

Combining all the probabilities, we prove that $\text{Adv}(t, m)$ is bounded by

$$\frac{\lfloor t/c_* \rfloor + 2m}{|PW|} + O\left(\frac{(t + c_* m)^2}{2^n}\right)$$

as stated.

For the lower bound, we describe two strategies from which the adversary can pick the one yielding better success probability depending on the parameters. In strategy A, the adversary computes separate paths of length c_* for $\lfloor (t - c_*)/c_* \rfloor$ passwords $p_i \| s \| c_*$ using $t - c_*$ Type 1 queries. He then makes a Type 2 query asking for $y = F_p^*(s, c_*)$. With probability $\lfloor (t - c_*)/c_* \rfloor / |PW|$, vertex y coincides with the endpoint of one of the paths, thus revealing the password p_0 . In such an event, the adversary then makes c_0 more Type 1 queries to compute $y'_0 = H^{(c_0)}(p_0 \| s_0 \| c_0)$ and answers 1 if $y'_0 = y_0$. All together the adversary used at most t Type 1 and one Type 2 queries to achieve success probability of $\lfloor (t - c_*)/c_* \rfloor / |PW|$.

In strategy B, the adversary constructs Q_1 to be a single path of length t starting from an arbitrary $p \| s \| c$. With probability $1 - O(t^2/2^n)$, the path will be cycle free. Its first $t - c_*$ vertices $p_i \| s_i \| c_i$ have their full paths $T_{p_i \| s_i \| c_i}$ completely contained in Q_1 . Assuming m to be much smaller than $t - c_*$, the adversary can pick m vertices $p_i \| s_i \| c_i$ along the path with distinct p_i and make at most m Type 2 queries with the corresponding (s_i, c_i) 's. With probability $m/|PW|$, it can identify the password. This completes the proof of Theorem 2. QED

VIII. CONCLUSION

Password-based KDFs are necessary in many security application. Despite their importance and widespread usage, rigorous analysis of such functions seems to have received relatively little attention in the literature compared to many other cryptographic schemes.

In this paper, we define a general security framework for password-based KDFs where salt and iteration count are included as parameters. Under this framework, we focus on the most commonly used construction $H^{(c)}(p \| s)$ and prove that the iteration count c , when fixed, does have an effect of stretching the password by $\log_2 c$ bits. Our analysis is done using a random functional graph representing H , conditioned upon a query graph representing information revealed to the attacker. It provides insights on the exact way that each parameter contributes to the overall security.

We then analyze two widely deployed KDFs defined in PKCS#5. We show that both are secure if the adversary cannot influence the parameters, but are subject to attacks otherwise. We also consider how such security weaknesses can be exploited in practice.

Finally, based on the insight gained from our earlier analysis, we propose a new password-based key derivation that is provably secure even when the attacker has full control of the salt and iteration count. The new proposal achieves stronger security while preserving the same efficiency as existing KDFs. We expect that the new proposal will find its application in practical implementations.

ACKNOWLEDGMENT

The authors wish to thank the Associate Editor and the anonymous reviewers for their careful reading and useful comments.

REFERENCES

- [1] *Digital Signature Standard*, 1994. FIPS PUB 186-2, National Institute of Standards and Technologies.
- [2] *Standard Specifications for Public-Key Cryptography*, 2000. IEEE Std 1363-2000, IEEE Computer Society.
- [3] *PKCS#5 v2.0: Password-Based Cryptography Standard*, 1999. RSA Laboratories.
- [4] T. Dierks and C. Allen, "The TLS protocol version 1.0. IETF RFC 2246," Internet Request for Comments, Jan. 1999.
- [5] J. Kelsey, B. Schneier, C. Hall, and D. Wagner, "Secure applications of low-entropy keys," in *Proc. First Int. Workshop ISW'97*. New York: Springer-Verlag, 1998.
- [6] A. Hevia, A. Desai, and Y. L. Yin, "A practical-oriented treatment of pseudorandom number generators," in *Advances in Cryptology—EUROCRYPT'02*. Berlin, Germany: Springer-Verlag, 2002.
- [7] IEEE P1363.2: Standard Specifications for Password-Based Public-Key Cryptographic Techniques, Draft D15 (2004, May). [Online]. Available: <http://grouper.ieee.org/groups/1363/passwdPK/draft.html>
- [8] M. Bellare, R. Canetti, and H. Krawczyk, "Keyed hash functions for message authentication," in *Advances in Cryptology—CRYPTO'96*. Berlin, Germany: Springer-Verlag, 1996.
- [9] P. Flajolet and A. M. Odlyzko, "Random mapping statistics," in *Advances in Cryptology—EUROCRYPT'89*. Berlin, Germany: Springer-Verlag, 1990.

Toward a General Correlation Theorem

Kishan Chand Gupta and Palash Sarkar

Abstract—In 2001, Nyberg proved three important correlation theorems and applied them to several cryptanalytic contexts. We continue the work of Nyberg in a more theoretical direction. We consider a general functional form and obtain its Walsh transform. Two of Nyberg's correlation theorems are seen to be special cases of our general functional form. S-box lookup, addition modulo 2^{2k} , and X-OR are three frequently occurring operations in the design of symmetric ciphers. We consider two methods of combining these operations and in each apply our main result to obtain the Walsh transform.

Index Terms—Boolean function, correlation, linear approximation, S-box, symmetric cipher, Walsh transform.

I. 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.

Manuscript received December 5, 2004; revised June 5, 2005.

K. C. Gupta was with the Applied Statistics Unit, Indian Statistical Institute, Kolkata 700 108, India. He is now with the Centre for Applied Cryptographic Research, University of Waterloo, Waterloo, ON N2L 3G1, Canada. (e-mail: kishan_t@isical.ac.in).

P. Sarkar is with the Applied Statistics Unit, Indian Statistical Institute, Calcutta 700 108, India (e-mail: palash@isical.ac.in).

Communicated by E. Okamoto, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2005.853326

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 this correspondence is to continue the direction of research initiated in [8]. We obtain the Walsh transform for the following general functional form:

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

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 $\mathbb{F}_2^{n_1+\dots+n_t}$ to \mathbb{F}_2 . We obtain a closed-form expression for the Walsh transform of h in terms of the Walsh transform of f and g_1, \dots, g_t . We show that two of Nyberg's results in [8] are special cases of our theorem. This underlines the importance of our result in the context of symmetric cipher cryptanalysis.

We also consider two applications of our result. The operations of S-box lookup, X-OR, and addition modulo 2^{2k} typically occur in the design of block and stream ciphers. We consider two possible ways of combining these operations. The first method is the 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 method considers the situation where an S-box is combined with addition modulo 2^{2k} . In both cases, we obtain complete expressions for the Walsh transform.

II. PRELIMINARIES

Let $\mathbb{F}_2 = \text{GF}(2)$ 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 $\text{wt}(x)$.

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

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

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

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

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

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. The correlation between two n -variable Boolean functions f and g is defined in the following manner (see, for example, [8]):

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

We have the following relationship: $c(f, g) = 2^{-n} W_{f \oplus g}(0)$ and $c(f, l_v) = 2^{-n} W_f(v)$, 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.

III. CONVOLUTION AND COMPOSITION THEOREMS FOR S-BOXES

The convolution for two n -variable Boolean functions is well known (see, for example, [1]).

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

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

We next prove a generalization of the Convolution Theorem.

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

$$\begin{aligned} W_h(u) &= \frac{1}{2^s} \sum_{v \in \mathbb{F}_2^s} W_{g_k}(u \oplus u_{k-1}) W_{g_{k-1}}(u_{k-1} \oplus u_{k-2}) \\ &\quad \dots W_{g_2}(u_2 \oplus u_1) W_{g_1}(u_1) \\ &= \frac{1}{2^s} \sum_{v \in \mathbb{F}_2^s} \prod_{i=1}^k W_{g_i}(u_i \oplus u_{i-1}) \end{aligned}$$

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

Proof: We prove Theorem 2 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 $f(x) = g_1(x) \oplus \dots \oplus g_{k-1}(x)$. This gives

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

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

$$\begin{aligned} W_h(u) &= \frac{1}{2^n} \sum_{u_{k-1} \in \mathbb{F}_2^n} W_{g_k}(u_k \oplus u_{k-1}) \\ &\quad \times \left(\frac{1}{2^{n(k-2)}} \sum_{(u_1, \dots, u_{k-2})} \prod_{i=1}^{k-1} W_{g_i}(u_i \oplus u_{i-1}) \right) \\ &= \frac{1}{2^s} \sum_{v \in \mathbb{F}_2^s} \prod_{i=1}^k W_{g_i}(u_i \oplus u_{i-1}). \end{aligned}$$

This proves the result. \square

Now we provide the Walsh transform of composition of an S-box and a Boolean function. A similar result is stated in [1] in terms of correlation matrices.

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

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

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

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

So we have

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

This proves the result. \square

IV. CORRELATION THEOREM

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

$$h(x_1, \dots, x_{t+1}) = f(g_1(x_1, x_2), g_2(x_2, x_3), \dots, g_t(x_t, x_{t+1})) \quad (5)$$

where $x_i \in \mathbb{F}_2^{m_i}$ for $1 \leq i \leq t+1$. Our task in this section is to compute $W_h(u)$ for $u \in \mathbb{F}_2^m$. In Theorem 4 (see later) we show that $W_h(w)$ is given by the following expression:

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

where $v = (v_1, \dots, v_t)$ with $v_i \in \mathbb{F}_2^{n_i}$, $M = m - m_1 - m_{t+1}$, $w = w_t = (w_{t,1}, \dots, w_{t,t+1})$ with $w_{t,i} \in \mathbb{F}_2^{m_i}$, $u = (w_{1,2}, \dots, w_{t-1,t})$ and for $1 \leq i \leq t$, $w_{i-1,i} \in \mathbb{F}_2^{m_i}$ with $w_{0,1} = (0, \dots, 0)$.

This result is obtained through a series of simplifications. Let $g': \mathbb{F}_2^m \rightarrow \mathbb{F}_2^n$ be an S-box defined by

$$g'(x_1, \dots, x_{t+1}) = (g_1(x_1, x_2), \dots, g_t(x_t, x_{t+1})). \quad (6)$$

Using the Composition Theorem we have the following result.

Proposition 1: Let h be defined by (5). 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 $v = (v_1, \dots, v_t)$, where $v_i \in \mathbb{F}_2^{n_i}$. We can write

$$\begin{aligned} (l_v \circ g')(x_1, \dots, x_{t+1}) &= l_v(g'(x_1, \dots, x_{t+1})) \\ &= l_v((g_1(x_1, x_2), \dots, g_t(x_t, x_{t+1}))) \\ &= l_{v_1}(g_1(x_1, x_2)) \oplus \dots \oplus l_{v_t}(g_t(x_t, x_{t+1})) \\ &= (l_{v_1} \circ g_1)(x_1, x_2) \oplus \dots \oplus (l_{v_t} \circ g_t)(x_t, x_{t+1}). \end{aligned} \quad (7)$$

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

$$h'_i(x_1, \dots, x_{t+1}) = (l_{v_i} \circ g_i)(x_i, x_{i+1}). \quad (8)$$

Given bit strings u_1, \dots, u_k we define $\delta(u_1, \dots, u_k) = 1$ if each u_1, \dots, u_k are all-zero bit strings; otherwise, $\delta(u_1, \dots, u_k) = 0$.

The Walsh transform of h'_i is given by the following proposition.

Proposition 2: Let h'_i be defined by (8). Then

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

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

Proof: We compute as follows:

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

where $y_i = (x_1, \dots, x_{i-1}, x_{i+2}, \dots, x_{t+1})$. The last statement follows from the fact that

$$\sum_{z \in \mathbb{F}_2^r} (-1)^{\langle w, z \rangle} = 2^r \delta(w).$$

This completes the proof. \square

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

Lemma 1: Let g' be defined as in (6). 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 $M = m - m_1 - m_{t+1}$, $w = w_t = (w_{t,1}, \dots, w_{t,t+1})$ with $w_{t,i} \in \mathbb{F}_2^{m_i}$, $u = (w_{1,2}, \dots, w_{t-1,t})$, and for $1 \leq i \leq t$, $w_{i-1,i} \in \mathbb{F}_2^{m_i}$ with $w_{0,1} = (0, \dots, 0)$.

Proof: Using (7), (8), and the Generalized Convolution Theorem, we have

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

where $w_i \in \mathbb{F}_2^m$ for $0 \leq i \leq t-1$ and $w_0 = (0, \dots, 0)$. For $0 \leq i \leq t$, write $w_i = (w_{i,1}, \dots, w_{i,t+1})$ with $w_{i,j} \in \mathbb{F}_2^{m_j}$. Set $\alpha_{i,j} = w_{i,j} \oplus w_{i-1,j}$ and $\alpha_i = (\alpha_{i,1}, \dots, \alpha_{i,t+1}) = w_i \oplus w_{i-1}$.

Set $\beta_i^t = (\alpha_{i,1}, \dots, \alpha_{i,i-1}, \alpha_{i,i+2}, \dots, \alpha_{i,t+1})$. Using Proposition 2, we obtain

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

The proof now follows from the following claim.

Claim: For $t \geq 2$, we have

$$\begin{aligned} & \sum_{(w_1, \dots, w_{t-1})} \prod_{i=1}^t W_{(l_{v_i} \circ g_i)}(\alpha_{i,i}, \alpha_{i,i+1}) \delta(\beta_i^t) \\ &= \sum_{(w_1, 2, \dots, w_{t-1}, t)} \prod_{i=1}^t W_{(l_{v_i} \circ g_i)}(w_{t,i} \oplus w_{i-1,i}, w_{i,i+1}). \quad (9) \end{aligned}$$

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 (9).

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 preceding expression as

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

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

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

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 $w_{1,t+1} = \dots = w_{t-2,t+1} = (0, \dots, 0)$. Also, the expression within the second sum evaluates to 1 only under the condition $w_{t,i} = w_{t-1,i}$ for $1 \leq i \leq t - 1$. We invoke the induction hypothesis on the first sum to obtain

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

This completes the proof of the claim and the lemma. \square

Finally, using Proposition 1 and Lemma 1 we obtain the Walsh transform of W_h .

Theorem 4: Let h be defined as in (5). Then

$$\begin{aligned} W_h(w) &= \frac{2^{m_1+m_{t+1}}}{2^{n+m}} \sum_{v \in \mathbb{F}_2^n} W_f(v) \\ &\quad \times \sum_{u \in \mathbb{F}_2^M} \prod_{i=1}^t W_{(l_{v_i} \circ g_i)}(w_{t,i} \oplus w_{i-1,i}, w_{i,i+1}) \quad (10) \end{aligned}$$

where $v = (v_1, \dots, v_t)$ with $v_i \in \mathbb{F}_2^{n_i}$, $M = m - m_1 - m_{t+1}$, $w = w_t = (w_{t,1}, \dots, w_{t,t+1})$ with $w_{t,i} \in \mathbb{F}_2^{m_i}$, $u = (w_{1,2}, \dots, w_{t-1,t})$ and for $1 \leq i \leq t$, $w_{i-1,i} \in \mathbb{F}_2^{m_i}$ with $w_{0,1} = (0, \dots, 0)$.

V. 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 4. First, we rewrite Theorem 4 for $t = 2$.

Theorem 5: Let h be defined as in (5) and $t = 2$. Then

$$\begin{aligned} & W_h(w_{2,1}, w_{2,2}, w_{2,3}) \\ &= \frac{2^{m_1+m_3}}{2^{m+n}} \sum_{v \in \mathbb{F}_2^n} W_f(v) \\ &\quad \times \sum_{w_{1,2} \in \mathbb{F}_2^{m_2}} W_{(l_{v_1} \circ g_1)}(w_{2,1}, w_{1,2}) \\ &\quad \times W_{(l_{v_2} \circ g_2)}(w_{2,2} \oplus w_{1,2}, w_{2,3}) \quad (11) \end{aligned}$$

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

$$f(a_1, \dots, a_n) = a_1 \oplus \dots \oplus a_n.$$

In this case, $W_f(1, \dots, 1) = 2^n$ and $W_f(v) = 0$ for $v \in \mathbb{F}_2^n \setminus \{(1, \dots, 1)\}$. Also $v_1 = (1, \dots, 1) \in \mathbb{F}_2^{n_1}$ and $v_2 = (1, \dots, 1) \in \mathbb{F}_2^{n_2}$. 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 5.

Corollary 1: 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

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

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 1 we obtain the following result of Nyberg [8] (stated in terms of Walsh transform).

Theorem 6 (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

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

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

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

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, $W_{(l_{v_1} \circ g_1)}(w_{2,1}) = 2^{m_1} \delta(v_1 \oplus w_{2,1}) = 2^{n_1} \delta(v_1 \oplus w_{2,1})$, since $m_1 = n_1$. Thus, $W_{(l_{v_1} \circ g_1)}(w_{2,1}) = 2^{n_1}$ if $v_1 = w_{2,1}$ and is equal to 0 otherwise. Let the right-hand side of (11) be \mathcal{A} . In this case, \mathcal{A} becomes

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

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

Theorem 7 (Nyberg [8, Theorem 3]): Let

$$h(x_1, x_3) = f(x_1, g(x_3)).$$

Then

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

VI. APPLICATIONS

In this section, we consider two other applications of Theorem 4. These are based on operations which typically occur in design of symmetric ciphers, namely S-box lookup, addition modulo 2^{2k} , and the X-OR operation. We consider two possible ways of combining these operations and obtain the Walsh transform in each case.

A. Brick Layering

In this subsection, we consider a map of the form

$$h(x, y, z) = g(g(x, y) \oplus g(y, z)). \quad (12)$$

Fig. 1 gives a diagrammatic view of the map. The term brick layering was used in [1] to denote a map which consists of several parallel applications of different S-boxes on disjoint subsets of the inputs which also form a partition of the input. In our case the X-OR and the second application of g is used to “glue” the outputs of the first two applications of g . In block cipher applications, g is usually a $2k$ -bit to $2k$ -bit S-box possibly the inverse function over $\text{GF}(2^{2k})$. Hence,

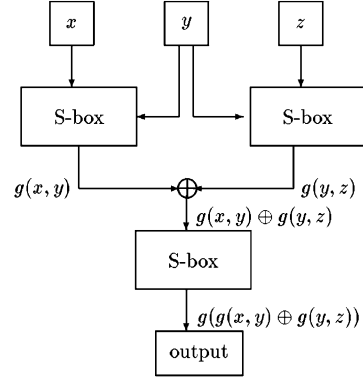


Fig. 1. Brick layering transformation.

we assume that g is an $2k$ -bit to $2k$ -bit map and x, y , and z are all k -bit strings. Let g_1, \dots, g_{2k} be the component functions of g . Let $\nu_i(x, y, z) = g_i(x, y) \oplus g_i(y, z)$ and $\nu = (\nu_1, \dots, \nu_{2k})$. Applying Corollary 1 with $n_1 = n_2 = 1$ we obtain

$$W_{\nu_i}(\delta_1, \delta_2, \delta_3) = \frac{1}{2^k} \sum_{u \in \mathbb{F}_2^k} W_{g_i}(u \oplus \delta_2, \delta_3) W_{g_i}(u, \delta_1). \quad (13)$$

Let h_1, \dots, h_{2k} be the component functions of h . We have

$$h_i(x, y, z) = g_i(\nu_1(x, y, z), \dots, \nu_{2k}(x, y, z)).$$

Now applying the Composition Theorem, for $(\gamma_1, \gamma_2, \gamma_3) \in \{0, 1\}^{3k}$, we get

$$W_{h_i}(\gamma_1, \gamma_2, \gamma_3) = \frac{1}{2^{2k}} \sum_{v \in \mathbb{F}_2^{2k}} W_{g_i}(v) W_{(l_v \circ \nu)}(\gamma_1, \gamma_2, \gamma_3). \quad (14)$$

The next step is to compute the Walsh transform of $(l_v \circ \nu)$. Let v be of weight r (i.e., $\text{wt}(v) = r$) with the bits in the j_1, \dots, j_r th positions to be 1 and all others to be 0. Then

$$(l_v \circ \nu)(x, y, z) = \mu_1(x, y, z) \oplus \dots \oplus \mu_r(x, y, z)$$

where $\mu_i = \nu_{j_i}$ for $1 \leq i \leq r$. Further, let $s = 3k(\text{wt}(v) - 1)$, $w = (u_1, \dots, u_{r-1})$, with each $u_i \in \mathbb{F}_2^{3k}$, $u_0 = (0, \dots, 0) \in \mathbb{F}_2^{3k}$ and $u_r = (\gamma_1, \gamma_2, \gamma_3)$. Now applying the Generalized Convolution Theorem, we have

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

Substituting in (14) and using (13) we obtain the Walsh transform for any component function of the map defined in (12).

Theorem 8: Let h be an S-box defined as in (12) and let h_1, \dots, h_{2k} be its component functions. Then

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

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

Theorem 8 provides the complete expression for the Walsh transform of any h_i .

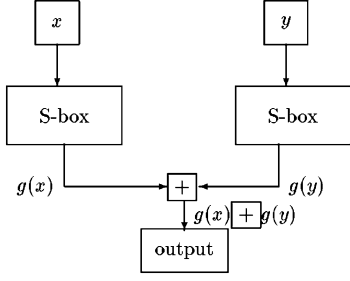


Fig. 2. Substitute and add.

B. Substitute-and-Add

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

$$h(x, y) = g(x) \boxplus g(y). \quad (15)$$

The map is shown diagrammatically in Fig. 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, \dots, g_{2k} .

For the sake of convenience, we will denote $\nu(x, y) = x \boxplus y$. The map ν is conveniently described by separating the carry part. Suppose (a_1, \dots, a_{2k}) and (b_1, \dots, b_{2k}) are the inputs to \boxplus . Then, the carry in the i th position is given by the function $c(a_1, \dots, a_i, b_1, \dots, b_i)$ 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, \dots, h_{2k} be the component functions of h . We can now write

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

Let

$$\begin{aligned} f_i(x, y) &= c_i(g_1(x), \dots, g_i(x), g_1(y), \dots, g_i(y)) \\ &= c_i(\mu_i(x, y)) \end{aligned}$$

where $\mu_i : \{0, 1\}^{4k} \rightarrow \{0, 1\}^{2i}$ is defined as

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

Applying the Composition Theorem for $(u, v) \in \{0, 1\}^{2k}$, we have

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

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

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

Thus we get the following result.

Theorem 9: Let h be defined as in (15) and h_1, \dots, h_{2k} be its component functions. Then

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

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

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.

VII. CONCLUSION

We have proved a result which provides the Walsh transform of a general functional form. As special cases, we obtain two of Nyberg's correlation theorems proved in [8]. We consider two applications of our results. These applications combine S-box lookup with addition modulo 2^{2k} and the X-OR operation. In each case, we obtain complete expressions for the Walsh transform. A possible future research problem is to apply our techniques to actual block ciphers.

ACKNOWLEDGMENT

The authors wish to thank Kaisa Nyberg, Johan Wallén, Willi Meier, and Vincent Rijmen for reading the correspondence and providing several suggestions.

REFERENCES

- [1] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard (Information Security and Cryptography)*. Berlin, Germany: Springer-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 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1995, pp. 24–38.
- [3] M. Hermelin and K. Nyberg, "Correlation properties of the bluetooth combiner generator," in *Proc. 2nd Int. Conf. Information Security and Cryptology of ICISC'99 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, pp. 17–29.
- [4] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
- [5] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology—EUROCRYPT 1993 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1994, pp. 386–397.
- [6] W. Meier and O. Staffelbach, "Correlation properties of combiners with memory in stream cipher," *J. Cryptol.*, vol. 5, no. 1, pp. 67–86, 1992.
- [7] K. Nyberg, "Linear approximation of block ciphers," in *Advances in Cryptology—EUROCRYPT 1994 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1995, pp. 439–444.
- [8] —, "Correlation theorems in cryptanalysis," in *Discr. Appl. Math.*, 2001, vol. 111, pp. 177–188.
- [9] P. Sarkar and S. Maitra, "Cross-correlation analysis of cryptographically useful Boolean functions and S-boxes," in *Theory Comput. Syst.*, 2002, vol. 35, pp. 39–57.
- [10] O. Staffelbach and W. Meier, "Cryptographic significance of the carry for ciphers based on integer addition," in *Advances in Cryptology—CRYPTO 1990 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1991, pp. 601–615.
- [11] J. Wallén, "Linear approximation of addition modulo 2^n ," presented at the 10th Annu. Workshop on Fast Software Encryption, AF-Borgen, Lund, Sweden, Feb. 24–26, 2003, pp. 277–290. Pre-proceedings.