New Findings on the Covering Sequence of Boolean Functions

Güzin Kurnaz

***Abstract*— The notion of covering sequence was first introduced by Carlet and Tarannikov in 2000. They also gave the complete characterization of balancednes, correlation immunity and resiliency of Boolean functions using the help of covering sequences. This work collects the known facts on covering sequences and characterizes correlation immunity and resiliency of Boolean functions using covering sequences in a different way.**

In addition to the traditional s-box criteria, the existence of equivalence mappings between component s-box Boolean functions is proposed by Fuller and Millan in 2003 as a new s-box criterion. In this work, the covering sequences of affine equivalent Boolean functions are studied for the first time in the literature.

***Index Terms*—Boolean functions, covering sequence, affine equivalence, correlation immunity.**

I. INTRODUCTION

BOOLEAN functions play an important role in modern cryptography; and their study from theoretical and practical perspectives is crucial in the provision of secure cryptographic applications such as block ciphers, stream ciphers and hash functions. Covering sequence of a Boolean function which has been shown to have deep relations with the cryptographic properties of Boolean functions was first introduced in 2000 by Carlet and Tarranikov [1].The complete characterizations of balancedness, correlation immunity and resiliency by means of the covering sequences are also given by Carlet and Tarannikov in the same work. We have shown that Walsh transform nulls and covering sequence are related by a linear equation and we experimentally confirmed this equation using a Matlab program for functions up to 5 bits. Walsh transform nulls that we found from covering sequences are shown to satisfy the characterization given by Carlet and Tarannikov [1]. Also looking at the theoretical Hamming weights of these null frequencies, one can see the similarity to (10).

In addition to the traditional s-box criteria, the existence of equivalence mappings between component s-box Boolean functions is proposed in [3] as a new s-box criterion. The linear classification of Boolean functions is meaningful for the following two reasons: first, equivalent functions have similar properties (like Hamming weight distribution in error-correction coding, same nonlinearity in cryptography). Second, the number of representatives is much less than the number of Boolean functions.This perspective allows the Boolean space to be considered as a structure in which all Boolean functions are grouped into equivalence classes and thus only one function from each class needs to be established for analysis. Recently the analysis of linear equivalence of Boolean functions was discussed in several papers [3, 4, 5, 6, 7]. In this work, we study the relations between the covering sequences of affine equivalent Boolean functions and explain them in Section 5.

Manuscript received October 3, 2007. Güzin Kurnaz: Electrical and Electronics Engineering Department, Middle East Technical University, Ankara-Turkey.(phone: 0312-2101374, e-mail: guzinkurnaz@yahoo.com).

II. BASIC NOTATIONS AND DEFINITIONS

This section is intended as a summary of the minimum mathematical knowledge required in treating the subject.

Let f be a Boolean function that produces a single-bit result for each possible combination of n Boolean variables; that is, $f(\mathbf{x}):GF(2)^n \rightarrow GF(2)$. Here GF denotes the Galois Field consisting of binary numbers {0,1}, with modulo 2 addition (XOR operation shown by $\oplus$) and multiplication (AND operation shown by a dot or nothing). The 1×2^n dimensional vector $\mathbf{f} = (f(00\ldots0), \ldots, f(11\ldots1))$ is defined as the truth table of f, where the input vector $\mathbf{x}$ is ordered lexicographically.

Definition 1: The Walsh transform of a Boolean function f is defined as [9]

$$W_f(\mathbf{w}) = \sum_{x\in GF(2)^n} (-1)^{f(\mathbf{x})} (-1)^{\mathbf{w}\mathbf{x}^T} \quad (1)$$

where $\mathbf{w}\in GF(2)^n$, $\mathbf{w}\mathbf{x}^{\mathrm{T}}$ is the inner product of the vectors $\mathbf{w}$ and $\mathbf{x}$. The 1×2^n dimensional vector $\mathbf{W}_f = (W_f(00\ldots0), \ldots, W_f(11\ldots1))$ is called the Walsh spectrum of f.

Definition 2: The autocorrelation of f corresponding to the shift vector a is denoted by

$$r_f(\boldsymbol{\alpha}) = \sum_{x\in GF(2)^n} (-1)^{f(\mathbf{x})} (-1)^{f(\mathbf{x}+\boldsymbol{\alpha})} = \sum_{x\in GF(2)^n} (-1)^{D_{\mathbf{a}} f(\mathbf{x})} \quad (2)$$

where $\boldsymbol{\alpha}\in GF(2)^n$ [9] and $D_{\mathbf{a}} f(\mathbf{x}) = f(\mathbf{x}) \oplus f(\mathbf{x}\oplus\mathbf{a})$ is called the derivative of f with respect to the input difference vector $\mathbf{a}$. All values of the autocorrelation can be collected in a 1×2^n dimensional vector $\mathbf{r}_f = (r_f(00\ldots0), \ldots, r_f(11\ldots1))$. Similarly,

the derivative vector is defined as

Daf = ($Da_f(00\ldots0)$, …, $Da_f(11\ldots1)$). (3)

Definition 3: An $n\times m$ S-box is a mapping from n binary inputs to m binary outputs, i.e., $F(\mathbf{x})$: $GF(2)^n \rightarrow GF(2)^m$. The output vector $F(\mathbf{x})=(f_1(\mathbf{x}),\ldots, f_m(\mathbf{x}))$ can be decomposed into m component functions

$f_i(\mathbf{x}) : GF(2)^n \rightarrow GF(2)$, $i=1,\ldots m$.

Definition 4: The set

$R(r, n) = \{ f(x) | \deg(f) \le r \}$ (4)

denotes the r^{th} order Reed-Muller code of codeword length 2^n. The term $R(r,n)/R(s,n)$, where $s<r\le n$, defines the set of cosets of $R(r,n)$ with respect to $R(s,n)$.

Definition 5: Nonlinearity of f is defined as the minimum distance from the set of affine functions and one can show that it is related to the maximum magnitude in the Walsh spectrum of f as follows

$$NL_f = 2^{n-1} - \tfrac{1}{2}\max_{\mathbf{w}} \left| W_f(\mathbf{w}) \right|. \quad (5)$$

Definition 6: f is called r^{th} order correlation immune (r-CI) if [10]

$$W_f(\mathbf{w}) = 0, \ \left\{\forall \mathbf{w} \in GF(2)^n \,|\, 1 \le wt(\mathbf{w}) \le r\right\}. \quad (6)$$

Definition 7: The support of the Walsh transform of f is defined as

$$S_f = \left\{ \mathbf{w} \in GF(2)^n \mid W_f(\mathbf{w}) \neq 0 \right\}. \quad (7)$$

Definition 8: A covering sequence of a function f is any binary sequence $\boldsymbol{\lambda} = \left(\lambda_{00..0}, \lambda_{0...01}, \ldots \lambda_{11....1}\right) = (\lambda_{\mathbf{a}})_{\mathbf{a}\in GF(2)^n}$ such that $\sum_{\mathbf{a}\in GF(2)^n} \lambda_{\mathbf{a}} \mathbf{D_a f} = (\rho\ \rho\ \ldots \rho) = \boldsymbol{\rho}$, is a vector with identical elements, where the derivative $\mathbf{D_a f}$ is defined by (3). The value of ρ is called the level of this sequence. If $\rho \neq 0$, then the covering sequence is said to be nontrivial [1].

Definition 9: The Fourier transform of the sequence λ at frequency **b** is defined as [1]

$$\hat{\lambda}(b) = \sum_{a\in GF(2)^n} \lambda_{\mathrm{a}} (-1)^{\mathbf{ab}^T} \quad (8)$$

III. ALREADY KNOWN FACTS

A proposition on the characterization of balancedness of a boolean function using covering sequence was given by Carlet and Tarannikov [1]. In section 3, we give the proof of this proposition in a diferent way. Then some important theorems and propositions on covering sequences are attached at the end of this section.

Proposition 1: [1] If a Boolean function on $GF(2)^n$ admits a nontrivial covering sequence then it is balanced. Conversely, any balanced Boolean function admits the constant sequence 1 as nontrivial covering sequence with level 2^{n-1}. As a result, any Boolean function is balanced if and only if it admits a nontrivial covering sequence.

***Proof*:** Starting from the second part of the proposition, let f be any balanced Boolean function on $GF(2)^n$. While calculating $\mathbf{D_a f}$,

$$\begin{aligned} \mathbf{D_1 f} &= [(\mathrm{f(0)} \oplus \mathrm{f(1)}), (\mathrm{f(1)} \oplus \mathrm{f(0)}), \ldots] \\ \mathbf{D_2 f} &= [(\mathrm{f(0)} \oplus \mathrm{f(2)}), (\mathrm{f(1)} \oplus \mathrm{f(3)}), \ldots] \\ &\vdots \\ \mathbf{D_{2^n-1} f} &= [(\mathrm{f(0)} \oplus \mathrm{f(2^n-1)}), \ldots] \end{aligned} \quad (9)$$

Notice that while a is running through 1 to 2^n–1, to each element $f(x)$ of the truth table, all remaining elements of the truth table except $f(x)$ itself are added once. That is, for example, all $f(1)$ through $f(2^n-1)$ are added to $f(0)$ exactly once. This is the same for all $f(x)$, $0 \le x \le 2^n - 1$. Since f is balanced, the complement of $f(0)$ is added to $f(0)$ exactly 2^{n-1} many cases, creating 1 as a result. Thus, each entry of $\mathbf{D_a f}$ becomes equal to 1 exactly 2^{n-1} times. Taking $\boldsymbol{\lambda} = [1\ldots.1]$, $\sum \lambda_a \mathbf{D_a f} = 2^{n-1}$. So the constant function 1 ($\boldsymbol{\lambda} = [1\ldots.1]$) is the covering sequence of all balanced functions with level 2^{n-1}.

For the first part of the proposition, assume f is balanced and the level of covering sequence is 0 (trivial covering sequence). Looking at (9), for this to happen, all summations $f(x) \oplus f(y) = 0$ for all x and y. Thus $f(\mathbf{x}) = f(\mathbf{y})$ must hold for all **x** and **y**. So the truth table of the function must be all 0's or all 1's. This contradicts with the first assumption that the function is balanced; which then completes the proof.

Theorem 1: [1] Let f be any Boolean function on $GF(2)^n$ and $\boldsymbol{\lambda} = (\boldsymbol{\lambda}_{\mathbf{a}})_{a\in GF(2)^n}$ any (real valued or integer valued) sequence. f admits λ as covering sequence if and only if $\hat{\lambda}$ takes constant value on the support of Walsh transform of f. Let r be this constant value, then the level of this covering sequence is the number $\frac{1}{2}\left[\left(\sum_{a\in GF(2)^n} \lambda_a \right) - r \right]$.

Theorem 2: [1] Let f be any Boolean function on $GF(2)^n$.

1- If f admits a covering sequence $\boldsymbol{\lambda} = (\boldsymbol{\lambda}_{\mathbf{a}})_{a\in GF(2)^n}$ with level ρ (resp. with level $\rho \neq 0$), then f is k^{th} order correlation-immune (resp. k-resilient), where $(k+1)$ is the minimum

Hamming weight of nonzero $b \in GF(2)^n$ such that $\hat{\lambda}(b) = r$, and $r = \hat{\lambda}(0) - 2\rho$.

2- Conversly if f is k^{th} order CI and it is not $(k+1)^{th}$ order CI then there exists one trivial covering sequence $\boldsymbol{\lambda} = (\boldsymbol{\lambda}_{\mathbf{a}})_{a\in GF(2)^n}$ with level ρ such that $k+1$ is the minimum

Hamming weight of nonzero $b \in GF(2)^n$ satisfying

$\hat{\lambda}(0)-2\rho$ .Thus,

$$wt(\mathbf{w}) \le \min wt(b \mid \hat{\lambda}(b)=\hat{\lambda}(0)-2\rho) \tag{10}$$

The proof of Theorem 2 is given in [1].

Proposition 2: [2] Let E be any vector subspace of $GF(2)^n$. Let f be any Boolean function on $GF(2)^n$. Then f admits a covering sequence $\boldsymbol{\lambda}$ with support $S \subseteq E$ if and only if the restriction of f to any coset of E (viewed as a function on E) admits the same covering sequence $\boldsymbol{\lambda}$.

Proposition 3: [2] Let E be any vector subspace of $GF(2)^n$ and (u+E) any of its cosets. Let f be any Boolean function on $GF(2)^n$. Assume it admits no derivative $\mathbf{D_a f}$ equal to the constant function 1. Then f admits the indicator of (u+E) as nontrivial covering sequence if and only if the support of $W_f(w)$ is disjoint from $E^{\perp}=\{\mathbf{x}\in GF(2)^n \mid \mathbf{x}.\mathbf{v}=0, \forall \mathbf{v}\in E\}$. This is equivalent to the fact that the restriction of f to any coset of E is balanced. The level of this covering sequence is then equal to $|E|/2$ and the indicator of every coset of E is also a covering sequence of f with the same level. More generally, any sequence $\boldsymbol{\lambda}$ such that for every $\mathbf{a}\in E$ and every $u\in GF(2)^n$, $\boldsymbol{\lambda}_{\mathbf{a+u}}=\boldsymbol{\lambda}_{\mathbf{u}}$ is also a covering sequence of f.

Remark 1: [2] Let f be any Boolean function on $GF(2)^n$ and $\boldsymbol{\lambda}=(\lambda_a)_{a\in GF(2)^n}$ a covering sequence of f. Let r be the constant value of $\hat{\boldsymbol{\lambda}}$ on the support of Walsh transform of f. Then the nonlinearity of f satisfies:

$$N_f \le 2^{n-1} - \frac{2^{n-1}}{\sqrt{\left|\hat{\lambda}^{-1}(r)\right|}}. \tag{11}$$

The proof of the above remark is given in [2].

IV. CHARACTERİZATION OF CORRELATION IMMUNITY OF BOOLEAN FUNCTIONS USING THE COVERING SEQUENCE OF THE FUNCTION

The aim of Section 4 is to find the relations between covering sequence and correlation immunity. We have shown that Walsh transform nulls and covering sequence are related by a linear equation (15) and we experimentally confirmed this equation using a Matlab program for functions up to 5 bits. Thus correlation immunity order can be determined just looking at one of the covering sequences of the function. As a result, we characterize the correlation immunity and thus the resiliency of a Boolean function using its covering sequence. Here is the characterization.

Calculation of correlation immunity order requires the calculation of the Walsh transform and finding the places of its zeros. Thus one has to solve the following equation for **w**;

$$W_f(\mathbf{w})=0$$

$$\sum_{x\in GF(2)^n}(-1)^{f(\mathbf{x})}(-1)^{\mathbf{w}.\mathbf{x}^T} = \sum_{x\in GF(2)^n}[1-2(f(\mathbf{x})\oplus \mathbf{w}.\mathbf{x})] = 2^n - 2\sum_{x\in GF(2)^n}(f(\mathbf{x})\oplus \mathbf{w}.\mathbf{x}) = 0 \tag{12}$$

or to solve the following equation

$$\sum_{\mathbf{x}\in GF(2)^n}(f(\mathbf{x})\oplus \mathbf{w}\bullet\mathbf{x}) = 2^{n-1}. \tag{13}$$

At this point recall the covering sequence relation

$$\sum_{a\in GF(2)^n}\lambda_a(f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{a})) = (\rho \quad \rho..\rho). \tag{14}$$

Taking $\boldsymbol{\lambda}$ as a binary sequence,

$$\sum_{a\in GF(2)^n}(\lambda_a f(a)\oplus \lambda_a f(\mathbf{x}\oplus\mathbf{a})) = \boldsymbol{\rho}. \tag{15}$$

Comparing (13) and (15), one can see the similarity.

$$\sum_{x\in GF(2)^n}(\lambda_{\mathbf{x}} f(\mathbf{x})\oplus \lambda_{\mathbf{x}} f(\mathbf{x}\oplus\mathbf{a})) = \boldsymbol{\rho} = (\sum_{x\in GF(2)^n} f(x)\oplus w\bullet x) + k \tag{16}$$

where k is any integer. Using the similarity above one gets

$$\lambda_{\mathbf{x}} = \mathbf{w}\bullet\mathbf{x}. \tag{17}$$

Thus for finding zeros of Walsh transform one must find all possible covering sequences and solve (17) for **w**. Thus correlation immunity order can be found from covering sequence. Matlab numeric analysis shows that the Walsh transform nulls satisfy (10) given by Carlet and Tarannikov in [1]. Also looking at the theoretical Hamming weights of these null frequencies, one can see the similarity to (10).

Taking Walsh transform of (17):

$$\sum_{\mathbf{x}\in GF(2)^n}(-1)^{\lambda_{\mathbf{x}}}(-1)^{\mathbf{b}.\mathbf{x}} = \sum_{\mathbf{x}\in GF(2)^n}(-1)^{\mathbf{w}.\mathbf{x}}(-1)^{\mathbf{b}.\mathbf{x}} \tag{18}$$

One gets

$$\hat{\lambda}'(\mathbf{b})*W_f(\mathbf{b}) = \delta(\mathbf{w}-\mathbf{b}) \tag{19}$$

where $*$ denotes convolution and δ is the delta function. If **w**=**b** delta function gives 1 otherwise gives 0. Thus,

$$wt(\mathbf{w}) \le wt(\mathbf{b} \mid \hat{\lambda}'(\mathbf{b})*W_f(\mathbf{b}) = 1) \tag{20}$$

$$\hat{\lambda}'(\mathbf{b}) = \sum_{a\in GF(2)^n}(1-2\lambda_a)(-1)^{(\mathbf{b}).a} = \delta(\mathbf{b}) - 2\hat{\lambda}(\mathbf{b}) \tag{21}$$

Then (17) becomes:

$$\hat{\lambda}'(\mathbf{b})*W_f(\mathbf{b}) = W_f(\mathbf{b})(1-2\hat{\lambda}(\mathbf{b})). \tag{22}$$

Solving for $\hat{\lambda}(\mathbf{b})$ from (21) and (22) one gets

$$\hat{\lambda}(b) = \sum_{a\in GF(2)^n}\lambda_a(1-2D_a f). \tag{23}$$

$$\hat{\lambda}(b) = \hat{\lambda}(0) - 2\rho. \tag{24}$$

This exactly gives (10).

From Proposition1 it is also known that balancedness can be determined from covering sequence knowledge. As a result, covering sequence gives complete knowledge of resiliency. To examine all these relations and characterizations, Matlab programs are used.

However for linear functions, nulls of the Walsh transform

can not be found from the covering sequences. This does not destroy the determination of correlation immunity order since for all linear functions the constant covering sequence 1 is found. By looking at the constant sequence $\boldsymbol{\lambda}$=1 one can tell that the function is linear.

Theorem 4 of [1] gives the characterization of all k^{th} order correlation-immune and all k-resilient functions by means of general covering sequences. Here the relation between Walsh transform nulls and covering sequence are given by equation (17). If one solves (17) for **w** and checks for its Hamming weight,

V. COVERING SEQUENCE AND AFFINE EQUIVALENCE

In this section, relations between the covering sequences of affine equivalent Boolean functions are studied. Affine equivalence is defined using the definition in [11].

If there exists a nonsingular binary nxn matrix **A** and $1xn$ vector **b** such that

$$f(x) = g(xA + b) \bmod R(s,n). \quad (25)$$

Then f and g are said to be equivalent [11]. In this case, due to the modulo operation the above equation becomes

$$f(\mathbf{x}) + g(\mathbf{xA}+\mathbf{b}) \in R(s,n). \quad (26)$$

and

$$f(\mathbf{x}) = g(\mathbf{x}.\mathbf{A}+\mathbf{b}) + v_s \quad (27)$$

where $v_s \in R(s,n)$.

If one chooses $v_s \in R(1,n)$ then this equivalence equation becomes the "*affine* equivalence" relation

$$f(\mathbf{x}) = g(\mathbf{xA}+\mathbf{b}) + \mathbf{xc}^T + d, \quad (28)$$

where $\mathbf{c} \in GF(2)^n$ and $d \in GF(2)$.

Walsh and autocorrelation spectra of affine equivalent Boolean functions are studied in [11, 12]. Here we study the covering sequences of affine equivalent functions.

Two important questions are: If two Boolean functions are equivalent then are the covering sequences and the level of covering sequences of these functions related? If one of these functions does not have a covering sequence then does the other function have a covering sequence?

Let us investigate this in three steps. Let f and g be affine equivalent Boolean functions.

$$g(\mathbf{x}) = f(\mathbf{x}.\mathbf{A}+\mathbf{b}) + \mathbf{xc}^T + d, \quad (29)$$

where $\mathbf{c} \in GF(2)^n$ and $d \in GF(2)$.

1. Let f does not have any covering sequence. Does g have any covering sequence?
2. Let $\lambda = (\lambda_a)_{\mathbf{a}\in GF(2)^n}$ is one of the covering sequences of f with level ρ. What are the corresponding covering sequence and its level for g ?
3. Are every covering sequences of f and g related?

Let us now investigate these three steps.

1. Assume f does not have any covering sequence. Thus, $\sum \lambda_a D_a f \neq \text{constant}$. Then,

$$\begin{aligned}\sum \lambda'_a D_a g &= \sum_a \lambda'_a (g(x)+g(x+a)) \\ &= \sum \lambda'_a (f(x.A+b)+x.c^T+d \\ &\quad + f(x.A+b+a.A)+x.c^T+a.c^T+d) \\ &= \sum \lambda'_a (f(x.A+b)+f(xA+a.A))+k \\ &= \sum_a \lambda'_a (f(y)+f(y+a.A))+k\end{aligned} \quad (30)$$

where k is a constant. Note that $\sum \lambda_a D_a g \neq \text{constant}$. Hence, if f does not have any covering sequence then its affine equivalent function g does not have any covering sequence either.

2. From Property 1, taking $\mathbf{B} = \mathbf{A}.\mathbf{x} + b$,

$$f \circ \mathbf{B} = f(\mathbf{x}.\mathbf{A}+b) = f'(\mathbf{x}) \quad (31)$$

$$g(\mathbf{x}) = f(\mathbf{x}.\mathbf{A}+b) + \mathbf{xc}^T + d = f'(\mathbf{x}) + \mathbf{xc}^T + d$$

$$\mathbf{D_a f'} = \mathbf{D_{aA} f} \circ \mathbf{B}$$

$$\mathbf{D_a g} = \mathbf{D_a f'} + \mathbf{x}.\mathbf{c}^T + d + (\mathbf{x}+\mathbf{a}).\mathbf{c}^T + d$$

$$\mathbf{D_a g} = \mathbf{D_{aA} f} \circ \mathbf{B} + \mathbf{a}.\mathbf{c}^T$$

Covering sequence relation for f is

$$\sum_{\mathbf{a}\in GF(2)^n} \lambda_a \mathbf{D_a f} = (\rho_f \ldots . \rho_f). \quad (32)$$

Covering sequence relation for g is

$$\sum_{a\in GF(2)^n} \lambda'_a \mathbf{D_a g} = (\rho_g, \rho_g, .. \rho_g) \quad = \boldsymbol{\rho}_\mathbf{g}. \quad (33)$$

(33) Can also be written as:

$$\sum_{a\in GF(2)^n} \lambda'_a (\mathbf{D_{Aa} f} \circ \mathbf{B} + \mathbf{a}.\mathbf{c}^T) = \boldsymbol{\rho}_\mathbf{g}. \quad (34)$$

Writing (34) in detail:

$$\begin{aligned}&\lambda_1' \mathbf{D_1 g}(1) + \lambda_2 \mathbf{D_2 g}(1) + \ldots . \\ &\lambda_1' \mathbf{D_1 g}(2) + \lambda_2 \mathbf{D_2 g}(2) + \ldots \\ &\vdots \qquad\qquad = \boldsymbol{\rho}_\mathbf{g} \\ &\lambda_1' \mathbf{D_1 g}(2^n) + \lambda_2 \mathbf{D_2 g}(2^n) + \ldots\end{aligned} \quad (35)$$

Here $\mathbf{D_i g}(j)$ is j^{th} bit of the vector $\mathbf{D_a g}$ for $\mathbf{a}=\mathbf{i}$. Using (34) and (35) with $\mathbf{c}$ (i) as the ith bit of vector $\mathbf{c}$.

$$\begin{aligned}&\left[\lambda_1' \mathbf{D_A f}(1)\right] \circ \mathrm{B} + \lambda_1' . \mathrm{c}^{\mathrm{T}}(1) + \left[\lambda_2' \mathbf{D_{A.2} f}(1)\right] \circ \mathrm{B} + \lambda_2' . \mathrm{c}^{\mathrm{T}}(1) + \ldots . \\ &\left[\lambda_1' \mathbf{D_A f}(2)\right] \circ \mathrm{B} + \lambda_1' . \mathrm{c}^{\mathrm{T}}(2) + \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \quad = \boldsymbol{\rho}_\mathbf{g} \\ &\vdots \\ &\left[\lambda_1' \mathbf{D_A f}(2^{\mathrm{n}})\right] \circ \mathrm{B} + \lambda_1' . \mathrm{c}^{\mathrm{T}}(2^{\mathrm{n}}) + \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots\end{aligned} \quad (36)$$

Equation (36) becomes:

$$\begin{aligned}&\left[\lambda_1' \mathbf{D_A f}(1.A+b)\right] + \lambda_1' . c^T(1) + \left[\lambda_2' D_{A.2} f(1.A+b)\right] + \lambda_2' . c^T(1) + \ldots \\ &\left[\lambda_1' \mathbf{D_{2A} f}(2.A+b)\right] + \lambda_1' . c^T(2) + \ldots \ldots \ldots \\ &\vdots \qquad\qquad = \boldsymbol{\rho}_\mathbf{g} \\ &\left[\lambda_1' D_{2^n A} f(2^n.A+b)\right] + \lambda_1' . c^T(2^n) + \ldots \ldots \ldots\end{aligned} \quad (37)$$

$$\beta_i = (\sum_a \lambda'_a)\mathbf{c}^T(i) \tag{38}$$

$$\lambda'_1\mathbf{D_1f}(i.A+b)+\beta_1+\lambda'_2D_2f(i.A+b)+\beta_2+\ldots\ldots = \lambda_1\mathbf{D_1f}(i)+\lambda_2\mathbf{D_2f}(i)+\ldots\ldots\ldots \tag{39}$$

There are 2^n-1 such equations. If one can find all $(\lambda'_a)_{a\in GF(2^n)}$ from $(\lambda_a)_{a\in GF(2^n)}$ then

$$\rho_f = \rho_g \tag{40}$$

Hence, at least one of the covering sequences of two affine equivalent functions are related by (37) and they have the same level.

3. If support of W_f is disjoint from $E^\perp$ then the indicator of every coset of E is covering sequence of f [2].

Support of W_f and W_g contain same number of frequency values. However may contain different frequencies. The largest fields that can be constructed from these supports are not same in general. So $E_f^\perp \neq E_g^\perp$ and $\left|E_f^\perp\right| \neq \left|E_g^\perp\right|$. Thus number of cossets of E_f is not equal to number of cossets of E_g in general. As a result, number of covering sequences of f is not equal to number of covering sequences of g.

VI. CONCLUSION

In this work, we have shown that Walsh transform nulls and covering sequence are related by a linear equation and experimentally confirmed this equation using a Matlab program for functions up to 5 bits. As a result, we characterize the correlation immunity and resiliency of Boolean functions using covering sequences with a different perspective than Carlet and Tarannikov.

Covering sequences of two arbitrary affine equivalent Boolean functions are studied. A novel relation between covering sequences of affine equivalent functions is obtained. It is also proven that if one of the affine functions does not have any covering sequence then its affine equivalent function does not have any either. Finally, we show that number of covering sequences of two equivalent functions are not equal in general.

REFERENCES

[1] C. Carlet and Y. Tarrannikov, "Covering Sequences of Boolean Functions and their Cryptographic Significance *Designs, Codes and Cryptography*, vol. 25, pp. 263-279, 2002.

[2] C. Carlet and S. Mesnager, "On the supports of the Walsh transforms of Boolean functions", *Proceedings of BFCA* (*First Workshop on Boolean Functions: Cryptography and Applications*), Rouen, France, 2005.

[3] J. Fuller, W. Millan, "Linear Redundancy in S-box". *Fast Software Encryption*, LNCS 2887, Springer-Verlag, , pp. 74-86, 2003.

[4] A.Biryukov, C.D.Canniere, A. Braeken, B. Preneel, "*Toolbox for Cryptanlysis: Linear and Affine Equivalence Algorithms*", Eurocrypt'03, LNCS 2656, pp. 33-50, 2003.

[5] W. Geiselmann, W. Meier, R. Steinwandt, "*An attack on the Isomorphisms of Polynomials Problem with One Secret*." International Journal of Information Security, pp. 59-64, 2003.

[6] A. Braeken, Y. Borissov, S. Nikova, B.Preneel, "Classification of Boolean Functions of 6 Variables or Less with respect to Cryptographic Properties", http://eprint.iacr.org, 2004.

[7] Q. Meng, H. Zhang, "*The Analysis of Linear Equivalence of Boolean Functions and Its Applications*", Chinese Journal of Computers , pp. 1528-153, 2004.

[8] M.A. Harrison, *"On the Classification of Boolean Functions by the General Linear and Affine Groups*", J. Soc. Indust. Appl. Math. 12, pp. 285-299,1964.

[9] A. Canteaut, C. Carlet, P. Charpin and C. Fontaine, "Propagation Characteristics and Correlation Immunity of Highly Nonlinear Boolean Functions", Eurocrypt 2000, LNCS 1807, pp. 507-522, 2000.

[10] Q. Meng, M. Yang, H. Zhang and Y. Liu, "*The Analysis of Affinely Equivalent Boolean Functions*", Chinese Journal of Computers, pp.1528-1532, 2005.

[11] B. Preneel, "*Analysis and Design of Cryptographic Hash Functions*", PhD Thesis, KU Leuven (Belgium), 1993.