4 Approximation by Linear Structures

The second main approach to hidden linearity is via linear structures. These are detected by difference calculus.

4.1 Linear structures of a Boolean map

Definition 1 Let $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ be a Boolean map, and $u \in \mathbb{F}_2^n$. Then the **difference map** is defined by $\Delta_u f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ is

$$\Delta_u f(x) := f(x+u) - f(x) \qquad \text{for all } x \in \mathbb{F}_2^n.$$

Lemma 1 *Let $f, g \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ and $u \in \mathbb{F}_2^n$. Then:*

(i) $\Delta_u(f+g) = \Delta_u f + \Delta_u g$,

(ii) $\operatorname{Deg} \Delta_u f \leq \operatorname{Deg} f - 1$.

Proof. (i) is trivial.

(ii) Assume without loss of generality: $q = 1$, $f = T^I$ is a monomial, and finally $f = T_1 \cdots T_r$. Then

$$\Delta_u f(x) = (x_1 + u_1) \cdots (x_r + u_r) - x_1 \cdots x_r$$

obviously hs degree $\leq r - 1$. $\diamond$

Corollary 1 *If f is constant, then $\Delta_u f = 0$ for all $u \in \mathbb{F}_2^n$.*

Corollary 2 *If f is affine, then $\Delta_u f$ constant for all $u \in \mathbb{F}_2^n$.*

Definition 2 (Evertse, Eurocrypt 87) A vector $u \in \mathbb{F}_2^n$ is called **linear structure** of $f \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$, if $\Delta_u f$ is constant.

Remarks

1. $\Delta_{u+v} f(x) = f(x+u+v) - f(x) = f(x+u+v) - f(x+v) + f(x+v) - f(x) = \Delta_u f(x+v) + \Delta_v f(x)$.
2. If f is affine, then every vector is a linear structure of f.
3. 0 always is a linear structure of f.
4. If u and v are linear structures, then so is $u + v$ by remark 1. Therefore the linear structures of f form a vector subspace of $\mathbb{F}_2^n$. On this subspace f is affine. We conclude that the converse of remark 2 is also true.

5. If $g : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^r$ is linear, then $\Delta_u(g \circ f) = g \circ \Delta_u f$.

Definition 3 For a Boolean map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ the vector space of its linear structures is called the **radical** Rad_f, its dimension, **linearity dimension** of f, and its codimension, **rank** of f, $\mathrm{Rank}\, f$.

4.2 The differential profile

For a Boolean map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ and $u \in \mathbb{F}_2^n$, $v \in \mathbb{F}_2^q$ let

$$\begin{aligned} D_f(u,v) &:= \{x \in \mathbb{F}_2^n \mid \Delta_u f(x) = v\}, \\ \delta_f(u,v) &:= \frac{1}{2^n} \# D_f(u,v). \end{aligned}$$

Definition 4 (Chabaud/Vaudenay, Eurocrypt 94) The function

$$\delta_f : \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{R}$$

is called the **differential profile** of f.

(The normalization with the coefficient $\frac{1}{2^n}$ is useful. In the literature the matrix $\# D_f(u,v)$ is called difference table.)

Remarks

1. If f is affine, $f(x) = Ax + b$, then $\Delta_u f(x) = Au$, hence

$$\begin{aligned} D_f(u,v) &= \{x \in \mathbb{F}_2^n | Au = v\} = \begin{cases} \mathbb{F}_2^n, & \text{if } Au = v, \\ \emptyset & \text{else,} \end{cases} \\ \delta_f(u,v) &= \begin{cases} 1, & \text{if } Au = v, \\ 0 & \text{else.} \end{cases} \end{aligned}$$

   Each row of the differential profile contains exactly one 1, and 0 else.

2. The following statements are equivalent:

$$\begin{aligned} u \text{ is a linear structure of } f &\iff D_f(u,v) = \begin{cases} \mathbb{F}_2^n & \text{for one } v, \\ \emptyset & \text{else} \end{cases} \\ &\iff \delta_f(u,v) = \begin{cases} 1 & \text{for one } v, \\ 0 & \text{else.} \end{cases} \end{aligned}$$

   The "row u" of the differential profile is 0 except exactly one entry 1.

3. For arbitrary f, and $u = 0$, we have

$$\delta_f(0,v) = \begin{cases} 1, & \text{if } v = 0, \\ 0 & \text{else} \end{cases}$$

   (row 0 of the differential profile).

4. $\sum_{v\in\mathbb{F}_2^q}\delta_f(u,v) = 1$ (row sums of the differential profile). In particular for each vector $u \in \mathbb{F}_2^n$ there is a $v \in \mathbb{F}_2^q$ such that $\delta_f(u,v) \geq \frac{1}{2^q}$.

We have shown:

Proposition 1 *For a Boolean map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ the following statements are equivalent:*

(i) *f is affine.*

(ii) *Each vector $u \in \mathbb{F}_2^n$ is linear structure of f.*

(iii) *Each row of the differential profile contains exactly one entry $\neq 0$.*

Remarks

5. $x \in D_f(u,v) \Leftrightarrow x + u \in D_f(u,v)$.

6. All values $\#D_f(u,v)$ are even: For $u = 0$ this follows from remark 3, else from remark 5. Therefore all $\delta_f(u,v)$ are integer multiples of $\frac{1}{2^{n-1}}$.

7. In the case $q = 1$ the autocorrelation, by its definition, can be expressed as
$$\kappa_f(x) = \delta_f(x,0) - \delta_f(x,1).$$

Exercise 1 How does the differential profile behave under affine transformations of the argument or image space?

Exercise 2 Show that for bijective f always $\delta_{f^{-1}}(v,u) = \delta_f(u,v)$.

4.3 Efficient calculation of the differential profile

The following lemma is the basis for the efficient calculation of differential profiles:

Lemma 2 *For every Boolean map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$*
$$\delta_f = \frac{1}{2^n}\vartheta_f * \vartheta_f.$$

Proof.
$$\begin{aligned}
\vartheta_f * \vartheta_f(u,v) &= \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q}\vartheta_f(x,y)\vartheta_f(x+u,y+v)\\
&= \sum_{x\in\mathbb{F}_2^n}\vartheta_f(x+u,f(x)+v)\\
&= \#\{x \in \mathbb{F}_2^n \mid f(x+u) = f(x)+v\}.\diamond
\end{aligned}$$

The convolution theorem yields

$$\hat{\delta}_f = \frac{1}{2^n}\hat{\vartheta}_f^2 = 2^n \lambda_f,$$

and we have shown:

Theorem 1 *The differential profile is, up to a constant factor, the Walsh transform of the linear profile:*

$$\lambda_f = \frac{1}{2^n}\hat{\delta}_f, \qquad \delta_f = \frac{1}{2^q}\hat{\lambda}_f.$$

Parseval's equation immediately gives:

Corollary 1 *For every Boolean map* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$

$$2^n \cdot \sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^q} \lambda_f(u,v)^2 = 2^q \cdot \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q} \delta_f(x,y)^2.$$

Corollary 2 *Two Boolean maps* $\mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *have the same linear profile, if and only if they have the same differential profile.*

Therefore we can efficiently calculate the differential profile of a map $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ by the following algorithm, that yields the linear profile as an intermediate result:

1. Calculate the spectrum $\hat{\vartheta}_f$.
2. Take the squares $\omega := \hat{\vartheta}_f^2$ and normalize $\lambda_f = \frac{1}{2^{2n}} \cdot \omega$.
3. Transform back to $\delta_f = \frac{1}{2^q}\hat{\lambda}_f = \frac{1}{2^{2n+q}}\hat{\omega}$.

The effort, after having calculated $\hat{\lambda}_f$, consists of additional $3N \cdot {}^2\log(N)$ "elementary operations". All in all this makes $6N \cdot {}^2\log(N)$ such operations plus N squarings, where $N = 2^{n+q}$ is the input size.

This entire procedure is in the sources as executable program `bma` ('Boolean Map Analysis').

Exercise Let $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ be a Boolean map. Show that

$$\sum_{u\in\mathbb{F}_2^n} \delta_f(u,v) = \frac{1}{2^n}\nu_f * \nu_f(v)$$

for all $v \in \mathbb{F}_2^q$. (Remember that ν_f is the preimage counter.)

Deduce that the following statements are equivalent (Zhang/Zheng, SAC '96):

(i) f is balanced.

(ii) $\sum_{u\in\mathbb{F}_2^n} \delta_f(u,v) = 2^{n-q}$ for all $v \in \mathbb{F}_2^q$ (all column sums of the differential profile).

(iii) $\sum_{u\in\mathbb{F}_2^n} \delta_f(u,0) = 2^{n-q}$ (first column sum of the differential profile).

4.4 The differential potential

Definition 5 (Nyberg, EUROCRYPT 93) For a Boolean map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ the quantity

$$\Omega_f := \max\{\delta_f(u,v) \mid u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^q, (u,v) \neq 0\}$$

is called **differential potential** of f.

Note: Nyberg denotes the maximum entry of the *difference table* (except at $(0,0)$) by "differential uniformity". Here I prefer a uniform treatment of the linear and the differential profiles and potentials.

Remarks

1. By remark 4 in 4.2 we have the bounds
$$\frac{1}{2^q} \leq \Omega_f \leq 1.$$

2. Ω_f takes the lower bound 2^{-q}, if and only if all $\delta_f(u,v) = 2^{-q}$ for $u \neq 0$, i. e., if all the difference maps $\Delta_u f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ are balanced. (The "row u" of the differential profile is constant.)

3. Since for $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ all values of the differential profile δ_f are multiples of $\frac{1}{2^{n-1}}$, the differential potential $\Omega_f \geq \frac{1}{2^{n-1}}$.

4. If f has a linear structure $\neq 0$, i. e., if $\mathrm{Rad}_f \neq 0$, then $\Omega_f = 1$.

Exercise 1 Show that Ω_f is invariant under affine transformations of $\mathbb{F}_2^n$ and $\mathbb{F}_2^q$.

Exercise 2 Show that if f is bijective, then $\Omega_{f^{-1}} = \Omega_f$.

Definition 6 (Nyberg, EUROCRYPT 93) A Boolean map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ is called **perfectly nonlinear**, if its differential potential has the (minimally possible) value $\Omega_f = 2^{-q}$.

Remarks

5. By remark 5 in 4.1 and proposition 3 in 3.2 this holds, if and only if $\beta \circ f$ is perfectly nonlinear for each linear form $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$, $\beta \neq 0$.

6. A perfectly nonlinear map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ cannot have any linear structure $u \neq 0$.

7. If a perfectly nonlinear map exists, then $q \leq n - 1$ by remark 3.

From remark 2 we conclude:

Proposition 2 $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *is perfectly nonlinear, if and only if the differential profile* δ_f *is constant* $= 2^{-q}$ *on* $(\mathbb{F}_2^n - \{0\}) \times \mathbb{F}_2^q$.

4.5 Good diffusion

Definition 7 A Boolean map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ has **good diffusion** with respect to $u \in \mathbb{F}_2^n$, if the difference function $\Delta_u f$ is balanced.

Remarks

1. For $q = 1$ this means $f(x + u) - f(x) = 0$ or 1 each for exactly 2^{n-1} vectors $x \in \mathbb{F}_2^n$. Let's denote the number of zeroes of the difference function by
$$\eta_f(u) := \#\{x \in \mathbb{F}_2^n \mid \Delta_u f(x) = 0\} = 2^n \delta_f(u, 0),$$
then good diffusion with respect to u is equivalent with $\eta_f(u) = 2^{n-1}$.

2. For general q good diffusion means, that $\#D_f(u, v) = 2^{n-q}$ and $\delta_f(u, v) = \frac{1}{2^q}$ for all $v \in \mathbb{F}_2^q$—i. e. the "row u" of the differential profile is constant.

3. With respect to 0 no map has good diffusion.

4. Affine maps don't have good diffusion with respect to any vector u.

5. A Boolean map f is perfectly nonlinear, if and only if it has good diffusion with respect to *all* vectors $u \in \mathbb{F}_2^n - \{0\}$.

Definition 8 (Webster/Tavares, Crypto 85) A Boolean *function* f fulfils the strict avalanche criterion (SAC), if f has good diffusion with respect to all canonical base vectors.

This means: Flipping one input bit changes exactly half of the values of f.

Remarks

6. Every perfectly nonlinear function fulfils the SAC.

We can express good diffusion of a Boolean function f by the convolution of the character form χ_f with itself:

$$\chi_f * \chi_f(u) = 2^n \kappa_f(u) = 2^n[\delta_f(u,0) - \delta_f(u,1)] = 2\eta_f(u) - 2^n,$$

where κ_f is the autocorrelation. Hence:

Lemma 3 *A Boolean function $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ has good diffusion with respect to u, if and only if*

$$\chi_f * \chi_f(u) = 0 \qquad \text{or in other words} \quad \kappa_f(u) = 0.$$

Moreover u is a linear structure of f, if and only if

$$\chi_f * \chi_f(u) = \pm 2^n \qquad \text{or in other words} \quad \kappa_f(u) = \pm 1.$$

Setting $u = 0$ we conclude

$$\chi_f * \chi_f(0) = 2^n,$$

since $\eta_f(0) = 2^n$. Therefore f is perfectly nonlinear, if and only if $\chi_f * \chi_f = \hat{1}$, the point mass in 0, or if $(\hat{\chi}_f)^2 = \widehat{\chi_f * \chi_f} = 2^n$ constant. This was just the definition of a bent function. Thus we have shown:

Corollary 1 (Dillon 1974) *A Boolean function f is perfectly nonlinear, if and only if it is bent.*

Corollary 2 (Nyberg, EUROCRYPT 91) *A Boolean map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ is perfectly nonlinear, if and only if it is bent.*

Proof. Each of these properties is equivalent analogous statement for all functions $\beta \circ f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ where $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$ an arbitrary linear form $\neq 0$. $\diamond$

An expression for a globally "as good as possible" diffusion of a Boolean function is the **global autocorrelation**

$$\tau_f := \sum_{x \in \mathbb{F}_2^n} \kappa_f(x)^2 = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} \hat{\kappa}_f(u)^2 = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} \hat{\chi}_f(u)^4;$$

we have used Parseval's equation and the corollary 5 of the convolution theorem in 2.3. In particular $\tau_f \geq \kappa_f(0)^2 = 1$, and we know already, that f is perfectly nonlinear, if and only if $\tau_f = 1$. Furthermore

$$\tau_f = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} \hat{\chi}_f(u)^4 \quad \leq \quad \frac{1}{2^n} \left[\sum_{u \in \mathbb{F}_2^n} \hat{\chi}_f(u)^2 \right]^2,$$

because all summands are ≥ 0; equality holds, if and only if at most one summand is > 0. Therefore $\tau_f \leq 2^n$, and equality holds, if and only if at most one $\hat{\chi}_f(u)^2 > 0$. This one term then must equal the total sum of squares 2^{2n}, hence $\hat{\chi}_f(u) = \pm 2^n$, hence $L_f(u) = \emptyset$ or $\mathbb{F}_2^n$, hence $f(x) = u \cdot x + 1$ or $f(x) = u \cdot x$ for all x. We have shown:

Proposition 3 *Let τ_f be the global autocorrelation of a Boolean function $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$. Then:*

(i) $1 \leq \tau_f \leq 2^n$.

(ii) $\tau_f = 1 \Longleftrightarrow f$ *perfectly nonlinear.*

(iii) $\tau_f = 2^n \Longleftrightarrow f$ *affine.*

4.6 The linearity distance

Let

$$\mathcal{LS}_n := \{f : \mathbb{F}_2^n \to \mathbb{F}_2 \mid f \text{ has a linear structure } \neq 0\}.$$

This is the union of the vector subspaces for a fixed linear structure, but it is in general not a vector subspace.

Definition 9 (Meier/Staffelbach, EUROCRYPT 89) For a Boolean function $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ the Hamming distance

$$\rho_f := d(f, \mathcal{LS}_n)$$

is called the **linearity distance** of f.

Remarks

1. $\rho_f = 0 \Leftrightarrow f$ has a linear structure $\neq 0$.
2. Because $\mathcal{A}_n \subseteq \mathcal{LS}_n$, we have $\rho_f \leq \sigma_f$, the nonlinearity.

How large is ρ_f else? To find an answer, we count: For a fixed vector $u \in \mathbb{F}_2^n$ we decompose $\mathbb{F}_2^n$ into two subsets

$$\begin{aligned} D_f(u,0) &= \{x \in \mathbb{F}_2^n \mid \Delta_u f(x) = 0\}, \\ D_f(u,1) &= \{x \in \mathbb{F}_2^n \mid \Delta_u f(x) = 1\} \end{aligned}$$

of sizes $n_0 = \eta_f(u) = 2^n \delta_f(u,0)$ and $n_1 = 2^n - \eta_f(u) = 2^n \delta_f(u,1)$.

First assume $n_0 \geq n_1$. To convert f to a function that has u as a linear structure, we have to change at least $\frac{n_1}{2}$ values, and that suffices: To see this let $D_f(u,1) = M_1' \cup M_1''$ be decomposed into any two subsets of the same size, where $x \in M_1' \Leftrightarrow x+u \in M_1''$, $\#M_1' = \#M_1'' = \frac{n_1}{2}$; then the function

$$f'(x) := \begin{cases} f(x)+1 & \text{for } x \in M_1', \\ f(x) & \text{else,} \end{cases}$$

has u as a linear structure:

$$\Delta_u f'(x) = f'(x+u) + f'(x) = \begin{cases} f(x+u)+f(x) & = 0 \quad \text{for } x \in M_0, \\ f(x+u)+f(x)+1 & = 0 \quad \text{for } x \in M_1', \\ f(x+u)+1+f(x) & = 0 \quad \text{for } x \in M_1'', \end{cases}$$

and this cannot be got with less changes.

If $n_0 < n_1$, in the same way we need $\frac{n_0}{2}$ changes. Therefore the distance of f to any function g, that has u as a linear structure, is

$$d(f,g) \geq n_f(u) := \min\{\frac{n_0}{2}, \frac{n_1}{2}\} = 2^{n-1} \cdot \min\{\delta_f(u,0), \delta_f(u,1)\},$$

and this value is assumed by a suitable g. We conclude

$$\rho_f = \min\{n_f(u) \mid u \in \mathbb{F}_2^n - \{0\}\}.$$

Since always $n_0 + n_1 = 2^n$, we have $n_f(u) \leq 2^{n-2}$. We have shown the first statement of:

Proposition 4 (Meier/Staffelbach, EUROCRYPT 89**)** *The linearity distance of a Boolean function $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ is*

$$\rho_f \leq 2^{n-2}.$$

Equality holds, if and only if f is perfectly nonlinear.

Proof. We have to show the second statement: In the count above for each vector $u \in \mathbb{F}_2^n - \{0\}$ we have $n_0 = \delta_f(u,0) = n_1 = \delta_f(u,1) = 2^{n-1}$. $\diamond$

Furthermore

$$\rho_f = 2^{n-1} \cdot \min\{\delta_f(u,v) \mid u \in \mathbb{F}_2^n - \{0\}, v \in \mathbb{F}_2\}.$$

Let this minimum be taken in (u_0, v_0), i. e. $\rho_f = 2^{n-1} \cdot \delta_f(u_0, v_0)$, then $\delta_f(u_0, v_0+1) = 1 - \delta_f(u_0, v_0)$ is maximum, whence $= \Omega_f$. We conclude:

Proposition 5 *The linearity distance ρ_f of a Boolean function f is tied to the differential potential Ω_f by the formula:*

$$\rho_f = 2^{n-1} \cdot (1 - \Omega_f).$$