A General Correlation Theorem

Kishan Chand Gupta and Palash Sarkar
Cryptology Research Group
Applied Statistics Unit
Indian Statistical Institute
203, B.T. Road
Kolkata 700108, India
e-mail:{kishan_t,palash}@isical.ac.in

Abstract

We obtain the Walsh transform of a very general functional form. Nyberg's correlation theorems are obtained as special cases of our result. We also apply the result to two typical situations and obtain complete expressions for the Walsh transform in each case.

Keywords : Boolean function, S-box, Walsh Transform, correlation, linear approximation, symmetric ciphers.

1 Introduction

Symmetric ciphers are a basic cryptographic primitive. In practice, symmetric ciphers are designed using nonlinear Boolean functions and S-boxes. One of the most effective methods of attacking symmetric ciphers is the technique of linear cryptanalysis [5]. The efficacy of this technique depends upon the ability to obtain good linear approximations of the constituent Boolean functions and S-boxes.

Linear approximations are studied using the technique of Walsh transform analysis. While it is usually easy to apply the Walsh transform to an individual constituent of a symmetric cipher, in general it is more difficult to apply the technique when a combination of primitives are used. This requires the development of a general methodology of Walsh transform applications.

One such important work has been done by Nyberg in [8]. This work unifies some of the previous approaches and obtains three key results on the Walsh transform of various functional forms. These are then applied to several typical cryptanalytic context.

The purpose of the current paper is to continue the direction of research initiated in [8]. We obtain the Walsh transform for a very general functional form:

$$h(x_1, x_2, \ldots, x_{t+1}) \quad = \quad f(g_1(x_1, x_2), g_2(x_2, x_3), \ldots, g_t(x_t, x_{t+1}))$$

where each g_i is a map from $\mathbb{F}_2^{m_i+m_{i+1}}$ to $\mathbb{F}_2^{n_i}$ and f is a Boolean function from $\mathbb{F}_2^{n_1+\cdots+n_t}$ to $\mathbb{F}_2$. A large class of symmetric cipher primitives is captured by the above general functional form. We obtain a relatively simple closed form expression for the Walsh transform of h in terms of the Walsh transform of f and $g_1, \ldots, g_t$. Our principle techniques in the analysis are a general form of the Convolution Theorem and the Composition Theorem for Walsh transform, which are also proved in the paper.

We show that two of Nyberg's results in [7] are special cases of our theorem. This underlines the importance of our result in the context of symmetric cipher cryptanalysis. We also consider two additional applications of our result. The first application is to a situation where an S-box is applied to the X-OR of two outputs of the application of the S-box to two input bit strings. The second application considers the situation where an S-box is combined with addition modulo 2^8. In both cases, we obtain complete expressions for the Walsh transform. Depending upon a particular application, it should be possible to simplify these expressions and use them for practical cryptanalysis.

2 Preliminaries

Let $\mathbb{F}_2 = GF(2)$ be the finite field of two elements. We consider the domain of an n-variable Boolean function to be the vector space $(\mathbb{F}_2^n, \oplus)$ over $\mathbb{F}_2$, where $\oplus$ is used to denote the addition operator over both $\mathbb{F}_2$ and the vector space $\mathbb{F}_2^n$. The inner product of two vectors $u, v \in \mathbb{F}_2^n$ will be denoted by $\langle u, v \rangle$. We will denote the weight of a binary string x by $\mathsf{wt}(x)$.

An n-variable Boolean function is a map $f : \mathbb{F}_2^n \to \mathbb{F}_2$. The Walsh Transform of an n-variable Boolean function f is an integer valued function $W_f : \mathbb{F}_2^n \to [-2^n, 2^n]$ defined by (see [4, page 414])

$$W_f(u) = \sum_{w \in \mathbb{F}_2^n} (-1)^{f(w) \oplus \langle u, w \rangle}. \tag{1}$$

The Walsh Transform is called the spectrum of f. The inverse Walsh Transform is given by

$$(-1)^{f(u)} = \frac{1}{2^n} \sum_{w \in \mathbb{F}_2^n} W_f(w)(-1)^{\langle u, w \rangle}. \tag{2}$$

An (n, m) S-box (or vectorial function) is a map $f : \{0,1\}^n \to \{0,1\}^m$. Let $f : \{0,1\}^n \to \{0,1\}^m$ be an S-box and $g : \{0,1\}^m \to \{0,1\}$ be an m-variable Boolean function. The composition of g and f, denoted by $g \circ f$ is an n-variable Boolean function defined by $(g \circ f)(x) = g(f(x))$.

Linear cryptanalysis [5] is a very powerful cryptanalytic method for block ciphers. The study of correlation between linear combinations of input and output of an S-box is therefore very important. If two functions are highly correlated, then they are "close" to each other and can be approximated one for the other. This finds applications in block ciphers in the following manner: if a linear combination of the output of an S-box is correlated to a linear combination of the input, then the S-box can be approximated by replacing the output linear combination by the input linear combination. The correlation between two n-variable Boolean functions f and g is defined in the following manner (see for example [8]).

$$c(f, g) = 2^{-n} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus g(x)}. \tag{3}$$

We have the following relationship $c(f, g) = 2^n W_{f \oplus g}(0)$ and $c(f, l_v) = W_f(v)$, where l_v is the linear function defined as $l_v(x) = \langle v, x \rangle$ for $x \in \mathbb{F}_2^n$. Thus correlation between a Boolean function and a linear function can be conveniently studied using Walsh transform analysis.

3 Convolution and Composition Theorems for S-Boxes

Convolution for two n-variable Boolean functions is well known [1].

Theorem 1 (Convolution Theorem) *Let f and g be n-variable Boolean functions and $h(x) = g(x) \oplus f(x)$. Then*

$$W_h(u) = \frac{1}{2^n} \sum_{v \in \mathbb{F}_2^n} W_g(v) W_f(v \oplus u). \tag{4}$$

Now convolution for more than two n-variable Boolean functions is given.

Theorem 2 (Generalized Convolution Theorem) *Let $g_1, \ldots, g_k$ be n-variable Boolean functions and $h(x) = g_1(x) \oplus \cdots \oplus g_k(x)$. Then for $u \in \mathbb{F}_2^n$*

$$W_h(u) = \frac{1}{2^s} \sum_{v \in \mathbb{F}_2^s} W_{g_k}(u \oplus u_{k-1}) W_{g_{k-1}}(u_{k-1} \oplus u_{k-2}) \cdots W_{g_2}(u_2 \oplus u_1) W_{g_1}(u_1) \quad (5)$$

$$= \frac{1}{2^s} \sum_{v \in \mathbb{F}_2^s} \prod_{i=1}^{k} W_{g_i}(u_i \oplus u_{i-1}) \quad (6)$$

where $s = n(k-1)$, $v = (u_1, \ldots, u_{k-1})$, $u_k = u$ and $u_0 = (0, \ldots, 0)$ with each $u_i \in \mathbb{F}_2^n$.

Proof : We prove the above Theorem by induction on k. For $k = 2$, the result follows from the Convolution Theorem. Assume that result holds for $(k-1) \geq 2$. We now apply the Convolution Theorem on the functions $g_k(x)$ and $f(x) = g_1(x) \oplus \cdots \oplus g_{k-1}(x)$. This gives

$$W_h(u) = \frac{1}{2^n} \sum_{u_{k-1} \in \mathbb{F}_2^n} W_f(u_{k-1}) W_{g_k}(u \oplus u_{k-1}) = \frac{1}{2^n} \sum_{u_{k-1} \in \mathbb{F}_2^n} W_f(u_{k-1}) W_{g_k}(u_k \oplus u_{k-1})$$

Now we invoke the induction hypothesis for $(k-1)$ on the function f to get

$$W_h(u) = \frac{1}{2^n} \sum_{u_{k-1} \in \mathbb{F}_2^n} W_{g_k}(u_k \oplus u_{k-1}) \left(\frac{1}{2^{n(k-2)}} \sum_{(u_1, \ldots, u_{k-2})} \prod_{i=1}^{k-1} W_{g_i}(u_i \oplus u_{i-1}) \right)$$

$$= \frac{1}{2^s} \sum_{v \in \mathbb{F}_2^s} \prod_{i=1}^{k} W_{g_i}(u_i \oplus u_{i-1}).$$

This proves the result. ■

Now we provide the Walsh Transform of composition of an S-box and a Boolean function.

Theorem 3 (Composition Theorem) *Let $g : \{0,1\}^n \to \{0,1\}^m$ and $f : \{0,1\}^m \to \{0,1\}$. Then for any $w \in \mathbb{F}_2^n$,*

$$W_{(f \circ g)}(w) = \frac{1}{2^m} \sum_{v \in \mathbb{F}_2^m} W_f(v) W_{(l_v \circ g)}(w)$$

where $(l_v \circ g)(x) = \langle v, g(x) \rangle$.

Proof : From the inverse Walsh transform (2) we know $(-1)^{f(x)} = \frac{1}{2^m} \sum_{v \in \mathbb{F}_2^m} W_f(v)(-1)^{\langle v, x \rangle}$. Let $y = g(x)$. Then

$$(-1)^{(f \circ g)(x)} = (-1)^{f(g(x))} = (-1)^{f(y)} = \frac{1}{2^m} \sum_{v \in \mathbb{F}_2^m} W_f(v)(-1)^{\langle v, y \rangle}$$

$$= \frac{1}{2^m} \sum_{v \in \mathbb{F}_2^m} W_f(v)(-1)^{\langle v, g(x) \rangle}$$

$$= \frac{1}{2^m} \sum_{v \in \mathbb{F}_2^m} W_f(v)(-1)^{(l_v \circ g)(x)}.$$

So we have

$$
\begin{aligned}
W_{f\circ g}(w) &= \sum_{x\in \mathbb{F}_2^n} (-1)^{(f\circ g)(x)\oplus\langle w,x\rangle} \\
&= \frac{1}{2^m}\sum_{x\in \mathbb{F}_2^n}\sum_{v\in \mathbb{F}_2^m} W_f(v)(-1)^{(l_v\circ g)(x)\oplus<w,x>} \\
&= \frac{1}{2^m}\sum_{v\in \mathbb{F}_2^m} W_f(v)\sum_{x\in \mathbb{F}_2^n}(-1)^{(l_v\circ g)(x)\oplus<w,x>} \\
&= \frac{1}{2^m}\sum_{v\in \mathbb{F}_2^m} W_f(v)W_{(l_v\circ g)}(w).
\end{aligned}
$$

This proves the result. ■

4 Correlation Theorem

In this section we prove the main correlation theorem. Let $g_1,\ldots,g_t$ be S-boxes, where for $1\le i\le t$, $g_i:\mathbb{F}_2^{m_i+m_{i+1}}\to\mathbb{F}_2^{n_i}$. Let $f:\mathbb{F}_2^n\to\mathbb{F}_2$ be a Boolean function, where $n=n_1+\cdots+n_t$. Let $m=m_1+\cdots+m_{t+1}$ and define a Boolean function $h:\mathbb{F}_2^m\to\mathbb{F}_2$ in the following manner.

$$
h(x_1,\ldots,x_{t+1}) = f(g_1(x_1,x_2),g_2(x_2,x_3),\ldots,g_t(x_t,x_{t+1})) \tag{7}
$$

where $x_i\in\mathbb{F}_2^{m_i}$ for $1\le i\le t+1$. Our task in this section is to compute $W_h(u)$ for $u\in\mathbb{F}_2^m$. This is done through a series of simplifications.

Let $g^{'}:\mathbb{F}_2^m\to\mathbb{F}_2^n$ be an S-box defined by

$$
g^{'}(x_1,\ldots,x_{t+1}) = (g_1(x_1,x_2),\ldots,g_t(x_t,x_{t+1})). \tag{8}
$$

Using the Composition Theorem we have

Proposition 4 *Let h be defined by (7). Then*

$$
W_h(u)=\frac{1}{2^n}\sum_{v\in\mathbb{F}_2^n} W_f(v)W_{(l_v\circ g^{'})}(u).
$$

For $v\in\mathbb{F}_2^n$, write $v=(v_1,\ldots,v_t)$, where $v_i\in\mathbb{F}_2^{n_i}$. We can write

$$
\begin{aligned}
(l_v\circ g^{'})(x_1,\ldots,x_{t+1})=l_v(g^{'}(x_1,\ldots,x_{t+1}) &= l_v((g_1(x_1,x_2),\ldots,g_t(x_t,x_{t+1})) \\
&= l_{v_1}(g_1(x_1,x_2))\oplus\cdots\oplus l_{v_t}(g_t(x_t,x_{t+1})) \\
&= (l_{v_1}\circ g_1)(x_1,x_2))\oplus\cdots\oplus(l_{v_t}\circ g_t)(x_t,x_{t+1})).
\end{aligned} \tag{9}
$$

For $1\le i\le t$, we define

$$
h_i^{'}(x_1,\ldots,x_{t+1}) = (l_{v_i}\circ g_i)(x_i,x_{i+1}). \tag{10}
$$

Given bit strings $u_1,\ldots,u_k$ we define $\delta(u_1,\ldots,u_k)=1$ if each $u_1,\ldots,u_k$ are all-zero bit strings; otherwise $\delta(u_1,\ldots,u_k)=0$. The Walsh transform of $h_i^{'}$ is given by the following proposition.

Proposition 5 *Let h_i' be defined by (10). Then*

$$W_{h_i'}(u) = 2^{M_i} W_{l_{v_i} \circ g_i}(u_i, u_{i+1}) \delta(\omega_i)$$

where $u = (u_1, \ldots, u_{t+1})$, $M_i = m - m_i - m_{i+1}$ and $\omega_i = (u_1, \ldots, u_{i-1}, u_{i+2}, \ldots, u_{t+1})$.

Proof : We compute as follows.

$$\begin{aligned}
W_{h_i'}(u) &= \sum_{x \in \mathbb{F}_2^m} (-1)^{h_i'(x) \oplus \langle u, x \rangle} \\
&= \sum_{x \in \mathbb{F}_2^m} (-1)^{l_{v_i}(g_i(x_i, x_{i+1})) \oplus \langle (u_1, \ldots, u_{t+1}), (x_1, \ldots, x_{t+1}) \rangle} \\
&= \sum_{y_i \in \mathbb{F}_2^{M_i}} (-1)^{\langle \omega_i, y_i \rangle} \times \sum_{(x_i, x_{i+1}) \in \mathbb{F}_2^{m_i + m_{i+1}}} (-1)^{l_{v_i}(g_i(x_i, x_{i+1})) \oplus \langle (u_i, u_{i+1}), (x_i, x_{i+1}) \rangle} \\
&= W_{(l_{v_i} \circ g_i)}(u_i, u_{i+1}) \sum_{y_i \in \mathbb{F}_2^{M_i}} (-1)^{\langle \omega_i, y_i \rangle} \\
&= 2^{M_i} W_{(l_{v_i} \circ g_i)}(u_i, u_{i+1}) \delta(\omega_i)
\end{aligned}$$

where $y_i = (x_1, \ldots, x_{i-1}, x_{i+2}, \ldots, x_{t+1})$. The last statement follows from the fact that $\sum_{z \in \mathbb{F}_2^r} (-1)^{\langle w, z \rangle} = 2^{|w|} \delta(w)$. This completes the proof. ■

Now we obtain the Walsh transform of $(l_v \circ g')$.

Lemma 6 *Let g' be defined as in (8). Then*

$$W_{(l_v \circ g')}(w) = \frac{2^{m_1 + m_{t+1}}}{2^m} \sum_{u \in \mathbb{F}_2^M} \prod_{i=1}^{t} W_{(l_{v_i} \circ g_i)}(w_{t,i} \oplus w_{i-1,i}, w_{i,i+1})$$

where $M = m - m_1 - m_{t+1}$, $w = w_t = (w_{t,1}, \ldots, w_{t,t+1})$ with $w_{t,i} \in \mathbb{F}_2^{m_i}$, $u = (w_{1,2}, \ldots, w_{t-1,t})$ and for $1 \le i \le t$, $w_{i-1,i} \in \mathbb{F}_2^{m_i}$ with $w_{0,1} = (0, \ldots, 0)$.

Proof : Using (9), (10) and the Generalized Convolution Theorem, we have

$$W_{(l_v \circ g')}(w_t) = \frac{1}{2^{m(t-1)}} \sum_{(w_1, \ldots, w_{t-1})} \prod_{i=1}^{t} W_{h_i'}(w_i \oplus w_{i-1})$$

where $w_i \in \mathbb{F}_2^m$ for $0 \le i \le t-1$ and $w_0 = (0, \ldots, 0)$. For $0 \le i \le t$, write $w_i = (w_{i,1}, \ldots, w_{i,t+1})$ with $w_{i,j} \in \mathbb{F}_2^{m_j}$. Set $\alpha_{i,j} = w_{i,j} \oplus w_{i-1,j}$ and $\alpha_i = (\alpha_{i,1}, \ldots, \alpha_{i,t+1}) = w_i \oplus w_{i-1}$.
Set $\beta_i^t = (\alpha_{i,1}, \ldots, \alpha_{i,i-1}, \alpha_{i,i+2}, \ldots, \alpha_{i,t+1})$. Using Proposition 5, we obtain

$$\begin{aligned}
W_{(l_v \circ g')}(w_t) &= \frac{1}{2^{m(t-1)}} \sum_{(w_1, \ldots, w_{t-1})} \prod_{i=1}^{t} W_{h_i'}(\alpha_i) \\
&= \frac{1}{2^{m(t-1)}} \sum_{(w_1, \ldots, w_{t-1})} \prod_{i=1}^{t} 2^{M_i} W_{l_{v_i} \circ g_i}(\alpha_{i,i}, \alpha_{i,i+1}) \delta(\beta_i^t) \\
&= \frac{2^{m_1 + m_{t+1}}}{2^m} \sum_{(w_1, \ldots, w_{t-1})} \prod_{i=1}^{t} W_{l_{v_i} \circ g_i}(\alpha_{i,i}, \alpha_{i,i+1}) \delta(\beta_i^t)
\end{aligned}$$

The proof now follows from the following claim.
Claim: For $t \geq 2$, we have

$$\sum_{(w_1,\ldots,w_{t-1})} \prod_{i=1}^{t} W_{l_{v_i} \circ g_i}(\alpha_{i,i}, \alpha_{i,i+1})\delta(\beta_i^t) \quad = \quad \sum_{(w_{1,2},\ldots,w_{t-1,t})} \prod_{i=1}^{t} W_{(l_{v_i} \circ g_i)}(w_{t,i} \oplus w_{i-1,i}, w_{i,i+1}) \qquad (11)$$

Proof : The claim is proved by induction on $t \geq 2$. Let $\mathcal{L}_t$ (resp. $\mathcal{R}_t$) be the left (resp. right) side of (11).
Base : Case $t = 2$. In this case, the left side becomes

$$\mathcal{L}_2 = \sum_{w_1} W_{l_{v_1} \circ g_1}(\alpha_{1,1}, \alpha_{1,2})\delta(\beta_1^2) W_{l_{v_2} \circ g_2}(\alpha_{2,2}, \alpha_{2,3})\delta(\beta_2^2).$$

Note that $\beta_1^2 = \alpha_{1,3} = w_{1,3} \oplus w_{0,3} = w_{1,3}$ and $\beta_2^2 = \alpha_{2,1} = w_{2,1} \oplus w_{1,1}$. Substituting the value of α's, we write the above expression as

$$\begin{aligned}
\mathcal{L}_2 &= \sum_{w_{1,1}} \sum_{w_{1,2}} \sum_{w_{1,3}} W_{l_{v_1} \circ g_1}(w_{1,1}, w_{1,2}) W_{l_{v_2} \circ g_2}(w_{2,2} \oplus w_{1,2}, w_{2,3} \oplus w_{1,3})\delta(w_{1,3})\delta(w_{2,1} \oplus w_{1,1}) \\
&= \sum_{w_{1,1}} \sum_{w_{1,2}} W_{l_{v_1} \circ g_1}(w_{1,1}, w_{1,2}) W_{l_{v_2} \circ g_2}(w_{2,2} \oplus w_{1,2}, w_{2,3})\delta(w_{2,1} \oplus w_{1,1}) \\
&= \sum_{w_{1,2}} \sum_{w_{1,1}} W_{l_{v_1} \circ g_1}(w_{1,1}, w_{1,2}) W_{l_{v_2} \circ g_2}(w_{2,2} \oplus w_{1,2}, w_{2,3})\delta(w_{2,1} \oplus w_{1,1}) \\
&= \sum_{w_{1,2}} W_{l_{v_1} \circ g_1}(w_{2,1}, w_{1,2}) W_{l_{v_2} \circ g_2}(w_{2,2} \oplus w_{1,2}, w_{2,3})
\end{aligned}$$

which is equal to $\mathcal{R}_2$, i.e., the right side of the claim for $t = 2$.
Induction hypothesis : Assume that the claim is true for $t - 1$.
Induction step : We now prove the result for t. We will use the induction hypothesis in this case. The main difficulty arises from the fact that the length of the w's and the α's increases by one. We have to take care of this while applying the induction hypothesis. First note that for $1 \leq i \leq t - 1$, we have $\delta(\beta_i^t) = \delta(\beta_i^{t-1})\delta(\alpha_{i,t+1})$. Now we compute

$$\begin{aligned}
\mathcal{L}_t &= \sum_{(w_1,\ldots,w_{t-2})} \prod_{i=1}^{t-1} W_{l_{v_i} \circ g_i}(\alpha_{i,i}, \alpha_{i,i+1})\delta(\beta_i^t) \sum_{w_{t-1}} W_{l_{v_t} \circ g_t}(\alpha_{t,t}, \alpha_{t,t+1})\delta(\beta_t^t) \\
&= \sum_{(w_1,\ldots,w_{t-2})} \prod_{i=1}^{t-1} W_{l_{v_i} \circ g_i}(\alpha_{i,i}, \alpha_{i,i+1})\delta(\beta_i^{t-1}) \\
&\quad \times \sum_{(w_{1,t+1},\ldots,w_{t-2,t+1})} \delta(\alpha_{1,t+1}) \ldots \delta(\alpha_{t-2,t+1}) \\
&\quad \times \sum_{w_{t-1}} W_{l_{v_t} \circ g_t}(\alpha_{t,t}, \alpha_{t,t+1})\delta(\beta_t^t) \\
&= \sum_{(w_1,\ldots,w_{t-2})} \prod_{i=1}^{t-1} W_{l_{v_i} \circ g_i}(\alpha_{i,i}, \alpha_{i,i+1})\delta(\beta_i^{t-1}) \\
&\quad \times \sum_{(w_{t-1,1},\ldots,w_{t-1,t})} \delta(\alpha_{t,1})\delta(\alpha_{t,2}) \ldots \delta(\alpha_{t,t-1}) \\
&\quad \times \sum_{(w_{1,t+1},\ldots,w_{t-2,t+1},w_{t-1,t+1})} W_{l_{v_t} \circ g_t}(\alpha_{t,t}, \alpha_{t,t+1})\delta(\alpha_{1,t+1}) \ldots \delta(\alpha_{t-2,t+1}).
\end{aligned}$$

Note that $\alpha_{1,t+1} = w_{1,t+1} \oplus w_{0,t+1} = w_{1,t+1}$ and for $i > 1$, $\alpha_{i,t+1} = w_{i,t+1} \oplus w_{i-1,t+1}$. Thus the expression within the last sum evaluates to $W_{l_{v_t} \circ g_t}(\alpha_{t,t}, \alpha_{t,t+1})$ only under the condition $w_{1,t+1} = \cdots = w_{t-2,t+1} = (0, \ldots, 0)$. Also the expression within the second sum evaluates to 1 only under the condition $w_{t,i} = w_{t-1,i}$ for $1 \le i \le t-1$. We invoke the induction hypothesis on the first sum to obtain.

$$\begin{aligned}
\mathcal{L}_t &= \sum_{(w_{1,2},\ldots,w_{t-2,t-1})} \prod_{i=1}^{t-1} W_{(l_{v_i} \circ g_i)}(w_{t-1,i} \oplus w_{i-1,i}, w_{i,i+1}) \\
&\quad \times \sum_{w_{t-1,t}} W_{l_{v_t} \circ g_t}(\alpha_{t,t}, \alpha_{t,t+1}) \\
&= \mathcal{R}_t.
\end{aligned}$$

This completes the proof of the claim and the lemma. ■

Finally using Proposition 4 and Lemma 6 we obtain the Walsh transform of W_h.

Theorem 7 *Let h be defined as in (7). Then*

$$W_h(w) = \frac{2^{m_1+m_{t+1}}}{2^{n+m}} \sum_{v \in \mathbb{F}_2^n} W_f(v) \sum_{u \in \mathbb{F}_2^M} \prod_{i=1}^{t} W_{(l_{v_i} \circ g_i)}(w_{t,i} \oplus w_{i-1,i}, w_{i,i+1}) \tag{12}$$

where $M = m - m_1 - m_{t+1}$, $w = w_t = (w_{t,1}, \ldots, w_{t,t+1})$ with $w_{t,i} \in \mathbb{F}_2^{m_i}$, $u = (w_{1,2}, \ldots, w_{t-1,t})$ and for $1 \le i \le t$, $w_{i-1,i} \in \mathbb{F}_2^{m_i}$ with $w_{0,1} = (0, \ldots, 0)$.

5 Nyberg's Correlation Theorems

In [8], Nyberg stated three correlation theorems – Theorems 3, 4 and 5 – which have important applications to cryptanalysis. Of these, Theorem 4 has been proved in [7] and the other two theorems are proved in [8]. In this section, we show that Nyberg's correlation theorems – Theorem 3 and 5 of [8] – can be obtained as special cases of Theorem 7. First we rewrite Theorem 7 for $t = 2$.

Theorem 8 *Let h be defined as in (7) and $t = 2$. Then*

$$W_h(w_{2,1}, w_{2,2}, w_{2,3}) = \frac{2^{m_1+m_3}}{2^{m+n}} \sum_{v \in \mathbb{F}_2^n} W_f(v) \sum_{w_{1,2} \in \mathbb{F}_2^{m_2}} W_{l_{v_1} \circ g_1}(w_{2,1}, w_{1,2}) W_{l_{v_2} \circ g_2}(w_{2,2} \oplus w_{1,2}, w_{2,3}) \tag{13}$$

where $v = (v_1, v_2)$ with $v_i \in \mathbb{F}_2^{n_i}$.

A special case is obtained when f is the linear function $f(a_1, \ldots, a_n) = a_1 \oplus \cdots \oplus a_n$. In this case $W_f(1, \ldots, 1) = 2^n$ and $W_f(v) = 0$ for $v \in \mathbb{F}_2^n \setminus \{(1, \ldots, 1)\}$. Also $v_1 = (1, \ldots, 1) \in \mathbb{F}_2^{n_1}$ and $v_2 = (1, \ldots, 1) \in \mathbb{F}_2^{n_2}$. We denote by $\mathbf{1}_k$ the all one vector of length k. When the value of k is clear from the context, we will simply write $\mathbf{1}$. We have the following corollary to Theorem 8.

Corollary 9 *Let $h(x_1, x_2, x_3) = \langle \mathbf{1}_n, (g_1(x_1, x_2), g_2(x_2, x_3)) \rangle$. Then*

$$W_h(w_{2,1}, w_{2,2}, w_{2,3}) = \frac{2^{m_1+m_3}}{2^m} \sum_{w_{1,2} \in \mathbb{F}_2^{m_2}} W_{l_{\mathbf{1}_{n_1}} \circ g_1}(w_{2,1}, w_{1,2}) W_{l_{\mathbf{1}_{n_2}} \circ g_2}(w_{2,2} \oplus w_{1,2}, w_{2,3}).$$

Substituting $n_1 = n_2 = 1$ we obtain $h(x_1, x_2, x_3) = g_1(x_1, x_2) \oplus g_2(x_2, x_3)$. Further, substituting $w_{2,2} = 0$ in Corollary 9 we obtain the the following result of Nyberg [8] (stated in terms of Walsh transform).

Theorem 10 (Nyberg [8], Theorem 5) *Let* $h(x_1,x_2,x_3) = g_1(x_1,x_2) \oplus g_2(x_2,x_3)$. *Then*

$$W_h(w_{2,1},0,w_{2,3}) = \frac{2^{m_1+m_3}}{2^m} \sum_{w_{1,2}\in\mathbb{F}_2^{m_2}} W_{g_1}(w_{2,1},w_{1,2})W_{g_2}(w_{1,2},w_{2,3}).$$

Now we turn to Theorem 3 of Nyberg [8]. For this we make the following substitution in the definition of h: $m_2 = 0$, $g = g_2$, $g_1(x) = x$ and hence $n_1 = m_1$. Thus h is now of the form $h(x_1,x_3) = f(x_1, g(x_3))$. In this situation, we have

$$\sum_{w_{1,2}\in\mathbb{F}_2^{m_2}} W_{l_{v_1}\circ g_1}(w_{2,1},w_{1,2})W_{l_{v_2}\circ g_2}(w_{2,2}\oplus w_{1,2},w_{2,3}) = W_{l_{v_1}\circ g_1}(w_{2,1})W_{l_{v_2}\circ g_2}(w_{2,3}).$$

Since $g_1(x) = x$, we have $(l_{v_1}\circ g_1)(x) = l_{v_1}(g_1(x)) = l_{v_1}(x) = \langle v_1, x\rangle$ and hence $W_{l_{v_1}\circ g_1}(w_{2,1}) = 2^{m_1}\delta(v_1 \oplus w_{2,1})$. Let the right side of the (13) be $\mathcal{A}$. In this case $\mathcal{A}$ becomes

$$\begin{aligned}
\mathcal{A} &= \frac{1}{2^{n_1+n_2}} \sum_{v\in\mathbb{F}_2^n} W_f(v) \sum_{w_{1,2}\in\mathbb{F}_2^{m_2}} W_{l_{v_1}\circ g_1}(w_{2,1},w_{1,2})W_{l_{v_2}\circ g_2}(w_{2,2}\oplus w_{1,2},w_{2,3}) \\
&= \frac{1}{2^{n_1+n_2}} \sum_{(v_1,v_2)\in\mathbb{F}_2^n} W_f(v_1,v_2)W_{l_{v_1}\circ g_1}(w_{2,1})W_{l_{v_2}\circ g_2}(w_{2,3}) \\
&= \frac{1}{2^{n_2}} \sum_{v_2\in\mathbb{F}_2^{n_2}} W_f(w_{2,1},v_2)W_{l_{v_2}\circ g}(w_{2,3}).
\end{aligned}$$

Now we have the following result of Nyberg [8] again stated in terms of Walsh transform.

Theorem 11 (Nyberg [8], Theorem 3) *Let* $h(x_1,x_3) = f(x_1, g(x_3))$. *Then*

$$W_h(w_{2,1},w_{2,3}) = \frac{1}{2^{n_2}} \sum_{v_2\in\mathbb{F}_2^{n_2}} W_f(w_{2,1},v_2)W_{l_{v_2}\circ g}(w_{2,3}).$$

6 Applications

In this section, we consider two other applications of Theorem 7. These are based on structures which typically occur in design of symmetric ciphers.

6.1 Brick Layering

In this section, we consider a map of the form

$$h(x,y,z) = g(g(x,y)\oplus g(y,z)). \tag{14}$$

Figure 1 gives a diagrammatic view of the map. The term brick layering was used in [1]. In block cipher applications g is usually an $2k$-bit to $2k$-bit S-box possibly the inverse function over $GF(2^{2k})$. For the purposes of analysing ciphers employing such mappings, it is useful to know the Walsh transform of h. We perform this task here, under the assumption that g is an $2k$-bit to $2k$-bit map and x, y and z are all k-bit strings. Let $g_1,\cdots,g_{2k}$ be the component functions of g. Let $\nu_i(x,y,z) = g_i(x,y)\oplus g_i(y,z)$ and $\nu = (\nu_1,\ldots,\nu_{2k})$. Applying Corollary 9 with $n_1 = n_2 = 1$ we obtain

$$W_{\nu_i}(\delta_1,\delta_2,\delta_3) = \frac{1}{2^k} \sum_{u\in\mathbb{F}_2^k} W_{g_i}(u\oplus\delta_2,\delta_3)W_{g_i}(u,\delta_1) \tag{15}$$

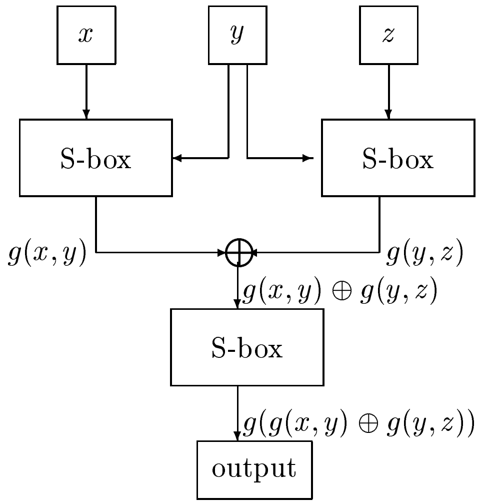

Figure 1: Brick layering transformation.

Let $h_1, \ldots, h_{2k}$ be the component functions of h. We have $h_i(x,y,z) = g_i(\nu_1(x,y,z), \ldots, \nu_{2k}(x,y,z))$. Now applying the Composition Theorem we get for $(\gamma_1, \gamma_2, \gamma_3) \in \{0,1\}^{3k}$,

$$W_{h_i}(\gamma_1, \gamma_2, \gamma_3) = \frac{1}{2^{2k}} \sum_{v \in \mathbb{F}_2^{2k}} W_{g_i}(v) W_{(l_v \circ \nu)}(\gamma_1, \gamma_2, \gamma_3) \tag{16}$$

The next step is to compute the Walsh transform of $(l_v \circ \nu)$. Let v be of weight r (i.e., $\mathsf{wt}(v) = r$) with the bits in the $j_1, \ldots, j_r$th positions to be 1 and all others to be 0. Then $(l_v \circ \nu)(x,y,z) = \mu_1(x,y,z) \oplus \cdots \oplus \mu_r(x,y,z)$, where $\mu_i = \nu_{j_i}$ for $1 \leq i \leq r$. Further, let $s = 3k(\mathsf{wt}(v) - 1)$, $w = (u_1, \ldots, u_{r-1})$, with each $u_i \in \mathbb{F}_2^{3k}$, $u_0 = (0, \ldots, 0) \in \mathbb{F}_2^{3k}$ and $u_r = (\gamma_1, \gamma_2, \gamma_3)$. Now applying the Generalized Convolution Theorem, we have

$$W_{(l_v \circ \nu)}(\gamma_1, \gamma_2, \gamma_3) = \frac{1}{2^s} \sum_{w \in \mathbb{F}_2^s} \prod_{i=1}^{r} W_{\mu_i}(u_i \oplus u_{i-1}) = \frac{1}{2^s} \sum_{w \in \mathbb{F}_2^s} \prod_{i=1}^{r} W_{\nu_{j_i}}(u_i \oplus u_{i-1}).$$

Substituting in (16) and using (15) we obtain the Walsh transform for any component function of the map defined in (14).

Theorem 12 *Let h be an S-box defined as in (14) and let $h_1, \ldots, h_{2k}$ be its component functions. Then*

$$\begin{aligned} W_{h_i}(\gamma_1, \gamma_2, \gamma_3) &= \frac{1}{2^{2k}} \sum_{v \in \mathbb{F}_2^{2k}} W_{g_i}(v) \frac{1}{2^{s+kr}} \\ &\times \sum_{(u_1, \ldots, u_{r-1})} \prod_{i=1}^{r} \sum_{w \in \mathbb{F}_2^k} W_{g_{j_i}}(w \oplus u_{i,2} \oplus u_{i-1,2}, u_{i,3} \oplus u_{i-1,3}) W_{g_{j_i}}(w, u_{i,1} \oplus u_{i-1,1}) \end{aligned}$$

where $u_i = (u_{i,1}, u_{i,2}, u_{i,3})$ with $u_{i,j} \in \mathbb{F}_2^k$ and for each $v \in \mathbb{F}_2^{2k}$, $r = \mathsf{wt}(v)$, $u_r = (\gamma_1, \gamma_2, \gamma_3)$.

Theorem 12 provides the complete expression for the Walsh transform of any h_i. In practice, this might be too complicated to work with and will have to be simplified or approximated depending on the particular application in hand.

6.2 Substitute-and-Add

In this section, we consider the map obtained by alternate application of an S-box and sum modulo 2^{2k}. More precisely, we consider the following map.

$$h(x,y) \quad = \quad g(x)\boxed{+}g(y). \tag{17}$$

The map is shown diagrammatically in Figure 2. We obtain the complete Walsh transform of each component function of h. As before we consider g to be an $2k$-bit to $2k$-bit S-box whose component functions are $g_1, \ldots, g_{2k}$.

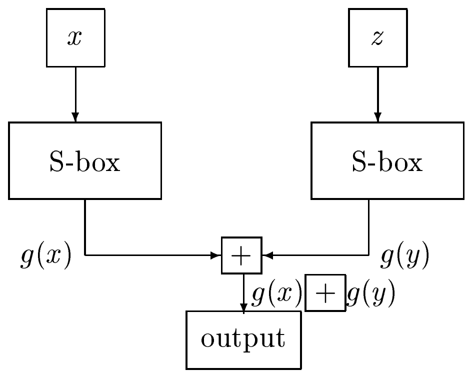

Figure 2: Substitute and add.

For the sake of convenience, we will denote $\nu(x,y) = x\boxed{+}y$. The map ν is conveniently described by separating the carry part. Suppose $(a_1, \ldots, a_{2k})$ and $(b_1, \ldots, b_{2k})$ are the inputs to $\boxed{+}$. Then the carry in the ith position is given by the function $c_{(}a_1, \ldots, a_i, b_1, \ldots, b_i)$ and $\nu_i = a_i \oplus b_i \oplus c_i$. The Walsh transform of the carry function has been described in [11]. Let $h_1, \ldots, h_{2k}$ be the component functions of h. We can now write

$$h_i(x,y) \quad = \quad g_i(x) \oplus g_i(y) \oplus c_i(g_1(x), \ldots, g_i(x), g_1(y), \ldots, g_i(y)).$$

Let $f_i(x,y) = c_i(g_1(x), \cdots, g_i(x), g_1(y), \cdots, g_i(y))) = c_i(\mu_i(x,y))$ where $\mu_i : \{0,1\}^{4k} \to \{0,1\}^{2i}$ is defined as $\mu_i(x,y) = (g_1(x), \cdots, g_i(x), g_1(y), \cdots, g_i(y))$. Applying the Composition Theorem for $(u,v) \in \{0,1\}^{2k}$, we have

$$W_{f_i}(u,v) \quad = \quad \frac{1}{2^{2i}} \sum_{w \in \mathbb{F}_2^{2i}} W_{c_i}(w) W_{(l_w \circ \mu_i)}(u,v)$$

Let $\lambda_i(x,y) = g_i(x) \oplus g_i(y)$ and hence $W_{\lambda_i}(u,v) = W_{g_i}(u) W_{g_i}(v)$. We have $h_i(x,y) = \lambda_i(x,y) \oplus, f_i(x,y)$. Using the convolution Theorem we have

$$\begin{aligned}
W_{h_i}(u,v) &= \frac{1}{2^{4k}} \sum_{(u_1,v_1) \in \mathbb{F}_2^{2k+2k}} W_{\lambda_i}(u_1,v_1) W_{f_i}(u \oplus u_1, v \oplus v_1) \\
&= \frac{1}{2^{4k}} \sum_{(u_1,v_1) \in \mathbb{F}_2^{2k+2k}} W_{g_i}(u_1) W_{g_i}(v_1) W_{f_i}(u \oplus u_1, v \oplus v_1) \\
&= \frac{1}{2^{4k+2i}} \sum_{(u_1,v_1) \in \mathbb{F}_2^{2k+2k}} W_{g_i}(u_1) W_{g_i}(v_1) \sum_{w \in \mathbb{F}_2^{2i}} W_{c_i}(w) W_{(l_w \circ \mu_i)}(u \oplus u_1, v \oplus v_1).
\end{aligned}$$

Thus we get the following result.

Theorem 13 *Let h be defined as in (17) and $h_1, \ldots, h_{2k}$ be its component functions. Then*

$$W_{h_i}(u,v) = \frac{1}{2^{4k+2i}} \sum_{(u_1,v_1)\in\mathbb{F}_2^{2k+2k}} W_{g_i}(u_1)W_{g_i}(v_1) \sum_{w\in\mathbb{F}_2^{2i}} W_{c_i}(w)W_{(l_w\circ\mu_i)}(u\oplus u_1, v\oplus v_1)$$

where $\mu_i(x,y) = (g_1(x), \cdots, g_i(x), g_1(y), \cdots, g_i(y))$.

The complete expression for $W_{h_i}(u,v)$ is obtained by computing the Walsh transform of $(l_w \circ \mu_i)$. This requires one more invocation of the Convolution Theorem and hence involves another summation. As in the previous case, the resulting expression becomes probably too complicated for practical analysis. Again depending on the context in which the result is applied, it should be possible to simplify or approximate the expression.

7 Conclusion

We have proved a result which provides the Walsh transform of a very general functional form. As special cases, we obtain two of Nyberg's correlation theorems proved in [8]. We also apply the result to two typical structures occuring in design of symmetric ciphers and obtain the complete expression of the Walsh transform in each case. It appears that our result can be applied to other situations and this remains a task of future research work.

References

[1] J. Daemen and V. Rijmen. *The Design of Rijndael: AES* - The Advanced Encryption Standard (Information Security and Cryptography). Spriner-Verlag 2002.

[2] C. Harpes, G. G. Kramer and J. L. Massey. A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-up Lemma. In *Advances in Cryptology - EUROCRYPT 1995*, pages 24–38, Lecture Notes in Computer Science, Springer-Verlag, 1995.

[3] M. Hermelin and K. Nyberg. Correlation Properties of the Bluetooth Combiner Generator. *The Second International Conference on Information Security and Cryptology of ICISC '99*, pages 17–29, Lecture Notes in Computer Science, Springer-Verlag, 2000.

[4] F. J. MacWillams and N. J. A. Sloane. *The Theory of Error Correcting Codes.* North Holland, 1977.

[5] M. Matsui. Linear Cryptanalysis Method for DES Cipher. In *Advances in Cryptology - EUROCRYPT 1993*, pages 386–397, Lecture Notes in Computer Science, Springer-Verlag, 1994.

[6] W. Meier and O. Staffelbach. Correlation Properties of Combiners with Memory in Stream Cipher. J. Cryptology. 5 (1) (1992) 67-86

[7] K. Nyberg. Linear Approximation of Block Ciphers. In *Advances in Cryptology - EUROCRYPT 1994*, pages 439–444, Lecture Notes in Computer Science, Springer-Verlag, 1995.

[8] K. Nyberg. Correlation Theorems in Cryptanalysis. Discrete Applied Mathematics 111 (2001) 177-188.

[9] P. Sarkar and S. Maitra. Cross-Correlation Analysis of Cryptographically Useful Boolean Functions and S-Boxes. Theory of Computing Systems , 35(1): 39-57 (2002).

[10] O. Staffelbach and W. Meier. Cryptographic Significance of the Carry for Ciphers Based on Integer Addition. In *Advances in Cryptology - CRYPT0 1990*, pages 601–615, Lecture Notes in Computer Science, Springer-Verlag, 1991.

[11] J Wallén. Linear Approximation of Addition Modulo 2^n. *Tenth Annual Workshop on Fast Software Encryption* , February 24-26, 2003, AF-Borgen, Lund, Sweden, pages 277–290, Pre-proceedings.