# Correlation Matrices

Joan Daemen, René Govaerts and Joos Vandewalle

Katholieke Universiteit Leuven
ESAT-COSIC
K. Mercierlaan 94, B-3001 Heverlee, Belgium

joan.daemen@esat.kuleuven.ac.be

**Abstract.** In this paper we introduce the *correlation matrix* of a Boolean mapping, a useful concept in demonstrating and proving properties of Boolean functions and mappings. It is argued that correlation matrices are the "natural" representation for the proper understanding and description of the mechanisms of linear cryptanalysis [4]. It is also shown that the difference propagation probabilities and the table consisting of the squared elements of the correlation matrix are linked by a scaled Walsh-Hadamard transform.

**Key Words:** Boolean Mappings, Linear Cryptanalysis, Correlation Matrices.

## 1 Introduction

Most components in encryption schemes are Boolean mappings. In this paper, we establish a relation between Boolean mappings and specific linear mappings over real vector spaces. The matrices that describe these mappings are called *correlation matrices*. The elements of these matrices consist of the correlation coefficients associated with linear combinations of input bits and linear combinations of output bits.

Correlation matrices describe correlation properties of Boolean mappings in a direct way and are therefore the natural representation for the description and understanding of the mechanisms of linear cryptanalysis [4]. Moreover, they provide a useful tool for theoretical derivations and proofs.

After giving some preliminary definitions, we describe the Walsh-Hadamard transform of Boolean functions. Subsequently, we introduce the concept of correlation matrices and show how to calculate elements of this matrix for some particular types of mappings. This is followed by a treatment of the correlation properties of iterated transformations. We conclude with deriving the relations between the table of difference propagation probabilities of a mapping and its correlation matrix. For a more thorough treatment of difference propagation and additional properties of correlation matrices we refer to [6].

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 275–285, 1995.
©1995 Springer-Verlag

## 2 Preliminaries

A binary *vector* consists of an array of binary-valued components, that are indexed starting from 0. A binary vector $a$ with *dimension* (or equivalently *length*) $n$ has components $a_0, a_1, \ldots, a_{n-1}$. The set of all binary vectors with dimension $n$ is denoted by $\mathbb{Z}_2^n$.

A Boolean function $f(a)$ is a two-valued function with domain $\mathbb{Z}_2^n$ for some $n$. A Boolean mapping $h(a)$ maps $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^m$ for some $n, m$ and can be seen as the parallel application of $m$ Boolean functions: $(h_1(a), h_2(a), \ldots, h_{m-1}(a))$. If $m = n$, the Boolean mapping is called a transformation of $\mathbb{Z}_2^m$. This transformation is called *invertible* if it is a bijection.

The addition modulo 2 of two binary variables $\alpha$ and $\beta$ is denoted by $\alpha + \beta$. Hence $\alpha + \beta$ is 0 if $\alpha = \beta$ and 1 otherwise. The bitwise addition, sum or difference of two binary vectors $a$ and $b$ is denoted by $a + b$ and consists of a vector $c$ with components $c_i = a_i + b_i$. If the plus sign is used to denote arithmetic addition, it will be clear form the context. A Boolean mapping $h$ is *linear* (with respect to bitwise addition) if $h(a + b) = h(a) + h(b)$ for all $a, b \in \mathbb{Z}_2^n$.

## 3 The Walsh-Hadamard transform

Linear cryptanalysis can be seen as the exploitation of *correlations* between linear combinations of bits of different intermediate encryption values in a block cipher calculation. The correlation between two Boolean function can be expressed by a *correlation coefficient* that ranges between $-1$ and 1:

**Definition 1.** *The correlation coefficient associated with a pair of Boolean functions $f(a)$ and $g(a)$ is denoted by $\mathrm{C}(f, g)$ and given by*

$$\mathrm{C}(f, g) = 2 \cdot \mathrm{prob}(f(a) = g(a)) - 1 \ .$$

From this definition it follows that $\mathrm{C}(f, g) = \mathrm{C}(g, f)$. If the correlation coefficient is different from zero the functions are said to be *correlated*.

A selection vector $w$ is a binary vector that *selects* all components $i$ of a vector that have $w_i = 1$. Analogous to the inner product of vectors in linear algebra, the linear combination of the components of a vector $a$ selected by $w$ can be expressed as $w^{\mathrm{t}}a$ where the t suffix denotes transposition of the vector $w$. A linear Boolean function $w^{\mathrm{t}}a$ is completely specified by its corresponding selection vector $w$.

Let $\hat{f}(a)$ be a real-valued function that is $-1$ for $f(a) = 1$ and $+1$ for $f(a) = 0$. This can be expressed by $\hat{f}(a) = (-1)^{f(a)}$. In this notation the real-valued function corresponding to a linear Boolean function $w^{\mathrm{t}}a$ becomes $(-1)^{w^{\mathrm{t}}a}$. The bitwise sum of two Boolean functions corresponds to the bitwise product of their real-valued counterparts, i.e.,

$$\widehat{f(a) + g(a)} = \hat{f}(a)\hat{g}(a) \ . \tag{1}$$

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 275–285, 1995.
©1995 Springer-Verlag

We define an *inner product* for real-valued functions, not to be confused with the inner product of *vectors*, by

$$< \hat{f}(a), \hat{g}(a) >= \sum_a \hat{f}(a)\hat{g}(a) \ , \tag{2}$$

It can easily be shown that

$$\mathrm{C}(f(a), g(a)) = 2^{-n} < \hat{f}(a), \hat{g}(a) > \ . \tag{3}$$

The real-valued functions corresponding to the linear Boolean functions form an orthogonal basis with respect to the defined inner product:

$$< (-1)^{u^{\mathrm{t}}a}, (-1)^{v^{\mathrm{t}}a} >= 2^n \delta(u+v) \ , \tag{4}$$

with $\delta(w)$ the real-valued function that is equal to 1 if $w$ is the zero vector and 0 otherwise. The representation of a Boolean function with respect to this basis is called its Walsh-Hadamard transform [5, 1]. The link between the Walsh-Hadamard transform of a Boolean function and its correlation with linear Boolean functions was first established in [2]. If the correlation coefficients $\mathrm{C}(f(a), w^{\mathrm{t}}a)$ are denoted by $\hat{F}(w)$ we have

$$\hat{f}(a) = \sum_w \hat{F}(w)(-1)^{w^{\mathrm{t}}a} \tag{5}$$

and dually

$$\hat{F}(w) = 2^{-n} \sum_a \hat{f}(a)(-1)^{w^{\mathrm{t}}a} \ , \tag{6}$$

summarized by

$$\hat{F}(w) = \mathcal{W}(f(a)) \ . \tag{7}$$

Hence a Boolean function is completely specified by the set of correlation coefficients with all linear functions.

The Walsh-Hadamard transform of the sum of two Boolean functions $f(a) + g(a)$ can be derived using (5). If $h = f + g$, we have

$$\hat{H}(w) = \sum_v \hat{F}(v+w)\hat{G}(v) \ . \tag{8}$$

Hence, addition modulo 2 in the Boolean domain corresponds to convolution in the transform domain. If the convolution operation is denoted by $\otimes$ this is expressed by

$$\mathcal{W}(f+g) = \mathcal{W}(f) \otimes \mathcal{W}(g) \ . \tag{9}$$

The subspace of $\mathbb{Z}_2^n$ generated by the vectors $w$ such that $\hat{F}(w) \neq 0$ is called its *support space* $\mathcal{V}_f$. The support space of the sum of two Boolean functions is a subspace of the (vector) sum of their corresponding support spaces: $\mathcal{V}_{f+g} \subseteq \mathcal{V}_f + \mathcal{V}_g$. This follows directly from the convolution property. Two Boolean functions are called *disjunct* if their support spaces are disjunct, i.e., if the intersection of

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 275–285, 1995.
©1995 Springer-Verlag

their support spaces only contains the origin. A vector $v \in \mathcal{V}_{f+g}$ with $f$ and $g$ disjunct, can be decomposed in only one way into a component $u \in \mathcal{V}_f$ and a component $w \in \mathcal{V}_g$. In this case the transform values of $h = f + g$ are given by

$$\hat{H}(v) = \hat{F}(u)\hat{G}(w) \text{ with } v = u + w \text{ and } u \in \mathcal{V}_f, w \in \mathcal{V}_g \ . \tag{10}$$

Pairs of Boolean functions that depend on non-overlapping sets of input bits are a special case of disjunct functions.

## 4 Correlation matrices

A mapping $h : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2^m$ can be decomposed into $m$ *component* Boolean functions: $(h_0, h_1, \ldots, h_{m-1})$. Each of these component functions $h_i$ has a Walsh-Hadamard transform $\hat{H}_i$. The vector function with components $\hat{H}_i$ is denoted by $\hat{H}$ and can be considered the Walsh-Hadamard transform of the mapping $h$. As in the case of Boolean functions, $\hat{H}$ completely determines the Boolean transformation $h$. The Walsh-Hadamard transform of any linear combination of components of $h$ is specified by a simple extension of (9):

$$\mathcal{W}(\mathrm{u}^{\mathrm{t}}h) = \bigotimes_{\mathrm{u}_i=1} \hat{H}_i \ . \tag{11}$$

All correlation coefficients between linear combinations of input bits and that of output bits of the mapping $h$ can be arranged in a $2^m \times 2^n$ *correlation matrix* $C^h$. The element $C_{uw}$ in row $u$ and column $w$ is equal to $\mathrm{C}(u^{\mathrm{t}}h(a), w^{\mathrm{t}}a)$. The rows of this matrix can be interpreted as

$$(-1)^{u^{\mathrm{t}}h(a)} = \sum_w C^h_{uw}(-1)^{w^{\mathrm{t}}a} \ . \tag{12}$$

A matrix $C^h$ defines a linear mapping with domain $\mathbb{R}^{2^n}$ and range $\mathbb{R}^{2^m}$. Let $\mathcal{R}$ be a mapping from the space of binary vectors to the space of real vectors, where a binary vector of dimension $n$ is depicted onto a real vector with dimension $2^n$. $\mathcal{R}$ is defined by

$$\mathcal{R} : \mathbb{Z}_2^n \mapsto \mathbb{R}^{2^n} : \alpha = \mathcal{R}(a) : \alpha_u = (-1)^{u^{\mathrm{t}}a} \ . \tag{13}$$

Since $\mathcal{R}(a+b) = \mathcal{R}(a)\mathcal{R}(b)$, $\mathcal{R}$ is a group-homomorphism from $< \mathbb{Z}_2^n, + >$ to $< \mathbb{R}^{2^n}, \cdot >$, with $\cdot$ denoting the componentwise product. From (12) it can easily be seen that

$$C^h\mathcal{R}(a) = \mathcal{R}(h(a)) \ . \tag{14}$$

Consider the composition of two Boolean mappings $h = h_2 \circ h_1$ or $h(a) = h_2(h_1(a))$, with $h_1$ mapping $n$-dimensional vectors to $p$-dimensional vectors and with $h_2$ mapping $p$-dimensional vectors to $m$-dimensional vectors. The correlation matrix of $h$ is determined by the correlation matrices of the component

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 275–285, 1995.
©1995 Springer-Verlag

mappings. We have

$$\begin{aligned}(-1)^{u^{\mathrm{t}}h(a)} &= \sum_v C_{uv}^{h_2}(-1)^{v^{\mathrm{t}}h_1(a)} \\ &= \sum_v C_{uv}^{h_2} \sum_w C_{vw}^{h_1}(-1)^{w^{\mathrm{t}}a} \\ &= \sum_w (\sum_v C_{uv}^{h_2} C_{vw}^{h_1})(-1)^{w^{\mathrm{t}}a} \ .\end{aligned}$$

Hence,

$$C^{h_2 \circ h_1} = C^{h_2} \times C^{h_1} \ , \tag{15}$$

with $\times$ denoting the matrix product. The input-output correlations of $h = h_2 \circ h_1$ are given by

$$\mathrm{C}(u^{\mathrm{t}}h(a), w^{\mathrm{t}}a) = \sum_v \mathrm{C}(u^{\mathrm{t}}h_1(a), v^{\mathrm{t}}a)\mathrm{C}(v^{\mathrm{t}}h_2(a), w^{\mathrm{t}}a) \ . \tag{16}$$

If $h$ is an invertible transformation in $\mathbb{Z}_2^n$, we have (with $b = h^{-1}(a)$)

$$\mathrm{C}(u^{\mathrm{t}}h^{-1}(a), w^{\mathrm{t}}a) = \mathrm{C}(u^{\mathrm{t}}b, w^{\mathrm{t}}h(b)) = \mathrm{C}(w^{\mathrm{t}}h(b), u^{\mathrm{t}}b) \ . \tag{17}$$

Using this fact and $C^h \times C^{(h^{-1})} = C^{h \circ h^{-1}} = I = C^h \times (C^h)^{-1}$ we obtain

$$(C^h)^{-1} = C^{(h^{-1})} = (C^h)^{\mathrm{t}} \ , \tag{18}$$

hence, $C^h$ is an orthogonal matrix.

This can be used to give an elegant proof of the following proposition:

**Proposition 1.** *Every linear combination of output bits of an invertible transformation is a balanced Boolean function of its input bits.*

**Proof :** If $h$ is an invertible transformation, its correlation matrix $C$ is orthogonal. Since $C_{00} = 1$ and all rows and columns have norm 1, it follows that there are no other elements in row 0 or column 0 different from 0. Hence, $\mathrm{C}(u^{\mathrm{t}}h(a), 0) = \delta(u)$ or equivalently, $u^{\mathrm{t}}h(a)$ is balanced for all $u \neq 0$. □

A mapping from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^m$ is converted into a mapping from $\mathbb{Z}_2^{n-1}$ to $\mathbb{Z}_2^m$ by fixing a single component of the input. More generally, a component of the input can be set equal to a linear combination of other input components, possibly complemented. Such a restriction is of the type

$$v^{\mathrm{t}}a = \epsilon \ , \tag{19}$$

with $\epsilon \in \mathbb{Z}_2$. Assume that $v_s \neq 0$. The restriction can be seen as the result of a mapping $a' = h_r(a)$ from $\mathbb{Z}_2^{n-1}$ to $\mathbb{Z}_2^n$ specified by $a'_i = a_i$ for $i \neq s$ and $a'_s = \epsilon + v^{\mathrm{t}}a + a_s$. The nonzero elements of the correlation matrix of $h_r$ are

$$C_{ww}^{h_r} = 1 \text{ and } C_{(v+w)w}^{h_r} = (-1)^{\epsilon} \text{ for all } w \text{ with } w_s = 0 \ . \tag{20}$$

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 275–285, 1995.
©1995 Springer-Verlag

It can be seen that columns indexed by $w$ with $w_s = 0$ have exactly two nonzero entries with magnitude 1 and those with $w_s = 1$ are all-zero. Omitting the latter gives a $2^n \times 2^{n-1}$ correlation matrix $C^{h_r}$ with only columns indexed by the vectors with $w_s = 0$.

The transformation restricted to the specified subset of inputs can be seen as the consecutive application of $h_r$ and the transformation itself. Hence, its correlation matrix $C'$ is given by $C \times C^{h_r}$. The elements of this matrix are

$$C'_{uw} = C_{uw} + (-1)^{\epsilon} C_{u(w+v)} \ , \tag{21}$$

if $w_s = 0$ and 0 if $w_s = 1$.

## 5 Specific types of mappings

Consider the transformation that consists of the bitwise addition of a constant vector $k$: $h(a) = a + k$. Since $u^{\mathrm{t}} h(a) = u^{\mathrm{t}} a + u^{\mathrm{t}} k$ the correlation matrix is a diagonal matrix with

$$C_{uu} = (-1)^{u^{\mathrm{t}} k} \ . \tag{22}$$

Therefore the effect of bitwise addition of a constant vector before (or after) a mapping $h$ on its correlation matrix is a multiplication of some columns (or rows) by $-1$.

Consider a linear transformation $h(a) = Ma$ with $M$ a $m \times n$ binary matrix. Since $u^{\mathrm{t}} h(a) = u^{\mathrm{t}} M a = (M^{\mathrm{t}} u)^{\mathrm{t}} a$ the elements of the corresponding correlation matrix are given by

$$C_{uw} = \delta(M^{\mathrm{t}} u + w) \ . \tag{23}$$

If $M$ is an invertible square matrix, the correlation matrix is a permutation matrix. The single nonzero element in row $u$ is in column $M^{\mathrm{t}} u$. The effect of applying an invertible linear transformation before (or after) a transformation $h$ on the correlation matrix is only a permutation of its columns (or rows).

Consider a mapping from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^m$ that consists of the parallel application of $\ell$ component mappings (S-boxes) from $\mathbb{Z}_2^{n_i}$ to $\mathbb{Z}_2^{m_i}$ with $\sum_i n_i = n$ and $\sum_i m_i = m$. We will call such a mapping a *boxed* mapping. We have $a = (a_{(0)}, a_{(1)}, \ldots, a_{(\ell-1)})$ and $b = (b_{(0)}, b_{(1)}, \ldots, b_{(\ell-1)})$ with the $a_{(i)}$ vectors of dimension $n_i$ and the $b_{(i)}$ vectors with dimension $m_i$. The mapping $b = h(a)$ is defined by $b_{(i)} = h_{(i)}(a_{(i)})$ for $0 \leq i < \ell$. With every S-box $h_{(i)}$ is associated a $2^{n_i} \times 2^{m_i}$ correlation matrix denoted by $C^{(i)}$. Since the $h_{(i)}$ are disjunct, (10) can be applied and the elements of the correlation matrix of $h$ are given by

$$C_{uw} = \prod_i C^{(i)}_{u_{(i)} w_{(i)}} \ . \tag{24}$$

with $u = (u_{(0)}, u_{(1)}, \ldots, u_{(\ell-1)})$ and $w = (w_{(0)}, w_{(1)}, \ldots, w_{(\ell-1)})$. In words this can be expressed as: the correlation coefficient associated with input selection $w$ and output selection $u$ is the product of its corresponding S-box input-output correlations $C^{(i)}_{u_{(i)} w_{(i)}}$.

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 275–285, 1995.
©1995 Springer-Verlag

## 6 Application to iterated transformations

Correlation matrices can be easily applied to express correlations in iterated transformations such as most block ciphers. The studied transformation is

$$\beta = \rho_q \circ \ldots \circ \rho_2 \circ \rho_1 \ , \tag{25}$$

with the $\rho_i$ selected from a set of invertible transformations $\{\rho[b]|b \in \mathbb{Z}_2^{n_\mathrm{b}}\}$ by round keys $\kappa^{(i)}$: $\rho_i = \rho[\kappa^{(i)}]$ The round keys $\kappa^{(i)}$ are derived from the cipher key $\kappa$ by the key schedule.

### 6.1 Fixed key

In the transform domain, a fixed succession of round transformations corresponds to a $2^n \times 2^n$ correlation matrix that is the product of the correlation matrices corresponding to the round transformations. We have

$$C = C^{\rho_q} \times \ldots \times C^{\rho_2} \times C^{\rho_1} \ . \tag{26}$$

Linear cryptanalysis exploits the occurrence of large elements in product matrices corresponding to all but a few rounds of a block cipher.

A $q$-round *linear trail* $\Omega$, denoted by

$$\Omega = (\omega_0 \triangleleft \rho_1 \triangleright \omega_1 \triangleleft \rho_2 \triangleright \omega_2 \triangleleft \ldots \triangleright \omega_{q-1} \triangleleft \rho_1 \triangleright \omega_q) \ , \tag{27}$$

is obtained by chaining $q$ single-round correlations $\mathrm{C}({\omega_i}^\mathrm{t}\rho_i(a), {\omega_{i-1}}^\mathrm{t}a)$. With this linear trail is associated a *correlation contribution coefficient* $\mathrm{C_p}$ ranging between $-1$ and $+1$.

$$\mathrm{C_p}(\Omega) = \prod_i C^{\rho_i}_{\omega_i \omega_{i-1}} \ . \tag{28}$$

From this definition and (26) we have

$$\mathrm{C}(u^\mathrm{t}\beta(a), w^\mathrm{t}a) = \sum_{\omega_0 = w, \omega_q = u} \mathrm{C_p}(\Omega) \tag{29}$$

Hence the correlation between $u^\mathrm{t}\beta(a)$ and $w^\mathrm{t}a$ is the sum of the correlation contribution coefficients of all $q$-round linear trails $\Omega$ with initial selection vector $w$ and terminal selection vector $u$.

### 6.2 Variable key

In cryptanalysis, the succession of round transformations is not known in advance but is governed by an unknown key or some input-dependent value. In general, the elements of the correlation matrix of $\rho_i$ depend on the specific value of the round key $\kappa^{(i)}$.

For some block ciphers the strong round-key dependence of the correlation and propagation properties of the round transformation have been cited as a

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 275–285, 1995.
©1995 Springer-Verlag

design criterion. The analysis of correlation or difference propagation would have to be repeated for every specific value of the cipher key, making linear and differential analysis infeasible. A typical problem with this approach is that the *quality* of the round transformation with respect to LC or DC strongly depends on the specific value of the round key. While the resistance against LC and DC may be very good on the average, specific classes of cipher keys can exhibit linear trails with excessive correlation contribution coefficients.

These complications can be avoided by designing the round transformation in such a way that the amplitudes of the elements of its correlation matrix are independent of the specific value of the round key. As was shown in Sect. 4, this is the case if the round transformation consists of a fixed transformation $\rho$ followed (or preceded) by the bitwise addition of the round key $\kappa^{(i)}$.

The correlation matrix $C^\rho$ is determined by the fixed transformation $\rho$. The correlation contribution coefficient of the linear trail $\Omega$ becomes

$$\mathrm{C_p}(\Omega) = \prod_i (-1)^{\omega_i^{\mathrm{t}} \kappa^{(i)}} C^\rho_{\omega_i \omega_{i-1}} = (-1)^{d_\Omega + \sum_i \omega_i^{\mathrm{t}} \kappa^{(i)}} |\mathrm{C_p}(\Omega)| \ . \tag{30}$$

with $d_\Omega$ equal to 1 if $\prod_i C^\rho_{\omega_i \omega_{i-1}}$ is negative and 0 otherwise. $|\mathrm{C_p}(\Omega)|$ is independent of the round keys, and hence only the sign of the correlation contribution coefficient depends on the round keys.

The correlation coefficient between $u^{\mathrm{t}}\beta(a)$ and $w^{\mathrm{t}}a$ can be expressed in terms of the correlation contribution coefficients of linear trails:

$$\mathrm{C}(u^{\mathrm{t}}\beta(a), w^{\mathrm{t}}a) = \sum_{\omega_0 = w, \omega_q = u} (-1)^{d_\Omega + \sum_i \omega_i^{\mathrm{t}} \kappa^{(i)}} |\mathrm{C_p}(\Omega)| \ . \tag{31}$$

The amplitude of this correlation coefficient is no longer independent of the round keys since the terms are added or subtracted depending on the value of the round keys.

### 6.3 Matsui's linear cryptanalysis of DES

The multiple-round linear expressions described in [4] correspond with what we call linear trails. The probability $p$ that such an expression holds corresponds with $\frac{1}{2}(1 + \mathrm{C_p}(\Omega))$, with $\mathrm{C_p}(\Omega)$ the correlation contribution coefficient of the corresponding linear trail. This implies that the considered correlation coefficient is assumed to be dominated by a single linear trail. This assumption is valid because of the large amplitude of the described correlation coefficients on the one hand and the structure of the DES round transformation on the other.

The correlation contribution coefficient of the linear trail is independent of the key and consists of the product of the correlation coefficients of its single-round components. In general, the elements of the correlation matrix of the DES round transformation are not independent of the round keys. In the linear trails described in [4] the independence is caused by the fact that the single-round correlations of the described linear trail only involve bits of a single S-box.

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 275–285, 1995.
©1995 Springer-Verlag

## 7 Difference propagation

Say we have two $n$-dimensional vectors $a$ and $a^*$ with bitwise difference $a+a^* = a'$. Let $b = h(a), b^* = h(a^*)$ and $b' = b + b^*$. Hence, the difference $a'$ propagates to the difference $b'$ through $h$. This is denoted by $(a' \dashv h \vdash b')$, In general $b'$ is not determined by $a'$ but depends on the value of $a$ (or $a^*$).

**Definition 2.** *The prop ratio* $\mathrm{R_p}$ *of a difference propagation* $(a' \dashv h \vdash b')$ *is given by*

$$\mathrm{R_p}(a' \dashv h \vdash b') = 2^{-n} \sum_a \delta(b' + h(a + a') + h(a)) \ . \tag{32}$$

The prop ratio ranges between 0 and 1 and must be an integer multiple of $2^{1-n}$. The difference propagation $(a' \dashv h \vdash b')$ restricts the values of $a$ to a fraction of all possible inputs. This fraction is given by $\mathrm{R_p}(a' \dashv h \vdash b')$. It can easily be seen that

$$\sum_{b'} \mathrm{R_p}(a' \dashv h \vdash b') = 1 \ . \tag{33}$$

Differential cryptanalysis [3] can be seen as the exploitation of large prop ratios.

The prop ratios of the difference propagations of Boolean functions and mappings can be expressed respectively in terms of their Walsh-Hadamard transform values and their correlation matrix elements. Analogous with (8), it can be shown that the components of the inverse transform of the componentwise product of two spectra $\hat{c}_{fg} = \mathcal{W}^{-1}(FG)$ are given by

$$\hat{c}_{fg}(b) = 2^{-n} \sum_a \hat{f}(a)\hat{g}(a+b) = 2^{-n} \sum_a (-1)^{f(a)+g(a+b)} \ . \tag{34}$$

$\hat{c}_{fg}(b)$ is not a Boolean function. It is generally referred to as the *cross correlation function* of $f$ and $g$. If $g = f$ it is called the autocorrelation function of $f$ and denoted by $\hat{r}_f$. The components of the spectrum of the autocorrelation function consist of the squares of the spectrum of $f$, i.e.,

$$\hat{F}(w)^2 = \mathcal{W}(\hat{r}_f(a)) \ . \tag{35}$$

This is generally referred to as the Wiener-Khintchine theorem [5].

The difference propagation in a Boolean function $f$ can be expressed easily in terms of the autocorrelation function. The prop ratio of difference propagation $(a' \dashv f \vdash 0)$ is given by

$$\begin{aligned} \mathrm{R_p}(a' \dashv f \vdash 0) &= 2^{-n} \sum_a \delta(f(a) + f(a+a')) \\ &= 2^{-n} \sum_a \frac{1}{2}(1 + \hat{f}(a)\hat{f}(a+a')) \\ &= \frac{1}{2}(1 + \hat{r}_f(a')) \\ &= \frac{1}{2}(1 + \sum_w (-1)^{w^{\mathrm{t}}a'} \hat{F}^2(w)) \ . \end{aligned} \tag{36}$$

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 275–285, 1995.
©1995 Springer-Verlag

The component of the autocorrelation function $\hat{r}_f(a')$ corresponds to the amount that $\mathrm{R_p}(a' \dashv f \vdash 0)$ deviates from 1/2.

For mappings from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^m$, let the autocorrelation function of $u^{\mathrm{t}}h(a)$ be denoted by $\hat{r}_u(a')$, i.e.,

$$\hat{r}_u(a') = 2^{-n} \sum_a (-1)^{u^{\mathrm{t}}h(a)+u^{\mathrm{t}}h(a+a')} \ . \tag{37}$$

The prop ratio of difference propagation $(a' \dashv h \vdash b')$ is given by

$$\begin{aligned}
\mathrm{R_p}(a' \dashv h \vdash b') &= 2^{-n} \sum_a \delta(h(a) + h(a+a') + b') \\
&= 2^{-n} \sum_a \prod_i \frac{1}{2}((-1)^{h_i(a)+h_i(a+a')+b'_i} + 1) \\
&= 2^{-n} \sum_a 2^{-m} \sum_u (-1)^{u^{\mathrm{t}}h(a)+u^{\mathrm{t}}h(a+a')+u^{\mathrm{t}}b'} \\
&= 2^{-m} \sum_u (-1)^{u^{\mathrm{t}}b'} 2^{-n} \sum_a (-1)^{u^{\mathrm{t}}h(a)+u^{\mathrm{t}}h(a+a')} \\
&= 2^{-m} \sum_u (-1)^{u^{\mathrm{t}}b'} \hat{r}_u(a') \\
&= 2^{-m} \sum_u (-1)^{u^{\mathrm{t}}b'} \sum_w (-1)^{w^{\mathrm{t}}a'} C_{uw}^2 \\
&= 2^{-m} \sum_{u,w} (-1)^{w^{\mathrm{t}}a'+u^{\mathrm{t}}b'} C_{uw}^2 \ .
\end{aligned} \tag{38}$$

Hence the array containing the prop ratios is the (scaled) two-dimensional Walsh-Hadamard transform of the array that contains the squares of the elements of the correlation matrix. Inverting the transform gives the dual expression:

$$C_{uw}^2 = 2^{-n} \sum_{a',b'} (-1)^{w^{\mathrm{t}}a'+u^{\mathrm{t}}b'} \mathrm{R_p}(a' \dashv h \vdash b') \ . \tag{39}$$

## 8 Conclusions

The correlation matrix of a Boolean mapping is an alternative representation that reveals properties of a more global nature. Correlation matrices are the "natural" representation for the description and understanding of linear cryptanalysis.

## References

1. S. W. Golomb, *Shift Register Sequences*, Holden–Day Inc., San Francisco, 1967.
2. G.Z. Xiao, J.L. Massey, A Spectral Characterization of Correlation-Immune Functions, *IEEE Trans. Inform. Theory*, Vol. 34, No. 3, 1988, pp. 569–571

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 275–285, 1995.
©1995 Springer-Verlag

3. E. Biham and A. Shamir, *Differential Cryptanalysis of of the Data Encryption Standard*, Springer-Verlag, 1993.
4. M. Matsui, Linear Cryptanalysis Method for DES Cipher, *Advances in Cryptology – Proceedings of Eurocrypt '93, LNCS 765*, T. Helleseth, Ed., Springer-Verlag 1993, pp. 386–397.
5. B. Preneel, *Analysis and Design of Cryptographic Hash Functions*, Doct. Dissertation KULeuven, 1993.
6. J. Daemen, *Cipher and Hash Function Design. Strategies Based on Linear and Differential Cryptanalysis*, Doct. Dissertation KULeuven, March 1995.

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 275–285, 1995.
©1995 Springer-Verlag