-l-1} $(\sum_{q,\omega \in \mathbb{F}_2^l} \hat{F}_H^l(q) \cdot (-1)^{\omega \cdot q} < 2^{n-l-1})$ or zero. This will make it possible to minimize the magnitude of the corresponding Walsh spectral coefficients. Consequently, it may provide further classification and enumeration of the classes of highly nonlinear resilient and/or Plateaued functions.

5. ACKNOWLEDGMENTS

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

6. REFERENCES

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

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

[3] R. Kui, P. Jaemin and K. Kwangjo. 2005. “On the Construction of Cryptographically Strong Boolean Functions with Desirable Trade-off,” Journal of Zhejiang University Science, vol. 6, No. 5, pp. 358–364, doi:10.1361/jzus.2005.A0358.

[4] M. Read. 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.

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

[6] R. S. Stanković and B. J. Falkowski. 2003. “The Haar Wavelet Transform: Its Status and Achievement,” Computers and Electrical Engineering, vol. 29, No. 1, pp. 25-44, doi:10.1016/S0045-7906(01)00011-8.

[7] B. J. Falkowski and S. Rahardja. 1996. “Walsh-like Functions and their Relations,” Proc. IEE Vision, Image and Signal Processing, vol. 143, No. 5, pp. 279-284, doi:1049/ip-vis:19960760.

[8] B. J. Falkowski and T. Sasao. 2005. “Unified Algorithm to Generate Walsh Functions in Four Different Orderings and Its Programmable Hardware Implementations,” Proc. IEE Vision, Image and Signal Processing., vol. 152, no. 6, pp. 819-826, doi:10.1049/ip-vis:20045123.

[9] B. J. Fino. 1972. “Relations Between Haar and Walsh/Hadamard Transforms,” Proc. IEEE, vol. 60, no. 5, pp. 647-648, doi:10.1109/PROC.1972.8719.

[10] S. Khuri. 1997. Computing with Haar Functions. Proc. 1997 Symposium on Applied Computing, 1997, pp. 223-227, doi:10.1145/331697.331744.

[11] H. M. Rafiq and M. U. Siddiqi. 2009. Haar Transformation of Linear Boolean Functions, Proc. IEEE International Conference on Signal Processing Systems, pp. 802-805, Singapore, doi:10.1109/ICSPS.2009.150.

[12] M. A. Thornton, D. M. Miller and R. Drechsler. 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, pp. 215-225, doi:10.1.1.21.8871.

[13] H. M. Rafiq and M. U. Siddiqi. 2015. “Correlation Immunity and Resiliency of Boolean Functions from Haar Domain Perspective,” ARPN Journal of Engineering and Applied Sciences, vol. 10, no. 22, pp. 17232-17238, ISSN 1819-6608.

[14] S. Gao, W. Ma, Y. Zhao, & Z. Zhuo. 2011. “Walsh Spectrum of Cryptographically Concatenating Functions and its Application in Constructing Resilient Boolean Functions”, Journal of Computational Information Systems, 7(4), pp. 1074-1081.

[15] A. Canteaut & M. Trabbia. 2000. Improved Fast Correlation Attacks using Parity-Check Equations of weight 4 and 5. In *Advances in Cryptology—EUROCRYPT 2000*. Springer Berlin Heidelberg, 2000, pp. 573-588.

[16] Canteaut, A. 2002, October. On the correlations between a combining function and functions of fewer variables. In *Information Theory Workshop, 2002. Proceedings of the 2002 IEEE* (pp. 78-81). IEEE.

[17] Charpin, P., & Pasalic, E. 2003, January. On propagation characteristics of resilient functions. In *Selected Areas in Cryptography* (pp. 175-195). Springer Berlin Heidelberg