4 Approximation durch lineare Strukturen

Die zweite wichtige Methode, versteckte Linearität aufzudecken, beruht auf „linearen Strukturen“. Diese werden durch Differenzenrechnung entdeckt.

4.1 Lineare Strukturen

Definition 1 Für eine Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ und einen Vektor $u \in \mathbb{F}_2^n$ ist die **Differenzenabbildung** $\Delta_u f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ definiert durch

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

Hilfssatz 1 *Für $f, g \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ und $u \in \mathbb{F}_2^n$ gilt:*

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

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

Beweis. (i) ist trivial.

(ii) Man kann der Reihe nach o. B. d. A. annehmen: $q = 1$, $f = T^I$ Monom, $f = T_1 \cdots T_r$. Dann ist

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

klar vom Grad $\leq r - 1$. $\diamond$

Korollar 1 *Ist f konstant, so $\Delta_u f = 0$ für alle $u \in \mathbb{F}_2^n$.*

Korollar 2 *Ist f affin, so $\Delta_u f$ konstant für alle $u \in \mathbb{F}_2^n$.*

Bemerkungen

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. (Produktregel) In der Situation

   $$\mathbb{F}_2^n \xrightarrow{(f,g)} \mathbb{F}_2^q \times \mathbb{F}_2^r \xrightarrow{\gamma} \mathbb{F}_2^s$$

   mit einer bilinearen Abbildung γ sei $h := \gamma \circ (f, g) \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^s$. Dann ist

   $$\begin{aligned}
   \Delta_u h(x) &= \gamma(f(x+u), g(x+u)) - \gamma(f(x), g(x)) \\
   &= \gamma(f(x+u), g(x+u)) - \gamma(f(x+u), g(x)) \\
   &+ \gamma(f(x+u), g(x)) - \gamma(f(x), g(x)) \\
   &= \gamma(f(x+u), g(x+u) - g(x)) + \gamma(f(x+u) - f(x), g(x)) \\
   &= \gamma(f(x+u), \Delta_u g(x)) + \gamma(\Delta_u f(x), g(x))
   \end{aligned}$$

3. Ist $g : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^r$ linear, so $\Delta_u(g \circ f) = g \circ \Delta_u f$.

Definition 2 (Evertse, Eurocrypt 87) Ein Vektor $u \in \mathbb{F}_2^n$ heißt **lineare Struktur** von $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$, wenn $\Delta_u f$ konstant ist.

Bemerkungen

4. Ist f affin, so ist jeder Vektor eine lineare Struktur von f.

5. 0 ist stets eine lineare Struktur von f.

6. Mit u und v ist auch $u + v$ lineare Struktur wegen Bemerkung 1. Die linearen Strukturen von f bilden also einen Untervektorraum von $\mathbb{F}_2^n$. Auf diesem ist f affin. Insbesondere gilt in Bemerkung 4 auch die Umkehrung.

7. Ist $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ eine Abbildung mit $f(0) = 0$, so ist $u \in \mathbb{F}_2^n$ genau dann lineare Struktur von f, wenn $f(x + u) - f(x)$ konstant, etwa $= c \in \mathbb{F}_2^q$ ist. Da dann $c = f(u) - f(0) = f(u)$, ist u in diesem Fall genau dann lineare Struktur von f, wenn

$$f(x + u) = f(x) + f(u) \quad \text{für alle } x \in \mathbb{F}_2^n.$$

8. Falls $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ quadratische Form mit zugehöriger Bilinearform β_f ist, so ist u genau dann lineare Struktur, wenn $\beta_f(u, x) = f(x + u) - f(x) - f(u) = 0$ für alle x, also wenn $u \in \mathrm{Rad}_f$. Das Radikal ist also in diesem Fall der Vektorraum der linearen Strukturen von f, und seine Dimension ist $n - \mathrm{Rang}\, f$. Insbesondere ist nach dem Korollar 2 in 2.8 f genau dann krumm, wenn $\mathrm{Rad}_f = 0$, also wenn die Linearitätsdimension $= 0$ ist im Sinne der folgenden Definition.

Definition 3 Für eine Boolesche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ wird der Vektorraum der linearen Strukturen als das **Radikal** Rad_f bezeichnet, seine Dimension als **Linearitätsdimension** von f und seine Codimension als **Rang** von f, $\mathrm{Rang}\, f$.

Bemerkungen

9. Ist $f = g \oplus h$ direkte Summe, so ist (u, v) für $u \in \mathbb{F}_2^r$ und $v \in \mathbb{F}_2^s$ genau dann lineare Struktur von f, wenn u lineare Struktur von g und v lineare Struktur von h ist. Insbesondere ist

$$\mathrm{Rad}_f = \mathrm{Rad}_g \oplus \mathrm{Rad}_h\,.$$

4.2 Das Differenzenprofil

Für eine BOOLEsche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ und $u \in \mathbb{F}_2^n$, $v \in \mathbb{F}_2^q$ sei

$$D_f(u,v) := \{x \in \mathbb{F}_2^n \mid \Delta_u f(x) = v\},$$

$$\delta_f(u,v) := \frac{1}{2^n} \# D_f(u,v).$$

Definition 4 (CHABAUD/VAUDENAY, EUROCRYPT 94) Die Funktion $\delta_f : \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{Q}$ heißt **Differenzenprofil** von f.

(Die Normierung mit dem Faktor $\frac{1}{2^n}$ erweist sich als zweckmäßig. In der Literatur wird die Matrix $\# D_f(u,v)$ auch als Differenzentabelle bezeichnet.)

Bemerkungen

1. Ist f affin, $f(x) = Ax + b$, so $\Delta_u f(x) = Au$, also

$$D_f(u,v) = \{x \in \mathbb{F}_2^n | Au = v\} = \begin{cases} \mathbb{F}_2^n, & \text{falls } Au = v, \\ \emptyset & \text{sonst,} \end{cases}$$

$$\delta_f(u,v) = \begin{cases} 1, & \text{falls } Au = v, \\ 0 & \text{sonst.} \end{cases}$$

   (Jede Zeile des Differenzenprofils enthält genau eine 1 und sonst nur Nullen.)

2. Es sind äquivalent:

$$\begin{aligned} u \text{ lineare Struktur von } f &\iff D_f(u,v) = \begin{cases} \mathbb{F}_2^n & \text{für ein } v, \\ \emptyset & \text{sonst,} \end{cases} \\ &\iff \delta_f(u,v) = \begin{cases} 1 & \text{für ein } v, \\ 0 & \text{sonst.} \end{cases} \end{aligned}$$

   (Die „Zeile u“ des Differenzenprofils ist 0 außer genau einem Eintrag 1.)

3. Für beliebiges f, aber $u = 0$ gilt

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

   („erste Zeile“ des Differenzenprofils).

4. $\sum_{v \in \mathbb{F}_2^q} \delta_f(u,v) = 1$ („Zeilensummen“ des Differenzenprofils). Insbesondere gibt es für jeden Vektor $u \in \mathbb{F}_2^n$ ein $v \in \mathbb{F}_2^q$ mit $\delta_f(u,v) \geq \frac{1}{2^q}$.

Damit ist klar:

Satz 1 *Für eine Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ sind äquivalent:*

(i) *f ist affin.*

(ii) *Jeder Vektor $u \in \mathbb{F}_2^n$ ist lineare Struktur von f.*

(iii) *Jede Zeile des Differenzenprofils enthält genau einen Eintrag $\neq 0$.*

Bemerkungen

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

6. Alle Werte $\#D_f(u,v)$ sind gerade: Für $u = 0$ folgt das aus Bemerkung 3, sonst aus Bemerkung 5. Daher sind alle $\delta_f(u,v)$ ganzzahlige Vielfache von $\frac{1}{2^{n-1}}$.

7. Was passiert bei Addition eines konstanten Vektors im Bild? Ist $g(x) = f(x) + b$, so $g(x+u) = f(x+u) + b$ und $g(x) + v = f(x) + b + v$, also $D_g(u,v) = D_f(u,v)$, insbesondere $\delta_g = \delta_f$.

8. Was passiert bei Addition eines konstanten Vektors im Urbild? Ist $h(x) = f(x+a)$, so

$$\begin{aligned} D_h(u,v) &= \{x \mid h(x+u) = h(x) + v\} \\ &= \{y - a \mid f(y+u) = f(y) + v\} = D_f(u,v) - a, \end{aligned}$$

   insbesondere $\delta_h = \delta_f$.

9. Was passiert bei linearen Transformationen im Bildraum? Ist $h \in GL_q(\mathbb{F}_2)$, so ist

$$\begin{aligned} D_{h \circ f}(u,v) &= \{x \mid h \circ f(x+u) = h \circ f(x) + v\} \\ &= \{x \mid f(x+u) = f(x) + h^{-1}(v)\} = D_f(u, h^{-1}(v)), \end{aligned}$$

   insbesondere werden die Spalten von δ_f permutiert.

10. Was passiert bei linearen Transformationen im Urbildraum? Ist $g \in GL_n(\mathbb{F}_2)$, so ist

$$\begin{aligned} D_{f \circ g}(u,v) &= \{x \mid f \circ g(x+u) = f \circ g(x) + v\} \\ &= \{g^{-1}(y) \mid f(y + g(u)) = f(y) + v\} = g^{-1}(D_f(g(u), v), \end{aligned}$$

    insbesondere werden die Zeilen von δ_f permutiert.

Die letzten vier Bemerkungen zusammen zeigen:

Satz 2 *Das Differenzenprofil δ_f einer* Boole*schen Abbildung f wird unter beliebigen affinen Transformationen von Bild und Urbild permutiert.*

Bemerkungen

11. Ist f bijektiv, so ist die Menge

$$D_{f^{-1}}(v,u) = \{y \in \mathbb{F}_2^n \mid f^{-1}(y+v) = f^{-1}(y) + u\}$$

für beliebige $u, v \in \mathbb{F}_2^n$ das Bild unter f von $D_f(u,v)$. Insbesondere sind beide Mengen gleich groß, und es folgt

$$\delta_{f^{-1}}(v,u) = \delta_f(u,v).$$

Das Differenzenprofil von f^{-1} ist – als Matrix geschrieben – also transponiert zum Differenzenprofil von f; insbesondere sind auch alle Spaltensummen des Differenzenprofils von f gleich 1. Dieses ist also, wie das Linearitätsprofil, ebenfalls eine doppelt stochastische Matrix und hat in der ersten Spalte oben eine 1, dann lauter Nullen.

12. Im Fall $q = 1$ lässt sich die Autokorrelation nach ihrer Definition als

$$\kappa_f(x) = \delta_f(x,0) - \delta_f(x,1)$$

ausdrücken.

Beispiele

1. Im Fall $n = 2$, $q = 1$, $f(x_1, x_2) = x_1x_2$, ist

$$D_f(u,v) = \{(x_1,x_2) \mid u_2x_1 + u_1x_2 = u_1u_2 + v\}.$$

Daraus bestimmt man

$\#D_f(u,v)$	0	1
00	4	0
01	2	2
10	2	2
11	2	2

$\delta_f(u,v)$	0	1
00	1	0
01	$\frac{1}{2}$	$\frac{1}{2}$
10	$\frac{1}{2}$	$\frac{1}{2}$
11	$\frac{1}{2}$	$\frac{1}{2}$

2. Ist $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ quadratische Form mit zugehöriger Bilinearform β_f, so $\Delta_u f(x) = f(x+u) - f(x) = f(u) + \beta_f(x,u)$. Also gilt

$$x \in D_f(u,v) \Longleftrightarrow \Delta_u f(x) = v \Longleftrightarrow \beta_f(x,u) = v - f(u).$$

Falls $f(u) = v$, gilt also $x \in D_f(u,v) \iff \beta_f(x,u) = 0$, falls $f(u) \neq v$, ist $x \in D_f(u,v) \iff \beta_f(x,u) = 1$. Daher gilt im Fall $u \in \mathrm{Rad}_f$:

$$D_f(u,v) = \begin{cases} \mathbb{F}_2^n & \text{falls } v = f(u), \\ \emptyset & \text{sonst.} \end{cases}$$

Falls $u \notin \mathrm{Rad}_f$, ist $H := \{x \mid \beta_f(u,x) = 0\}$ ein 1-codimensionaler Unterraum von $\mathbb{F}_2^n$ und $\bar{H} = \{x \mid \beta_f(u,x) = 1\}$ die dazu parallele Hyperebene. Daher ist

$$D_f(u,v) = \begin{cases} H & \text{falls } v = f(u), \\ \bar{H} & \text{sonst.} \end{cases}$$

Für das Differenzenprofil folgt

$$\delta_f(u,v) = \begin{cases} 1, & \text{wenn } u \in \mathrm{Rad}_f \text{ und } v = f(u), \\ 0, & \text{wenn } u \in \mathrm{Rad}_f \text{ und } v \neq f(u), \\ \frac{1}{2} & \text{wenn } u \notin \mathrm{Rad}_f, \end{cases}$$

und für die Autokorrelation

$$\kappa_f(x) = \delta_f(x,0) - \delta_f(x,1) = \begin{cases} \pm 1 & \text{für } x \in \mathrm{Rad}_f \\ 0 & \text{sonst.} \end{cases}$$

3. Sei $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ quadratisch mit zugehöriger bilinearer Abbildung

$$\beta_f(x,y) = f(x+y) - f(x) - f(y) + f(0).$$

Dann ist

$$D_f(u,v) = \{x \mid f(x+u) - f(x) = v\} = \{x \mid \alpha_{f,u}(x) = v - f(u) + f(0)\}$$

mit der linearen Abbildung $\alpha_{f,u}\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$, $\alpha_{f,u}(x) = \beta_f(x,u)$. Daher gilt

$$D_f(u,v) = \mathrm{Kern}\,\alpha_{f,u}, \quad \text{falls } v = f(u) - f(0);$$

ist allgemeiner $v - f(u) + f(0)$ im Bild von $\alpha_{f,u}$, so ist $D_f(u,v)$ eine Nebenklasse des Unterraums $\mathrm{Kern}\,\alpha_{f,u}$, ansonsten $D_f(u,v) = \emptyset$. Setzt man $s_u := \mathrm{Dim}\,\mathrm{Bild}\,\alpha_{f,u}$, so ist $1 \leq s_u \leq q$ und

$$\#D_f(u,v) = \begin{cases} 2^{n-s_u} & \text{falls } v - f(u) + f(0) \in \mathrm{Bild}(\alpha_{f,u}), \\ 0 & \text{sonst.} \end{cases}$$

4.3 Effiziente Berechnung des Differenzenprofils

Grundlage für die effiziente Berechnung von Differenzenprofilen ist der folgende Hilfssatz:

Hilfssatz 2 *Für jede* Boolesche *Abbildung* $f: \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *gilt*

$$\delta_f = \frac{1}{2^n}\vartheta_f * \vartheta_f.$$

Beweis. Das folgt aus der Gleichungskette

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

Aus dem Faltungssatz folgt damit direkt

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

also:

Hauptsatz 1 *Das Differenzenprofil ist bis auf einen konstanten Faktor die* Walsh*-Transformierte des Linearitätsprofils:*

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

Mit der Gleichung von Parseval folgt unmittelbar:

Korollar 1 *Für jede* Boolesche *Abbildung* $f: \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *gilt*

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

Korollar 2 *Zwei* Boolesche *Abbildungen* $\mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *haben genau dann das gleiche Linearitätsprofil, wenn sie das gleiche Differenzenprofil haben.*

Das Differenzenprofil der Abbildung $f: \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ lässt sich also nach folgendem Algorithmus berechnen, der das Linearitätsprofil als Zwischenergebnis liefert:

1. Bestimmung von $\hat{\vartheta}_f$.

2. Quadrieren $\omega := \hat{\vartheta}_f^2$, $\lambda_f = \frac{1}{2^{2n}} \cdot \omega$.

3. Rücktransformation $\delta_f = \frac{1}{2^q}\hat{\lambda}_f = \frac{1}{2^{2n+q}}\hat{\omega}$.

Der Aufwand, wenn man $\hat{\lambda}_f$ schon berechnet hat, besteht aus weiteren $3N \cdot {}^2\log(N)$ „elementaren Operationen“, insgesamt also im wesentlichen aus $6N \cdot {}^2\log(N)$ solchen Operationen plus N Quadrierungen, wobei $N = 2^{n+q}$ die Größe des Inputs ist.

Beispiele

1. Ist f durch das Polynom $T_1T_1 + T_3T_4$ gegeben, so

$$\omega(x,y) = \begin{cases} 256 & \text{für } x = 0,\ y = 0, \\ 0 & \text{für } x \neq 0,\ y = 0, \\ 16 & \text{für } y = 1, \end{cases}$$

$$\delta_f(u,v) = \begin{cases} 1 & \text{für } u = 0,\ v = 0, \\ 0 & \text{für } u = 0,\ v = 1, \\ \frac{1}{2} & \text{sonst.} \end{cases}$$

2. Ebenso folgt für $T_1T_2 + T_1T_3 + T_2T_3$:

$$\delta_f(u,v) = \begin{cases} 1 & \text{für } u = 0,\ v = 0 \text{ und für } u = 111,\ v = 1, \\ 0 & \text{für } u = 0,\ v = 1 \text{ und für } u = 111,\ v = 0, \\ \frac{1}{2} & \text{sonst.} \end{cases}$$

3. Für $T_1 \cdots T_n$ folgt

$$\delta_f(u,v) = \begin{cases} 1 & \text{für } u = 0,\ v = 0, \\ 0 & \text{für } u = 0,\ v = 1, \\ 1 - \frac{1}{2^{n-1}} & \text{für } u \neq 0,\ v = 0, \\ \frac{1}{2^{n-1}} & \text{für } u \neq 0,\ v = 1. \end{cases}$$

   Für $(T_1 + 1) \cdots (T_n + 1)$ ist das Ergebnis das gleiche.

4. Für die fünf Normalformen von Abbildungen $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$ erhalten wir für δ_f der Reihe nach die Tabellen:

	00	01	10	11
00	1	0	0	0
01	1	0	0	0
10	1	0	0	0
11	1	0	0	0

	00	01	10	11
00	1	0	0	0
01	1	0	0	0
10	0	0	1	0
11	0	0	1	0

	00	01	10	11
00	1	0	0	0
01	0	1	0	0
10	0	0	1	0
11	0	0	0	1

	00	01	10	11
00	1	0	0	0
01	$\frac{1}{2}$	0	$\frac{1}{2}$	0
10	$\frac{1}{2}$	0	$\frac{1}{2}$	0
11	$\frac{1}{2}$	0	$\frac{1}{2}$	0

	00	01	10	11
00	1	0	0	0
01	0	$\frac{1}{2}$	0	$\frac{1}{2}$
10	$\frac{1}{2}$	0	$\frac{1}{2}$	0
11	0	$\frac{1}{2}$	0	$\frac{1}{2}$

5. Für den Volladdierer – siehe 3.1 – erhalten wir ebenso:

δ_f	00	01	10	11
000	1	0	0	0
001	0	$\frac{1}{2}$	0	$\frac{1}{2}$
010	0	$\frac{1}{2}$	0	$\frac{1}{2}$
011	$\frac{1}{2}$	0	$\frac{1}{2}$	0
100	0	$\frac{1}{2}$	0	$\frac{1}{2}$
101	$\frac{1}{2}$	0	$\frac{1}{2}$	0
110	$\frac{1}{2}$	0	$\frac{1}{2}$	0
111	0	0	0	1

Hilfssatz 3 *Für jede* Boole*sche Abbildung* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *gilt*

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

für alle $v \in \mathbb{F}_2^q$.

Beweis. Durch Aufsummieren in Hilfssatz 2 folgt

$$\begin{aligned}
2^n \sum_{u\in\mathbb{F}_2^n} \delta_f(u,v) &= \sum_{u\in\mathbb{F}_2^n}\sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q} \vartheta_f(x,y)\vartheta_f(u+x,v+y) \\
&= \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q} \vartheta_f(x,y)\cdot\left[\sum_{u\in\mathbb{F}_2^n} \underbrace{\vartheta_f(u+x,v+y)}_{\nu_f(v+y)\text{-mal 1, sonst 0}}\right] \\
&= \sum_{y\in\mathbb{F}_2^q}\left[\sum_{x\in\mathbb{F}_2^n} \underbrace{\vartheta_f(x,y)}_{\nu_f(y)\text{-mal 1, sonst 0}}\right]\cdot\nu_f(v+y) \\
&= \sum_{y\in\mathbb{F}_2^q} \nu_f(y)\cdot\nu_f(v+y) \\
&= \nu_f * \nu_f(v).\diamond
\end{aligned}$$

Aus Hilfssatz 3 und Satz 5 in 3.2 folgt sofort die folgende Verallgemeinerung von Bemerkung 11 in 4.2:

Satz 3 (Zhang/Zheng, SAC '96) *Für $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ sind folgende Aussagen äquivalent:*

(i) *f ist balanciert.*

(ii) *$\sum_{u \in \mathbb{F}_2^n} \delta_f(u, v) = 2^{n-q}$ für alle $v \in \mathbb{F}_2^q$ (alle „Spaltensummen" des Differenzenprofils).*

(iii) *$\sum_{u \in \mathbb{F}_2^n} \delta_f(u, 0) = 2^{n-q}$ (1. „Spaltensumme" des Differenzenprofils).*

4.4 Das differenzielle Potenzial

Definition 5 (Nyberg, Eurocrypt 93) Für eine Boolesche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ heißt

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

differenzielles Potenzial von f.

Anmerkung. In der Literatur wird der maximale Eintrag der Differenzentabelle (außer bei $(0, 0)$) als differenzielle Uniformität bezeichnet.

Bemerkungen

1. Ω_f ist invariant unter affinen Transformationen von $\mathbb{F}_2^n$ und $\mathbb{F}_2^q$.

2. Wegen Bemerkung 4 in 4.2 folgt

$$\frac{1}{2^q} \leq \Omega_f \leq 1.$$

3. Die untere Grenze $\Omega_f = 2^{-q}$ wird genau dann angenommen, wenn für $u \neq 0$ alle $\delta_f(u, v) = 2^{-q}$ sind, d. h., wenn alle Differenzenabbildungen $\Delta_u f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ balanciert (3.2) sind. („Zeile u" des Differenzenprofils konstant.)

4. Hat f eine lineare Struktur $\neq 0$, d. h., ist $\mathrm{Rad}_f \neq 0$, so ist $\Omega_f = 1$.

5. Ist f bijektiv, so $\Omega_{f^{-1}} = \Omega_f$.

6. Da für $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ alle Werte des Differenzenprofils δ_f stets Vielfache von $\frac{1}{2^{n-1}}$ sind, ist das differenzielle Potenzial $\Omega_f \geq \frac{1}{2^{n-1}}$.

Beispiele

1. Ist f affin, so $\Omega_f = 1$.
2. Im Fall $n = 2$, $q = 1$, $f(x_1, x_2) = x_1 x_2$, ist $\Omega_f = \frac{1}{2}$.
3. Im Falle einer quadratischen Abbildung folgt aus Beispiel 3 in 4.2 der folgende Satz:

Satz 4 (Seberry, Zhang, Zheng, Eurocrypt 94) *Sei $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ eine quadratische Abbildung.*

(i) *Ist $\mathrm{Rad}_f \neq 0$, so ist $\Omega_f = 1$.*

(ii) *Ist f nichtausgeartet, so ist $\Omega_f = \frac{1}{2^s}$ mit $1 \leq s \leq q$, insbesondere $\Omega_f \leq \frac{1}{2}$. Dabei ist $s = q$ nur möglich, wenn $n = 2q$ und f krumm. In allen anderen Fällen, insbesondere, wenn f balanciert ist, gilt $1 \leq s \leq q-1$.*

Hilfssatz 4 *Sei $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ quadratisch und bijektiv und $u \in \mathbb{F}_2^n - \{0\}$. Dann gibt es mindestens eine Linearform $\beta \in \mathcal{L}_n - \{0\}$, so dass $\beta \circ f$ den Vektor u als lineare Struktur hat.*

Beweis. Es ist $D_f(u, 0) = \emptyset$; insbesondere ist die Differenzenabbildung $\Delta_u f$ nicht balanciert. Also ist mindestens ein $\beta \circ \Delta_u f = \Delta_u(\beta \circ f)$ nicht balanciert. Da diese Differenzenfunktion aber affin ist, muss sie dann konstant sein. Das war zu zeigen. $\diamond$

Satz 5 (Seberry, Zhang, Zheng, Eurocrypt 94) *Sei $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ eine bijektive quadratische Abbildung mit $\Omega_f = \frac{1}{2^{n-1}}$. Dann gilt*

(i) *Jeder Vektor $u \in \mathbb{F}_2^n - \{0\}$ ist lineare Struktur von $\beta \circ f$ für genau eine Linearform $\beta \in \mathcal{L}_n - \{0\}$.*

(ii) *Für jede Linearform $\beta \in \mathcal{L}_n - \{0\}$ hat die quadratische Funktion $\beta \circ f$ den Rang $n - 1$.*

(iii) *n ist ungerade.*

Beweis. (i) Nach Bemerkung 6 in 4.2 sind alle $\delta_f(u, v) = 0$ oder $\frac{1}{2^{n-1}}$. Die Differenzenabbildung $\Delta_u f$ nimmt also genau 2^{n-1} Werte an (jeweils doppelt).

Annahme: u ist für zwei verschiedene Linearformen β_1, β_2 lineare Struktur von $\beta_i \circ f$. Da über dem Grundkörper $\mathbb{F}_2$ zwei verschiedene Vektoren $\neq 0$ stets linear unabhängig sind, lassen sich β_1, β_2 zu einer Basis $\beta_1, \ldots, \beta_n$ von $\mathcal{L}_n$ ergänzen. Dann ist

$$g := \begin{pmatrix} \beta_1 \circ f \\ \vdots \\ \beta_n \circ f \end{pmatrix} = h \circ f \quad \text{mit } h \in GL_n(\mathbb{F}_2),$$

also $\Omega_g = \Omega_f = \frac{1}{2^{n-1}}$. Aber $\Delta_u g$ hat die ersten beiden Komponenten konstant, kann also höchstens 2^{n-2} veschiedene Werte annehmen: Widerspruch.

(ii) Nach (i) besteht eine bijektive Beziehung zwischen Vektoren $u \neq 0$ und Linearformen $\beta \neq 0$. Also hat umgekehrt $\beta \circ f$ für jedes $\beta \in \mathcal{L}_n - \{0\}$ genau eine lineare Struktur $\neq 0$. Also hat jedes $\beta \circ f$ den Rang $n-1$.

(iii) Da der Rang einer quadratischen Funktion nach Satz 8 in 1.7 stets gerade ist, muss n ungerade sein. $\diamond$

Korollar 1 *Sei $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ eine bijektive quadratische Abbildung. Dann ist $\Omega_f \geq \frac{1}{2^{n-1}}$, wenn n ungerade, und $\Omega_f \geq \frac{1}{2^{n-2}}$, wenn n gerade.*

Beweis. Die erste Aussage gilt nach Bemerkung 6 viel allgemeiner. Die zweite folgt, da Ω_f nicht $\frac{1}{2^{n-1}}$ sein kann. $\diamond$

Definition 6 (Nyberg, Eurocrypt 93) Eine Boolesche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ heißt **perfekt nichtlinear**, wenn das differenzielle Potenzial den minimalen Wert $\Omega_f = 2^{-q}$ hat.

Bemerkungen

7. Das ist nach Bemerkung 3 in 4.1 und Satz 4 in 3.2 genau dann der Fall, wenn $\beta \circ f$ für jede Linearform $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$, $\beta \neq 0$ perfekt nichtlinear ist.

8. Perfekt nichtlineare Abbildungen $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ haben insbesondere keine linearen Strukturen $u \neq 0$.

Aus Bemerkung 3 folgt:

Satz 6 *Genau dann ist $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ perfekt nichtlinear, wenn das Differenzenprofil δ_f auf $(\mathbb{F}_2^n - \{0\}) \times \mathbb{F}_2^q$ konstant $= 2^{-q}$ ist.*

Beispiele

3. Für die fünf Normalformen von Abbildungen $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$ ist Ω_f der Reihe nach 1, 1, 1, $\frac{1}{2}$, $\frac{1}{2}$. Insbesondere ist $\frac{1}{2}$ der kleinstmögliche Wert für Abbildungen $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$.

4. Ist $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ quadratische Form, so ist nach Beispiel 2 in 4.2

$$\Omega_f = \begin{cases} \frac{1}{2}, & \text{wenn Rang } f = n, \\ 1 & \text{sonst.} \end{cases}$$

4.5 Gute Diffusion

Definition 7 Eine BOOLEsche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ hat **gute Diffusion** bezüglich $u \in \mathbb{F}_2^n$, wenn die Differenzenabbildung $\Delta_u f$ balanciert ist.

Bemerkungen

1. Im Fall $q = 1$ bedeutet das $f(x+u)-f(x) = 0$ oder 1 für jeweils genau 2^{n-1} Vektoren $x \in \mathbb{F}_2^n$. Bezeichnet man die Anzahl der Nullstellen der Differenzenfunktion mit

$$\eta_f(u) := \#\{x \in \mathbb{F}_2^n \mid \Delta_u f(x) = 0\} = 2^n \delta_f(u, 0),$$

   so ist die gute Diffusion bezüglich u äquivalent zu $\eta_f(u) = 2^{n-1}$.

2. Für allgemeines q bedeutet die gute Diffusion, dass $\#D_f(u, v) = 2^{n-q}$ bzw. $\delta_f(u, v) = \frac{1}{2^q}$ für jedes $v \in \mathbb{F}_2^q$, dass also die „Zeile u“ des Differenzenprofils konstant ist.

3. Bezüglich 0 hat keine Abbildung gute Diffusion.

4. Affine Abbildungen haben für keinen Vektor u gute Diffusion.

5. Eine BOOLEsche Abbildung f ist genau dann perfekt nichtlinear, wenn sie gute Diffusion bezüglich *aller* Vektoren $u \in \mathbb{F}_2^n - \{0\}$ hat, wie im Beispiel $f(x_1, x_2) = x_1 x_2$.

Definition 8 (WEBSTER/TAVARES, CRYPTO 85) Eine BOOLEsche *Funktion* f erfüllt das **Lawinenkriterium** (SAC = ‘strict avalanche criterion’), wenn f gute Diffusion für alle kanonischen Basisvektoren hat.

Das bedeutet: Das „Umkippen“ eines Input-Bits ändert genau die Hälfte aller Werte von f.

Bemerkungen

6. Jede perfekt nichtlineare Funktion erfüllt das Lawinenkriterium.

Gute Diffusion einer BOOLEschen Funktion f lässt sich auch durch die Faltung der Charakter-Form χ_f mit sich selbst ausdrücken:

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

wobei κ_f die Autokorrelation ist. Also:

Hilfssatz 5 *Eine* Boolesche *Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ hat genau dann gute Diffusion bezüglich u, wenn*

$$\chi_f * \chi_f(u) = 0 \qquad bzw. \quad \kappa_f(u) = 0.$$

Genau dann ist u lineare Struktur von f wenn

$$\chi_f * \chi_f(u) = \pm 2^n \qquad bzw. \quad \kappa_f(u) = \pm 1.$$

Speziell für $u = 0$ folgt

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

da $\eta_f(0) = 2^n$. Also ist f genau dann perfekt nichtlinear, wenn $\chi_f * \chi_f = \hat{1}$, die Punktmasse in 0, ist, oder wenn $(\hat{\chi}_f)^2 = \widehat{\chi_f * \chi_f} = 2^n$ konstant ist. Das war gerade die Definition einer krummen Funktion. Wir haben also gezeigt:

Korollar 1 (Dillon 1974) *Eine* Boolesche *Funktion f ist genau dann perfekt nichtlinear, wenn sie krumm ist.*

Korollar 2 *Falls es eine perfekt nichtlineare Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ gibt, ist n gerade.*

Satz 7 (Nyberg, Eurocrypt 91) *Eine* Boolesche *Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ ist genau dann perfekt nichtlinear, wenn sie krumm ist.*

Beweis. Beide Eigenschaften sind jeweils äquivalent dazu, dass sie für alle Funktionen $\beta \circ f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ gelten, wo $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$ eine beliebige Linearform $\neq 0$ ist. $\diamond$

Korollar 3 *Ist die Urbilddimension n ungerade, so $\Omega_f > \frac{1}{2^q}$. Ist zusätzlich $q \leq n-1$, so $\Omega_f \geq \frac{1}{2^q} + \frac{1}{2^{n-1}}$.*

Beweis. Die zweite Aussage folgt, weil Ω_f Vielfaches von $\frac{1}{2^{n-1}}$ sein muss und $\frac{1}{2^q} \geq \frac{1}{2^{n-1}}$. $\diamond$

Korollar 4 *Für $n \geq 3$ und $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^{n-1}$ ist $\Omega_f \geq \frac{1}{2^{n-2}}$.*

Beweis. Das folgt, weil f nicht perfekt nichtlinear sein kann wie bei Korollar 3. $\diamond$

Ein Maß für eine global „möglichst gute“ Diffusion einer Booleschen Funktion ist die **globale Autokorrelation**

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

wobei die Umformung auf der PARSEVAL-Gleichung und Korollar 4 zum Faltungssatz in 2.3 beruht. Insbesondere ist $\tau_f \geq \kappa_f(0)^2 = 1$, und wir wissen schon, dass f genau dann perfekt nichtlinear ist, wenn $\tau_f = 1$.

Weiter ist

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

da alle Summanden ≥ 0 sind, mit Gleichheit genau dann, wenn höchstens ein Summand > 0 ist. Also ist $\tau_f \leq 2^n$, und die Gleichheit gilt genau dann, wenn höchstens ein $\hat{\chi}_f(u)^2 > 0$ ist. Dieses eine muss dann gleich der gesamten Quadratsumme 2^{2n} sein, also $\hat{\chi}_f(u) = \pm 2^n$, also $L_f(u) = \emptyset$ oder $\mathbb{F}_2^n$, also $f(x) = u \cdot x + 1$ oder $f(x) = u \cdot x$ für alle x. Damit ist gezeigt:

Satz 8 *Für die globale Autokorrelation τ_f einer* BOOLE*schen Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ gilt:*

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

(ii) $\tau_f = 1 \Longleftrightarrow f$ *perfekt nichtlinear.*

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

(iv) *Ist f quadratische Form vom Rang r, so $\tau_f = 2^{n-r}$.*

(v) *Ist $f = g \oplus h$ direkte Summe, so $\tau_f = \tau_g \tau_h$.*

Beweis. Die vierte Aussage folgt, weil

$$\tau_f = \sum_{x \in \mathbb{F}_2^n} \kappa_f(x)^2 = \sum_{x \in \mathrm{Rad}_f} 1$$

nach Beispiel 2 in 4.2, die fünfte direkt aus $\kappa_f(x, y) = \kappa_g(x)\kappa_h(y)$. $\diamond$

Für die Berechnung zweckmäßig ist die folgende Formel:

$$\begin{aligned} \tau_f &= \sum_{x \in \mathbb{F}_2^n} \kappa_f(x)^2 = \sum_{x \in \mathbb{F}_2^n} [\delta_f(x,0) - \delta_f(x,1)]^2 \\ &= \sum_{x \in \mathbb{F}_2^n} \left([\delta_f(x,0) + \delta_f(x,1)]^2 - 4\delta_f(x,0)\delta_f(x,1) \right), \end{aligned}$$

also:

Hilfssatz 6 *Für die globale Autokorrelation τ_f einer* BOOLE*schen Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ gilt:*

$$\tau_f = 2^n - 4 \cdot \sum_{x \in \mathbb{F}_2^n} \delta_f(x,0)\delta_f(x,1).$$

4.6 Die Linearitätsdistanz

Sei

$$\mathcal{LS}_n := \{f : \mathbb{F}_2^n \to \mathbb{F}_2 \mid f \text{ hat lineare Struktur } \neq 0\}.$$

Das ist die Vereinigung der Untervektorräume zu fester linearer Struktur, aber im allgemeinen selbst kein Untervektorraum.

Definition 9 (Meier/Staffelbach, Eurocrypt 89) Für eine Boolesche Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ heißt die Hamming-Distanz

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

die **Linearitätsdistanz** von f.

Bemerkungen

1. Die Linearitätsdistanz ist invariant unter affinen Transformationen.
2. $\rho_f = 0 \Leftrightarrow f \in \mathcal{LS}_n$.
3. Da $\mathcal{A}_n \subseteq \mathcal{LS}_n$, ist $\rho_f \leq \sigma_f$, die Nichtlinearität.

Wie groß ist ρ_f sonst? Zur Antwort hilft eine Zählung: Für einen festen Vektor $u \in \mathbb{F}_2^n$ lässt sich $\mathbb{F}_2^n$ in die beiden Mengen

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

der Größen $n_0 = \eta_f(u) = 2^n \delta_f(u,0)$ und $n_1 = 2^n - \eta_f(u) = 2^n \delta_f(u,1)$ zerlegen.

Nehmen wir zunächst $n_0 \geq n_1$ an. Um f zu einer Funktion mit u als linearer Struktur zu machen, muss man mindestens $\frac{n_1}{2}$ Werte abändern, und damit schafft man es wirklich: Sei nämlich $D_f(u,1) = M_1' \cup M_1''$ irgendwie in zwei gleichgroße Mengen zerlegt mit $x \in M_1' \Leftrightarrow x + u \in M_1''$, $\#M_1' = \#M_1'' = \frac{n_1}{2}$; dann hat die Funktion

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

den Vektor u als lineare Struktur:

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

und mit weniger Änderungen ist das nicht zu schaffen.

Falls $n_0 < n_1$, benötigt man analog $\frac{n_0}{2}$ Wertänderungen. Also ist die Distanz von f zu jeder Funktion g, die u als lineare Struktur hat,

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

und für geeignetes g wird dieser Wert angenommen. Es folgt

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

Da stets $n_0 + n_1 = 2^n$, ist $n_f(u) \leq 2^{n-2}$. Damit ist gezeigt:

Satz 9 (Meier/Staffelbach, Eurocrypt 89) *Für die Linearitätsdistanz einer* Boole*schen Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ gilt*

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

Die Gleichheit ist äquivalent dazu, dass f perfekt nichtlinear ist.

Beweis der zweiten Aussage: In der obigen Zählung ist für jeden Vektor $u \in \mathbb{F}_2^n - \{0\}$ stets $n_0 = 2^n \cdot \delta_f(u,0) = n_1 = 2^n \cdot \delta_f(u,1) = 2^{n-1}$.$\diamond$

Es folgt weiter

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

Wird dieses Minimum in (u_0, v_0) angenommen, also $\rho_f = 2^{n-1} \cdot \delta_f(u_0, v_0)$, so ist $\delta_f(u_0, v_0 + 1) = 1 - \delta_f(u_0, v_0)$ maximal, also $= \Omega_f$. Gezeigt ist also:

Satz 10 *Die Linearitätsdistanz ρ_f einer* Boole*schen Funktion f lässt sich durch das differenzielle Potential Ω_f so ausdrücken:*

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

Auch die Linearitätsdistanz ist also kein neues Maß für die Nichtlinearität, auch hier gilt, dass sie historisch vor dem differenziellen Potenzial eingeführt wurde.

Ist $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ quadratische Form vom Rang r, so

$$\rho_f = \begin{cases} 2^{n-2}, & \text{wenn } r = n, \\ 0 & \text{sonst,} \end{cases}$$

passend dazu, dass f im ersten Fall krumm ist und im zweiten Fall stets eine lineare Struktur $\neq 0$ hat