3 Approximation durch lineare Relationen

In diesem Abschnitt suchen wir nach verstecker Linearität einer Boolеschen Abbildung, indem wir nach Linearkombinationen der Output-Bits Ausschau halten, die von einer Linearkombination der Input-Bits linear abhängen – zumindest für einige Argumente.

3.1 Transformation von Indikatorfunktionen

Definition 1 Für $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ heißt $\vartheta_f : \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{R}$,

$$\vartheta_f(x,y) := \begin{cases} 1, & \text{wenn } y = f(x), \\ 0 & \text{sonst,} \end{cases}$$

Indikatorfunktion von f.

Bestimmen wir die Walsh-Transformation einer solchen; dabei kommt die Menge

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

vor, wo die Funktion $v \cdot f$ mit der durch u bestimmten Linearform übereinstimmt. Je größer die Menge $L_f(u,v)$, desto enger ist die „Approximation“ von f durch die Linearformen zu u und v.

$$\begin{aligned} \hat{\vartheta}_f(u,v) &= \sum_{x\in\mathbb{F}_2^n} \sum_{y\in\mathbb{F}_2^q} \vartheta_f(x,y)(-1)^{u\cdot x+v\cdot y} \\ &= \sum_{x\in\mathbb{F}_2^n} (-1)^{u\cdot x+v\cdot f(x)} \\ &= \#L_f(u,v) - (2^n - \#L_f(u,v)). \end{aligned}$$

Damit ist gezeigt:

Satz 1 *Für eine* Boolesche *Abbildung* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *ist die* Walsh-*Transformation der Indikatorfunktion gegeben durch*

$$\hat{\vartheta}_f(u,v) = \sum_{x\in\mathbb{F}_2^n} (-1)^{u\cdot x+v\cdot f(x)} = 2\cdot \#L_f(u,v) - 2^n.$$

Insbesondere ist $-2^n \le \hat{\vartheta}_f \le 2^n$*, und alle Werte von* $\hat{\vartheta}_f$ *sind gerade.*

Die Herleitung des Satzes ergibt als Zwischenschritt:

Korollar 1 *Ist* $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$ *die durch* v *definierte Linearform, so ist*

$$\hat{\vartheta}_f(u,v) = \hat{\chi}_{\beta\circ f}(u).$$

Definition 2 Für eine BOOLEsche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ heißt die reellwertige Funktion $\hat{\vartheta_f} : \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{R}$ (WALSH-) **Spektrum** von f. Das Maximum

$$\max_{(\mathbb{F}_2^n \times \mathbb{F}_2^q) - \{0\}} |\hat{\vartheta}_f|$$

heißt **Spektralradius** von f.

Man stellt sich das Spektrum $\hat{\vartheta}_f$ von f als $2^n \times 2^q$-Matrix vor, deren Zeilen mit $u \in \mathbb{F}_2^n$ und deren Spalten mit $v \in \mathbb{F}_2^q$ indiziert sind. Die Spalten sind nach dem Korollar 1 gerade die Spektren der BOOLEschen Funktionen $\beta \circ f$ für alle Linearformen $\beta \in \mathcal{L}_q$.

Bemerkungen

1. Da $L_f(0,0) = \mathbb{F}_2^n$, ist $\hat{\vartheta}_f(0,0) = 2^n$. Die obere Grenze in Satz 1 wird also für jedes f angenommen; die untere Grenze wird nur von geeigneten f angenommen.

2. Für $u \neq 0$ ist dagegen

$$\hat{\vartheta}_f(u,0) = \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x} = 0.$$

Die erste Spalte des Spektrums, die „Spalte 0“, hat also die Gestalt $(2^n, 0, \ldots, 0)$.

Korollar 2 (Spaltensummen des Spektrums) *Ist $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$ die durch v definierte Linearform, so ist*

$$\begin{aligned} \sum_{u \in \mathbb{F}_2^n} \hat{\vartheta}_f(u,v) &= \begin{cases} 2^n, & \textit{wenn } \beta \circ f(0) = 0, \\ -2^n & \textit{sonst,} \end{cases} \\ \sum_{u \in \mathbb{F}_2^n} \hat{\vartheta}_f(u,v)^2 &= 2^{2n}. \end{aligned}$$

Beweis. Das folgt aus Korollar 2 zur Umkehrformel in 2.2 bzw. aus Korollar 1 und der PARSEVAL-Gleichung (Satz 4 in 2.3). $\diamond$

Aus Satz 5 in 2.4 folgt ferner

$$\max |\hat{\vartheta}_f(\bullet, v)| = \max |\hat{\chi}_{\beta \circ f}| \geq 2^{n/2} \qquad \text{für jeden Vektor } v \in \mathbb{F}_2^q$$

mit Gleichheit genau dann, wenn $\beta \circ f$ krumm ist. Also:

Korollar 3 *Für den Spektralradius einer* BOOLE*schen Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ gilt*

$$\max_{(\mathbb{F}_2^n \times \mathbb{F}_2^q) - \{0\}} |\hat{\vartheta}_f| \geq 2^{\frac{n}{2}},$$

mit Gleichheit genau dann, wenn $\beta \circ f$ für jede Linearform $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$, $\beta \neq 0$, krumm ist.

Definition 3 (NYBERG, EUROCRYPT 91) Eine Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ heißt **krumm**, wenn ihr Spektralradius gleich $2^{n/2}$ ist.

Bemerkungen

3. Ist f bijektiv (also insbesondere $q = n$), so ist offensichtlich $\vartheta_{f^{-1}}(y,x) = \vartheta_f(x,y)$ für alle $x, y \in \mathbb{F}_2^n$. Die Menge

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

ist das Bild unter f von $L_f(u,v)$; insbesondere ist sie gleich groß. Daher ist auch

$$\hat{\vartheta}_{f^{-1}}(v,u) = \hat{\vartheta}_f(u,v)$$

für alle $u, v \in \mathbb{F}_2^n$. Das Spektrum $\hat{\vartheta}_{f^{-1}}$ ist also transponiert zum Spektrum $\hat{\vartheta}_f$.

4. Im Fall $q = 1$ ist $\hat{\chi}_f(u) = \hat{\vartheta}_f(u,1)$ nach Korollar 1 in 2.1. Insgesamt gilt im Fall $q = 1$ also:

$$\hat{\vartheta}_f(u,v) = \begin{cases} 2^n, & \text{wenn } u = 0,\ v = 0, \\ 0, & \text{wenn } u \neq 0,\ v = 0, \\ \hat{\chi}_f(u), & \text{wenn } v = 1. \end{cases}$$

5. Sei $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ direkte Summe von $g\colon \mathbb{F}_2^r \longrightarrow \mathbb{F}_2^q$ und $h\colon \mathbb{F}_2^s \longrightarrow \mathbb{F}_2^q$. Dann ist für jede Linearform $\beta\colon \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$ auch $\beta \circ f = \beta \circ g \oplus \beta \circ h$. Es folgt

$$\hat{\vartheta}_f(u,v,w) = \hat{\chi}_{\beta\circ f}(u,v) = \hat{\chi}_{\beta\circ g}(u) \cdot \hat{\chi}_{\beta\circ h}(v) = \hat{\vartheta}_g(u,w) \cdot \hat{\vartheta}_h(v,w)$$

für alle $u \in \mathbb{F}_2^r, v \in \mathbb{F}_2^s, w \in \mathbb{F}_2^q$, wenn β die zu w gehörige Linearform ist.

6. Sei $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ affin, also $f(x) = Ax + b$ mit $A \in M_{n,q}(\mathbb{F}_2)$ und $b \in \mathbb{F}_2^q$. Dann ist

$$L_f(u,v) = \{x \in \mathbb{F}_2^n | u^t x = v^t A x + v^t b\} = \{x \in \mathbb{F}_2^n | (u^t - v^t A)x = v^t b\},$$

und das ist der Kern der Linearform $u^t - v^t A$, falls $v^t b = 0$, und parallel dazu, falls $v^t b = 1$. Es gibt also die Fälle

$$\#L_f(u,v) = \begin{cases} 2^n, & \text{falls } v^t A = u^t \text{ und } v^t b = 0, \\ 0, & \text{falls } v^t A = u^t \text{ und } v^t b = 1, \\ 2^{n-1}, & \text{falls } v^t A \neq u^t. \end{cases}$$

Daraus folgt

$$\hat{\vartheta}_f(u,v) = 2 \cdot \#L_f(u,v) - 2^n = \begin{cases} 2^n, & \text{falls } v^t A = u^t \text{ und } v^t b = 0, \\ -2^n, & \text{falls } v^t A = u^t \text{ und } v^t b = 1, \\ 0, & \text{falls } v^t A \neq u^t. \end{cases}$$

Das Spektrum enthält also in jeder Spalte (d. h. bei konstantem v) genau einen Eintrag $\pm 2^n$ und sonst lauter Nullen.

7. Hat umgekehrt das Spektrum von f diese Gestalt, so $\beta \circ f$ affin für alle Linearformen $\beta\colon \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$. Also ist f affin. Damit ist gezeigt:

Satz 2 *Die Abbildung $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ ist genau dann affin, wenn jede Spalte des Spektrums $\hat{\vartheta}_f$ von f genau einen Eintrag $\neq 0$ hat.*

Beispiele

1. Für $f : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2$, $f(x_1, x_2) = x_1 x_2$, erhalten wir mit Bemerkung 4 das Spektrum

	$v =$	
$\hat{\vartheta}_f(u,v)$	0	1
$u = 00$	4	2
01	0	2
10	0	2
11	0	-2

2. Ebenso ergibt sich für $f \in \mathcal{F}_4$, gegeben durch das Polynom $T_1T_2+T_3T_4$, die Wertetabelle

$\hat{\vartheta}_f(u,v)$	$v=$ 0	1
$u=0000$	16	4
0001	0	4
0010	0	4
0011	0	−4
0100	0	4
0101	0	4
0110	0	4
0111	0	−4
1000	0	4
1001	0	4
1010	0	4
1011	0	−4
1100	0	−4
1101	0	−4
1110	0	−4
1111	0	4

3. Und für $f \in \mathcal{F}_3$, gegeben durch das Polynom $T_1T_2 + T_1T_3 + T_2T_3$:

$\hat{\vartheta}_f(u,v)$	$v=$ 0	1
$u=000$	8	0
001	0	4
010	0	4
011	0	0
100	0	4
101	0	0
110	0	0
111	0	−4

4. Ebenso erhalten wir die Werte für die Polynome $T_1 \cdots T_n$ und $(T_1+1)\cdots(T_n+1)$ aus den Beispielen 3 und 4 in 2.7.

5. Der „Halbaddierer“ ist die Abbildung $f : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$ mit den Komponenten-Polynomen $f_1 = T_1T_2$ und $f_2 = T_1 + T_2$. Er ergibt die Wertetabellen

$\vartheta_f(x,y)$	$y=$ 00	01	10	11
$x=00$	1	0	0	0
01	0	1	0	0
10	0	1	0	0
11	0	0	1	0

$\hat{\vartheta}_f(u,v)$	$v=$ 00	01	10	11
$u=00$	4	0	2	−2
01	0	0	2	2
10	0	0	2	2
11	0	4	−2	2

6. Der „Volladdierer“ ist die Abbildung $f : \mathbb{F}_2^3 \longrightarrow \mathbb{F}_2^2$ mit den Komponenten-Polynomen $f_1 = T_1T_2 + T_1T_3 + T_2T_3$ und $f_2 = T_1 + T_2 + T_3$. Er ergibt die Wertetabellen

	$y =$			
$\vartheta_f(x,y)$	00	01	10	11
$x = 000$	1	0	0	0
001	0	1	0	0
010	0	1	0	0
011	0	0	1	0
100	0	1	0	0
101	0	0	1	0
110	0	0	1	0
111	0	0	0	1

	$v =$			
$\hat{\vartheta}_f(u,v)$	00	01	10	11
$u = 000$	8	0	0	-4
001	0	0	4	0
010	0	0	4	0
011	0	0	0	4
100	0	0	4	0
101	0	0	0	4
110	0	0	0	4
111	0	8	-4	0

Satz 3 *Für die Komposition zweier* Boole*scher Abbildungen* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$, $h\colon \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^r$ *gilt:*

$$\hat{\vartheta}_{h\circ f}(u,w) = \frac{1}{2^q} \cdot \sum_{v\in\mathbb{F}_2^q} \hat{\vartheta}_f(u,v)\hat{\vartheta}_h(v,w).$$

Beweis. Das ist eine einfache Umsummierung:

$$\begin{aligned}
\sum_{v\in\mathbb{F}_2^q} \hat{\vartheta}_f(u,v)\hat{\vartheta}_h(v,w) &= \sum_{v\in\mathbb{F}_2^q}\sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q} (-1)^{u\cdot x+v\cdot f(x)+v\cdot y+w\cdot h(y)} \\
&= \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q} (-1)^{u\cdot x+w\cdot h(y)} \cdot \underbrace{\sum_{v\in\mathbb{F}_2^q} (-1)^{v\cdot[f(x)+y]}}_{\begin{cases} 2^q, & \text{falls } y = f(x), \\ 0 & \text{sonst,}\end{cases}} \\
&= 2^q \cdot \sum_{x\in\mathbb{F}_2^n} (-1)^{u\cdot x+w\cdot h(f(x))} \\
&= 2^q \cdot \hat{\vartheta}_{h\circ f}(u,w)
\end{aligned}$$

wie behauptet. $\diamond$

Bemerkungen

8. Ist $h \in GL(\mathbb{F}_2^q)$ eine lineare Transformation des Bildraums, so entsteht $\hat{\vartheta}_{h\circ f}$ aus $\hat{\vartheta}_f$ durch Multiplikation der Wertetabelle von rechts mit einer Permutationsmatrix.

9. Bei einer Verschiebung im Bildraum ändern sich einige Spalten des Spektrums im Vorzeichen: Für $b \in \mathbb{F}_2^q$ gilt

$$\begin{aligned} \vartheta_{f+b}(x,y) &= \vartheta_f(x, y-b), \\ \hat{\vartheta}_{f+b}(u,v) &= (-1)^{v\cdot b}\hat{\vartheta}_f(u,v). \end{aligned}$$

10. Ist $g \in GL(\mathbb{F}_2^n)$ eine lineare Transformation des Urbildraums, so entsteht $\hat{\vartheta}_{f\circ g}$ aus $\hat{\vartheta}_f$ durch Multiplikation des Spektrums von links mit einer Permutationsmatrix.

11. Bei einer Verschiebung im Urbildraum ändern sich einige Zeilen des Spektrums im Vorzeichen: Für $a \in \mathbb{F}_2^n$ und $g(x) = f(x+a)$ gilt

$$\begin{aligned} \vartheta_g(x,y) &= \vartheta_f(x+a, y), \\ \hat{\vartheta}_g(u,v) &= (-1)^{u\cdot a}\hat{\vartheta}_f(u,v). \end{aligned}$$

12. Insbesondere ist der Spektralradius und sein Quadrat $\max \hat{\vartheta}_f^2$ auf $\mathbb{F}_2^n \times \mathbb{F}_2^q - \{(0,0)\}$ invariant unter $GA(\mathbb{F}_2^n) \times GA(\mathbb{F}_2^q)$, also unter affinen Transformationen in Bild und Urbild.

3.2 Urbildzähler und balancierte Abbildungen

Bei der zu Bemerkung 2 in 3.1 analogen Gleichung für $\hat{\vartheta}_f(0,v)$, also die erste Zeile des Spektrums, kommt der **Urbildzähler** $\nu_f : \mathbb{F}_2^q \longrightarrow \mathbb{N}$,

$$\nu_f(y) := \#f^{-1}(y) = \#\{x \in \mathbb{F}_2^n \mid f(x) = y\} = \sum_{x\in\mathbb{F}_2^n} \vartheta_f(x,y),$$

vor:

$$\begin{aligned} \hat{\vartheta}_f(0,v) &= \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q} \vartheta_f(x,y)(-1)^{v\cdot y} \\ &= \sum_{y\in\mathbb{F}_2^q} \nu_f(y)(-1)^{v\cdot y} \\ &= \hat{\nu_f}(v). \end{aligned}$$

Durch Aufsummieren erhält man eine neue Erkenntnis:

$$\sum_{v\in\mathbb{F}_2^q} \hat{\vartheta}_f(0,v) = \sum_{v\in\mathbb{F}_2^q} \hat{\nu}_f(v) = 2^q \cdot \nu_f(0)$$

nach 2.2. Hierbei ist $\nu_f(0)$ die Anzahl der Nullstellen von f. Damit ist bewiesen:

Hilfssatz 1 *Für eine* BOOLE*sche Abbildung* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *gilt:*

$$\begin{aligned} \hat{\vartheta}_f(0, v) &= \hat{\nu}_f(v), \\ \sum_{v \in \mathbb{F}_2^q - \{0\}} \hat{\vartheta}_f(0, v) &= 2^q \cdot \nu_f(0) - 2^n. \end{aligned}$$

Übungsaufgabe. Zeige, dass für jedes $u \in \mathbb{F}_2^n$

$$\sum_{v \in \mathbb{F}_2^q} \hat{\vartheta}_f(u, v) = 2^q \cdot \sum_{x \in V(f)} (-1)^{u \cdot x}$$

ist, wobei $V(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 0\}$ die Nullstellenmenge von f ist.

Eine wichtige Eigenschaft BOOLEscher Abbildungen für kryptologische Anwendungen ist die Balanciertheit – unbalancierte Abbildungen ergeben eine ungleichmäßige Wahrscheinlichkeitsverteilung auf den Geheimtexten und bieten daher einen Ansatz für statistische Angriffe:

Definition 4 Eine Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ heißt **balanciert**, wenn alle Urbildmengen $f^{-1}(y)$ für $y \in \mathbb{F}_2^q$ gleich groß sind.

Bemerkungen

1. f ist genau dann balanciert, wenn der Urbildzähler ν_f konstant ist.

2. Ist f balanciert, so muss f surjektiv sein, insbesondere $n \geq q$, und der Urbildzähler ist konstant $\nu_f = 2^{n-q}$; im Fall $n = q$ sind genau die bijektiven Abbildungen balanciert.

3. Nach Bemerkung 3 in 2.1 und Bemerkung 2 ist f genau dann balanciert, wenn $\hat{\nu}_f(0) = 2^n$ und $\hat{\nu}_f(v) = 0$ für $v \neq 0$, also nach Hilfssatz 1 genau dann, wenn

$$\hat{\vartheta}_f(0, v) = \begin{cases} 2^n & \text{für } v = 0, \\ 0 & \text{sonst.} \end{cases}$$

   Auf diese Weise hängt die Balanciertheit eng mit der ersten Zeile („Zeile 0“) des Spektrums zusammen.

4. Eine BOOLEsche *Funktion* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ ist balanciert, wenn sie die Werte 0 und 1 beide genau 2^{n-1}-mal annimmt; anders ausgedrückt, wenn ihre Wahrheitstafel genau 2^{n-1} Nullen enthält, also wenn $d(f, 0) = 2^{n-1}$ oder $\mathrm{wt}(f) = 2^{n-1}$. Wendet man Korollar 2 in 2.1 speziell auf die Linearform 0 an, so folgt, dass f genau dann balanciert ist, wenn $\hat{\chi}_f(0) = 0$.

5. Aus Hilfssatz 3 in 2.4 und der Tatsache, dass im Fall $n \geq 2$ die Zahl 2^{n-1} der Nullstellen einer balancierten Funktion gerade ist, folgt, dass sie den Grad $\leq n-1$ hat.

6. Ist $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ surjektiv linear, so ist f balanciert, denn die Gleichung $f(x) = 0$ beschreibt den Untervektorraum Kern f der Codimension q, wird also von genau 2^{n-q} Elementen erfüllt. Die anderen Urbildmengen sind die Nebenklassen von Kern f. Allgemeiner ist jede surjektive affine Abbildung balanciert.

7. Für $g \in \mathcal{G}_n, h \in \mathcal{G}_q$ und $\tilde{f} = \omega_{(g,h)} f$ gilt offensichtlich $\nu_{\tilde{f}}(y) = \nu_f(h^{-1}y)$: Beliebige Transformationen von $\mathbb{F}_2^n$ lassen den Urbildzähler ungeändert, Transformationen von $\mathbb{F}_2^q$ permutieren seine Werte.

8. Die Balanciertheit von f ist invariant unter Bijektionen von $\mathbb{F}_2^n$ und $\mathbb{F}_2^q$, also unter der gesamten Gruppe $\mathcal{G}_n \times \mathcal{G}_q$ aus Abschnitt 1.5.

9. Die Funktion $f : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2$, $f(x_1, x_2) = x_1 x_2$, ist nicht balanciert, da sie drei Nullstellen hat. Nach Bemerkung 7 und 1.5, Beispiel 4, ist also keine der quadratischen Funktionen in $\mathcal{F}_2$ balanciert. Daher gibt es in $\mathcal{F}_2$ nur sechs balancierte Funktionen: die nichtkonstanten affinen.

10. Da es insgesamt 2^n Urbilder gibt, ist

$$\sum_{y \in \mathbb{F}_2^q} \nu_f(y) = 2^n.$$

11. Ist $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ eine *beliebige* BOOLEsche Funktion, so ist die einfache Erweiterung $\breve{f} : \mathbb{F}_2^{n+1} \longrightarrow \mathbb{F}_2$ balanciert. Denn da

$$\breve{f}(1, x_1, \ldots, x_n) = 1 + \breve{f}(0, x_1, \ldots, x_n),$$

werden die Werte 0 und 1 gleich oft angenommen.

12. Eine quadratische Form $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ ist genau dann balanciert, wenn f vom Typ $Q_{III}(m)$ ist, bzw. wenn $f|_{\mathrm{Rad}_f}$ nicht konstant ist.

Satz 4 (SEBERRY/ZHANG/ZHENG, EUROCRYPT 94) *Eine* BOOLE*sche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ ist genau dann balanciert, wenn für jede Linearform $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$, $\beta \neq 0$, die Linearform $\beta \circ f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ balanciert ist.*

Beweis. Wenn f balanciert ist, ist offensichtlich jede Komponentenfunktion $f_1, \ldots f_q : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ balanciert. Eine beliebige Linearform $\beta \neq 0$ lässt sich durch einen linearen Automorphismus h von $\mathbb{F}_2^q$ auf die erste Koordinate abbilden; also ist $\beta \circ f$ ebenfalls balanciert.

Umgekehrt ist zu zeigen, dass der Urbildzähler $\nu_f = 2^{n-q}$ konstant ist.

Nach Bemerkung 4 und Korollar 1 zu Satz 1 ist für $v \in \mathbb{F}_2^q - \{0\}$ stets $\hat{\vartheta}_f(0,v) = \hat{\chi}_{v\cdot f}(0) = 0$. Da außerdem $\hat{\vartheta}_f(0,0) = 2^n$, folgt die Behauptung aus Bemerkung 3. $\diamond$

Korollar 1 *Ist* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *balanciert, so* $\operatorname{Grad} f \leq n-1$.

Beweis. Das gilt nach Bemerkung 5 für jede Komponentenfunktion. $\diamond$

Der nächste Satz drückt die Balanciertheit durch das Faltungsquadrat des Urbildzählers ν_f aus:

Satz 5 *Für eine Abbildung* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *sind äquivalent:*
(i) f *ist balanciert.*
(ii) $\nu_f * \nu_f = 2^{2n-q}$ *konstant.*
(iii) $\nu_f * \nu_f(0) = 2^{2n-q}$.

Beweis. „(i) $\Longrightarrow$ (ii)“ ist fast trivial:

$$\nu_f * \nu_f(v) = \sum_{y\in\mathbb{F}_2^q} \nu_f(y)\nu_f(v+y) = 2^q \cdot 2^{n-q} \cdot 2^{n-q} = 2^{2n-q}.$$

„(ii) $\Longrightarrow$ (iii)“ ist die Einschränkung auf einen Spezialfall.
„(iii) $\Longrightarrow$ (i)“: Es ist

$$\begin{aligned} 2^{2n-q} = \nu_f * \nu_f(0) &= \sum_{y\in\mathbb{F}_2^q} \nu_f(y)^2, \\ 2^n &= \sum_{y\in\mathbb{F}_2^q} \nu_f(y). \end{aligned}$$

Die Cauchy-Schwarz-Ungleichung ergibt

$$2^{2n} = \left[\sum_{y\in\mathbb{F}_2^q} 1\cdot\nu_f(y)\right]^2 \leq \sum_{y\in\mathbb{F}_2^q} 1^2 \cdot \sum_{y\in\mathbb{F}_2^q} \nu_f(y)^2 = 2^q \cdot 2^{2n-q}.$$

Die Gleichheit impliziert, dass $\nu_f(y)$ ein konstantes Vielfaches von 1, also konstant ist. $\diamond$

3.3 Krumme Abbildungen

Einige einfache Folgerungen aus der Definition 3 von krummen Abbildungen sind:

Bemerkungen

1. Nach den Korollaren zu Satz 1 ist $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ genau dann krumm, wenn

$$\hat{\vartheta}_f(u,v) = \pm 2^{n/2} \qquad \text{für alle } u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^q - \{0\},$$

   d. h., wenn das Spektrum (ausser in der ersten Spalte) nur die Werte $\pm 2^{n/2}$ annimmt.

2. Wenn eine krumme Abbildung existiert, muss n nach Korollar 1 zu Satz 5 in 2.4 gerade sein.

3. Wie im Fall $q = 1$ gilt auch allgemein: Ist f krumm und g affin, so ist $f + g$ krumm. Für jede Linearform $\beta \neq 0$ auf $\mathbb{F}_2^q$ ist nämlich $\beta \circ f$ krumm, $\beta \circ g$ affin und $\beta \circ (f + g) = \beta \circ f + \beta \circ g$.

4. Nach Bemerkung 12 in 3.1 ist die Eigenschaft „krumm“ invariant unter affinen Transformationen von Bild und Urbild.

5. Nach Satz 6 in 2.4 folgt auch allgemein für krumme Abbildungen, dass der algebraische Grad $\leq \frac{n}{2}$ ist.

6. Sie $f = g \oplus h$ direkte Summe. Dann ist f genau dann krumm, wenn alle $\beta \circ f$ krumm sind, also alle $\beta \circ g$ und $\beta \circ h$, also genau dann, wenn g und h krumm sind. (Nach Satz 9 in 2.8.)

Satz 6 (Nyberg, Eurocrypt 91) *Eine krumme Abbildung $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ existiert genau dann, wenn $n \geq 2q$ und gerade ist.*

Beweis. Es gebe eine krumme Abilsung f. Das Spektrum $\hat{\vartheta}_f$ nimmt für $v \neq 0$ nur die Werte $\pm 2^{n/2}$ an; sei

$$r := \#\{v \in \mathbb{F}_2^q - \{0\} \mid \hat{\vartheta}_f(0,v) = +2^{n/2}\}.$$

Für die Summe $S := \sum_{v \in \mathbb{F}_2^q - \{0\}} \hat{\vartheta}_f(0,v)$ folgt dann

$$S = 2^{n/2} \cdot [r - (2^q - 1 - r)] = 2^{n/2} \cdot [2r - 2^q + 1].$$

Andererseits ist nach dem Hilfssatz 1

$$S = 2^q \cdot \nu_f(0) - 2^n,$$

$$\nu_f(0) = \frac{S + 2^n}{2^q} = 2^{\frac{n}{2}-q} \cdot [2r - 2^q + 2^{n/2} + 1].$$

Da der Faktor in eckigen Klammern ungerade ist, kann $\nu_f(0)$ nur dann eine ganze Zahl sein, wenn $2^{\frac{n}{2}-q}$ ganz, also $\frac{n}{2} \geq q$ ist.

Für die umgekehrte Richtung nehmen wir $n = 2m \geq 2q$ gerade an. Der Vektorraum $\mathbb{F}_2^m$ wird mit einer passenden Multiplikation als Körper

$\mathbb{F}_{2^m}$ interpretiert. Seien $a_1, \ldots, a_q \in \mathbb{F}_2^m$ über $\mathbb{F}_2$ linear unabhängig. Die Komponenten $f_1, \ldots, f_q$ der Abbildung $f\colon \mathbb{F}_2^m \times \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^q$ werden dann so definiert:

$$f_i(x, y) = a_i x \cdot y \quad \text{für } x, y \in \mathbb{F}_2^m,$$

wobei das Produkt $a_i x$ im Körper $\mathbb{F}_{2^m}$ gebildet wird; das ist ein Spezialfall der MAIORANA-MCFARLAND-Konstruktion, Satz 7 in Abschnitt 2.4. Insbesondere sind die f_i krumme Funktionen. Ist nun $\beta\colon \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$ eine beliebige Linearform $\neq 0$ und $\beta(z) = b_1 z_1 + \cdots + b_q z_q$, so ist

$$\beta \circ f(x, y) = (b_1 a_1 + \cdots b_q a_q) x \cdot y$$

ebenfalls eine MAIORANA-MCFARLAND-Funktion, also krumm. $\diamond$

3.4 Das Linearitätsprofil

Sei $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ eine BOOLEsche Abbildung. In Abschnitt 3.1 wurden für $u \in \mathbb{F}_2^n$, $v \in \mathbb{F}_2^q$ die Mengen $L_f(u, v)$ eingeführt. Nach dieser Definition und Satz 1 ist

$$\#L_f(u, v) = 2^n - d(\alpha, \beta \circ f) = 2^{n-1} + \frac{1}{2}\,\hat{\vartheta}_f(u, v),$$

wenn α und β die durch das Skalarprodukt mit u bzw. v definierten Linearformen sind. Als Bezeichnungen werden weiterhin verwendet:

$$\begin{aligned} p_f(u, v) &:= \frac{\#L_f(u, v)}{2^n} = 1 - \frac{d(\alpha, \beta \circ f)}{2^n} = \frac{1}{2} + \frac{\hat{\vartheta}_f(u, v)}{2^{n+1}}, \\ \lambda_f(u, v) &:= (2p_f(u, v) - 1)^2 = \frac{1}{2^{2n}} \cdot \hat{\vartheta}_f(u, v)^2. \end{aligned}$$

Definition 5 Die Funktion

$$\lambda_f : \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{Q}$$

heißt **Linearitätsprofil** von f. Die Größen $p_f(u, v)$ und $\lambda_f(u, v)$ heißen **Wahrscheinlichkeit** bzw. **Potenzial** der linearen Relation $(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^q$ für f.

Anmerkung. Die Verwendung des Quadrats bei der Definition des Linearitätsprofils wurde von MATSUI 1999 eingeführt und erweist sich als sehr sinnvoll. Nicht üblich, aber, wie sich zeigen wird, ebenfalls sinnvoll, ist die Normierung mit dem Faktor $\frac{1}{2^{2n}}$.

Bemerkungen

1. Es gilt stets
$$0 \leq \lambda_f(u,v) \leq 1,$$
$$p_f(u,v) = \frac{1 \pm \sqrt{\lambda_f(u,v)}}{2},$$
und nach Satz 1 in 3.1 sind alle Werte von λ_f ganzzahlige Vielfache von $\frac{1}{2^{2n-2}}$.

2. Für $v = 0$ gilt $v \cdot f(x) = u \cdot x$ genau dann, wenn x in der durch $u \cdot x = 0$ beschriebenen Hyperebene liegt. Also ist
$$\begin{aligned} \#L_f(u,0) &= \begin{cases} 2^n, & \text{wenn } u = 0, \\ 2^{n-1} & \text{sonst,} \end{cases} \\ p_f(u,0) &= \begin{cases} 1, & \text{wenn } u = 0, \\ \frac{1}{2} & \text{sonst,} \end{cases} \\ \lambda_f(u,0) &= \begin{cases} 1, & \text{wenn } u = 0, \\ 0 & \text{sonst.} \end{cases} \end{aligned}$$
(„Erste Spalte“ des Linearitätsprofils; auch aus 3.1 klar.)

3. Alle „Spaltensummen“ des Linearitätsprofils sind 1:
$$\sum_{u \in \mathbb{F}_2^n} \lambda_f(u,v) = 1.$$
Das folgt aus Korollar 2 zu Satz 1 in 3.1. Insbesondere gibt es zu jedem $v \in \mathbb{F}_2^q$ ein $u \in \mathbb{F}_2^n$ mit $\lambda_f(u,v) \geq \frac{1}{2^n}$.

4. Ebenso folgt aus 3.1, dass die „erste Zeile“ des Linearitätsprofils aus den Einträgen $\hat{\nu}_f(v)^2/2^{2n}$ besteht, und aus 3.2 dass f genau dann balanciert ist, wenn diese Zeile die Form $10\ldots0$ hat. Ferner ist f genau dann krumm, wenn alle Spalten außer der ersten konstant $= \frac{1}{2^n}$ sind.

5. Ist f bijektiv, so folgt aus Bemerkung 3 in 3.1, dass
$$p_{f^{-1}}(v,u) = p_f(u,v), \qquad \lambda_{f^{-1}}(v,u) = \lambda_f(u,v)$$
für alle $u, v \in \mathbb{F}_2^n$. Insbesondere ist das Linearitätsprofil von f^{-1} (als Matrix geschrieben) das Transponierte des Linearitätsprofils von f. Ferner sind auch alle Zeilensummen des Linearitätsprofils einer bijektiven Abbildung f gleich 1; dieses ist also eine doppelt stochastische Matrix.

6. Ist $p_f(u,v) > \frac{1}{2}$, so wird durch das Skalarprodukt $u \cdot x$ die Parität von $v \cdot f(x)$ besser als durch bloßes Raten geschätzt, das mit Wahrscheinlichkeit $\frac{1}{2}$ das richtige Bit trifft. Im Falle $p_f(u,v) < \frac{1}{2}$ ist die Schätzung

schlechter als bloßes Raten, aber dann ergibt die Negation $u \cdot x + 1$ eine überzufällig gute Schätzung. Insgesamt ist eine lineare Relation (u, v) „nutzbar für die lineare Kryptoanalyse“, wenn $p_f(u, v) \neq \frac{1}{2}$, also wenn $\lambda_f(u, v) > 0$.

7. Die Relation $(0, 0)$ hat zwar die Wahrscheinlichkeit 1, ist aber natürlich „nutzlos“; sie sagt nichts über f aus.

8. Nach Bemerkung 12 in 3.1 ändert sich bei affiner Transformation in Bild und Urbild das Linearitätsprofil jeweils um eine Permutation der Spalten bzw. Zeilen.

9. Ist $f = g \oplus h$ direkte Summe, so

$$\lambda_f(x, y, z) = \frac{1}{2^{2n}} \cdot \hat{\vartheta}_f(x, y, z)^2 = \frac{1}{2^{2r}} \cdot \hat{\vartheta}_g(x, z)^2 \cdot \frac{1}{2^{2s}} \cdot \hat{\vartheta}_h(y, z)^2$$
$$= \lambda_g(x, z) \cdot \lambda_h(y, z)$$

für alle $x \in \mathbb{F}_2^r$, $y \in \mathbb{F}_2^s$, $z \in \mathbb{F}_2^q$.

Beispiele

1. Ist f linear, so gibt es zu jedem $v \in \mathbb{F}_2^q$ ein $u \in \mathbb{F}_2^n$ mit $\lambda_f(u, v) = 1$, nämlich den Vektor, der die Linearform $v \cdot f$ definiert. Die anderen Einträge $\lambda_f(u, v)$ dieser Zeile des Linearitätsprofils müssen dann 0 sein.

2. Ist f affin, so gibt es ebenfalls zu jedem $v \in \mathbb{F}_2^q$ ein $u \in \mathbb{F}_2^n$ mit $\lambda_f(u, v) = 1$: Ist $f(x) = Ax + b$, so

$$p_f(u, v) = \begin{cases} 1, & \text{falls } v^t A = u^t \text{ und } v^t b = 0, \\ 0, & \text{falls } v^t A = u^t \text{ und } v^t b = 1, \\ \frac{1}{2}, & \text{falls } v^t A \neq u^t, \end{cases}$$

$$\lambda_f(u, v) = \begin{cases} 1, & \text{falls } v^t A = u^t, \\ 0, & \text{falls } v^t A \neq u^t. \end{cases}$$

3. Umgekehrt folgt, wenn das Linearitätsprofil in jeder Spalte genau einen Wert $\neq 0$ hat, dass f affin sein muss, siehe Satz 2 in 3.1.

4. Für $f : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2$, $f(x_1, x_2) = x_1 x_2$, ergibt sich das Linearitätsprofil am einfachsten aus der Gleichung $\lambda_f = \frac{1}{16} \hat{\vartheta}_f^2$:

$\lambda_f(u, v)$	0	1
00	1	$\frac{1}{4}$
01	0	$\frac{1}{4}$
10	0	$\frac{1}{4}$
11	0	$\frac{1}{4}$

5. Weitere Beispiele kann man ebenfalls direkt den Wertetabellen für $\hat{\vartheta}_f$ aus 3.1 entnehmen, so für den Volladdierer:

$\lambda_f(u,v)$	00	01	10	11
000	1	0	0	$\frac{1}{4}$
001	0	0	$\frac{1}{4}$	0
010	0	0	$\frac{1}{4}$	0
011	0	0	0	$\frac{1}{4}$
100	0	0	$\frac{1}{4}$	0
101	0	0	0	$\frac{1}{4}$
110	0	0	0	$\frac{1}{4}$
111	0	1	$\frac{1}{4}$	0

6. Für die „affinen Normalformen“ der Abbildungen $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$ aus 1.5,

$$\binom{0}{0}, \binom{T_1}{0}, \binom{T_1}{T_2}, \binom{T_1T_2}{0}, \binom{T_1T_2}{T_2},$$

sind die Linearitätsprofile der Reihe nach:

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

	00	01	10	11
00	1	1	0	0
01	0	0	0	0
10	0	0	1	1
11	0	0	0	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	1	$\frac{1}{4}$	$\frac{1}{4}$
01	0	0	$\frac{1}{4}$	$\frac{1}{4}$
10	0	0	$\frac{1}{4}$	$\frac{1}{4}$
11	0	0	$\frac{1}{4}$	$\frac{1}{4}$

	00	01	10	11
00	1	0	$\frac{1}{4}$	$\frac{1}{4}$
01	0	1	$\frac{1}{4}$	$\frac{1}{4}$
10	0	0	$\frac{1}{4}$	$\frac{1}{4}$
11	0	0	$\frac{1}{4}$	$\frac{1}{4}$

3.5 Das lineare Potenzial

Die Größe

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

bezeichnet das maximale Potenzial einer nichttrivialen linearen Relation. Je größer es ist, desto „näher“ an der Linearität ist f. Um „möglichst nichtlineare“ Abbildungen zu konstruieren, wird man also versuchen, Λ_f möglichst klein zu halten. Λ_f ist das Linearitätsmaß der linearen Kryptoanalyse.

Definition 6 Für eine BOOLEsche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ heißt Λ_f das **lineare Potenzial** von f.

Bemerkungen

1. Es ist stets $0 \leq \Lambda_f \leq 1$. Ist f affin, so ist $\Lambda_f = 1$. Insbesondere ist im Fall $n = 1$, q beliebig, stets $\Lambda_f = 1$.

2. Es ist
$$\Lambda_f = \frac{1}{2^{2n}} \cdot \max_{(\mathbb{F}_2^n \times \mathbb{F}_2^q) - \{(0,0)\}} \hat{\vartheta}_f^2.$$
(Das lineare Potenzial ist das umnormierte Quadrat des Spektralradius.) Insbesondere ist Λ_f unter affinen Transformationen von Bild und Urbild invariant.

3. Im Fall $q = 1$ ist
$$\Lambda_f = \frac{1}{2^{2n}} \cdot \max \hat{\chi}_f^2.$$

4. Allgemein gilt für $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$
$$\Lambda_f = \frac{1}{2^{2n}} \cdot \max_{\beta \in \mathcal{L}_q - \{0\}} \hat{\chi}_{\beta \circ f}^2 = \max_{\beta \in \mathcal{L}_q - \{0\}} \Lambda_{\beta \circ f}.$$

5. Weiter gilt im Fall $q = 1$ für eine direkte Summe $f = g \oplus h$, dass
$$\lambda_f(x, y, a) = \lambda_g(x, a) \cdot \lambda_h(y, a)$$
für $x \in \mathbb{F}_2^r$, $y \in \mathbb{F}_2^s$, $a \in \mathbb{F}_2$. Also ist $\Lambda_f = \Lambda_g \cdot \Lambda_h$. (Die Verallgemeinerung auf höhere Dimensionen q des Bildraums klappt so nicht!)

6. Ist f bijektiv, so $\Lambda_{f^{-1}} = \Lambda_f$.

Aus Korollar 3 zu Satz 1 in 3.1 oder Bemerkung 3 in 3.4 folgt also:

Satz 7 (CHABAUD/VAUDENAY, EUROCRYPT 94) *Für jede* BOOLE*sche Abbildung* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *ist*
$$\Lambda_f \geq \frac{1}{2^n};$$
die Gleichheit gilt genau dann, wenn f *krumm ist.*

Die krummen Abbildungen sind also die „möglichst nichtlinearen“ Abbildungen bezüglich des Maßes Λ_f. Sie existieren allerdings höchstens im Fall $n \geq 2q$ gerade. Im Fall $q < n < 2q$ oder n ungerade ist die Minimierung von Λ_f komplizierter, z. T. sogar noch ein offenes Problem, siehe Kapitel 5.

Korollar 1 *Ist f nicht krumm und $n \geq 2$, so ist*

$$\Lambda_f \geq \frac{1}{2^n} + \frac{1}{2^{2n-2}}.$$

Insbesondere gilt das stets, wenn die Dimension n ungerade oder $n < 2q$ ist.

Beweis. Λ_f muss $> \frac{1}{2^n}$ und ganzzahliges Vielfaches von $\frac{1}{2^{2n-2}}$ sein. $\diamond$

Beispiele

1. Für $f : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2$, $f(x_1, x_2) = x_1 x_2$, ist $\Lambda_f = \frac{1}{4}$, da f krumm. Das passt auch zum Linearitätsprofil aus 3.4.

2. Wir betrachten die Abbildung

$$f : \mathbb{F}_2^3 \longrightarrow \mathbb{F}_2, \qquad f(x_1, x_2, x_3) = x_1 x_2 + x_1 x_2 x_3 + x_3$$

Die Wahrheitstafel von f und den 8 möglichen Linearformen zu den Vektoren $u \in \mathbb{F}_2^3$ sieht so aus:

		$u =$							
x	$f(x)$	000	001	010	011	100	101	110	111
000	0	0	0	0	0	0	0	0	0
001	1	0	1	0	1	0	1	0	1
010	0	0	0	1	1	0	0	1	1
011	1	0	1	1	0	0	1	1	0
100	0	0	0	0	0	1	1	1	1
101	1	0	1	0	1	1	0	1	0
110	1	0	0	1	1	1	1	0	0
111	1	0	1	1	0	1	0	0	1

Daraus ergeben sich Wahrscheinlichkeiten und Potenziale (hier „zu Fuß“ bestimmt, ohne Verwendung von ϑ_f):

$p_f(u,v)$	0	1
000	1	$\frac{3}{8}$
001	$\frac{1}{2}$	$\frac{7}{8}$
010	$\frac{1}{2}$	$\frac{5}{8}$
011	$\frac{1}{2}$	$\frac{5}{8}$
100	$\frac{1}{2}$	$\frac{5}{8}$
101	$\frac{1}{2}$	$\frac{5}{8}$
110	$\frac{1}{2}$	$\frac{3}{8}$
111	$\frac{1}{2}$	$\frac{3}{8}$

$\lambda_f(u,v)$	0	1
000	1	$\frac{1}{16}$
001	0	$\frac{9}{16}$
010	0	$\frac{1}{16}$
011	0	$\frac{1}{16}$
100	0	$\frac{1}{16}$
101	0	$\frac{1}{16}$
110	0	$\frac{1}{16}$
111	0	$\frac{1}{16}$

Das maximale Potenzial $\Lambda_f = \lambda_f(001, 1) = \frac{9}{16}$ ist also durch die dritte Koordinate gegeben: *Es gilt* $f(x_1, x_2, x_3) = x_3$ *mit Wahrscheinlichkeit* $\frac{7}{8}$. Insbesondere ist f nicht krumm.

3. Beim Halbaddierer und beim Volladdierer ist das lineare Potenzial 1, repräsentiert durch die 1 am Ende der zweiten Spalte des Linearitätsprofils. Das ist aber auch kein Wunder, da beide Abbildungen ja eine lineare Koordinatenfunktion haben: $T_1 + T_2$ bzw. $T_1 + T_2 + T_3$.

4. Ebenso ist für alle reduzierten Normalformen von Abbildungen $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$ das lineare Potenzial 1. Daher ist 1 auch der kleinstmögliche Wert von Λ_f für *beliebige* Abbildungen $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$. Man sollte für Bitblock-Chiffren keine 2×2-S-Boxen verwenden.

5. Für alle drei Typen $Q_x(m)$ von quadratischen Formen folgt

$$\Lambda_f = \frac{1}{2^{2m}}.$$

Also gilt:

Satz 8 *Sei* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ *quadratische Form vom Rang* r*. Dann ist das lineare Potenzial* $\Lambda_f = \frac{1}{2^r}$.

Ist $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ eine quadratische Abbildung, so ist für jede Linearform $\beta\colon \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$ auch $\beta \circ f$ quadratisch. Sei $r_\beta := \operatorname{Rang} \beta \circ f$. Dann ist

$$\Lambda_f = \max_{\beta \in \mathcal{L}_q - \{0\}} \Lambda_{\beta \circ f} = \max_{\beta \in \mathcal{L}_q - \{0\}} \frac{1}{2^{r_\beta}} = \frac{1}{2^s}$$

mit $s := \min_\beta r_\beta$. Man beachte, dass $\operatorname{Rang} f = \max_\beta r_\beta$.

Satz 9 (i) *Ist* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *eine quadratische Abbildung, so*

$$\Lambda_f = \frac{1}{2^s}$$

mit $0 \le s \le \operatorname{Rang} f \le n$*. Ist* f *nicht krumm, so*

$$\Lambda_f \ge \frac{1}{2^{n-1}}.$$

(ii) *Ist* f *quadratisch und balanciert, so*

$$\Lambda_f \ge \begin{cases} \frac{1}{2^{n-1}} & \text{wenn } n \text{ ungerade,} \\ \frac{1}{2^{n-2}} & \text{wenn } n \text{ gerade.} \end{cases}$$

Beweis. (i) wurde oben gezeigt. (ii) folgt, weil nach Bemerkung 12 in 3.2 alle $\beta \circ f$ vom Typ $Q_{III}(m)$ sind, also insbesondere alle $r_\beta \le n-1$. Ist n gerade, so müssen sogar alle $r_\beta \le n-2$ sein. $\diamond$

3.6 Die Nichtlinearität BOOLEscher Abbildungen

Definition 7 (i) (PIEPRZYK/FINKELSTEIN 1988) Die **Nichtlinearität** einer BOOLEschen Funktion $f: \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ ist die HAMMING-Distanz

$$\sigma_f := d(f, \mathcal{A}_n)$$

zum Unterraum der affinen Funktionen.

(ii) (NYBERG 1992) Für eine Abbildung $f : \mathbb{F}_2^n \longrightarrow F_2^q$ ist die **Nichtlinearität** definiert als

$$\sigma_f := \min\{\sigma_{\beta \circ f} \mid \beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2 \text{ affin}, \beta \neq 0\}.$$

Bemerkungen

1. σ_f ist invariant unter affinen Transformationen im Bild- und Urbildbereich, also unter $GA_n \times GA_q$.
2. $\sigma_f = \min\{d(\beta \circ f, \alpha) \mid \alpha \in \mathcal{A}_n, \beta \in \mathcal{A}_q - \{0\}\}$.

Hilfssatz 2 *Die Nichtlinearität einer* BOOLE*schen Funktion* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ *ist*

$$\sigma_f = 2^{n-1} - \frac{1}{2} \max |\hat{\chi}_f|.$$

Beweis. Sei α die lineare, $\bar{\alpha}$ die nichtlineare affine Funktion zu $u \in \mathbb{F}_2^n$. Dann gilt nach Korollar 2 in 2.1

$$\begin{aligned} d(f, \alpha) &= 2^{n-1} - \frac{1}{2}\hat{\chi}_f(u), \\ d(f, \bar{\alpha}) &= 1 - d(f, \alpha) = 2^{n-1} + \frac{1}{2}\hat{\chi}_f(u), \\ d(f, \{\alpha, \bar{\alpha}\}) &= 2^{n-1} - \frac{1}{2}|\hat{\chi}_f(u)|. \end{aligned}$$

Daraus folgt die Behauptung. $\diamond$

Satz 10 *Die Nichtlinearität einer* BOOLE*schen Abbildung* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *ist*

$$\sigma_f = 2^{n-1} - \frac{1}{2} \max |\hat{\vartheta}_f|,$$

wobei das Maximum über $\mathbb{F}_2^n \times \mathbb{F}_2^q - \{(0,0)\}$ *gebildet wird.*

Beweis. Das folgt aus Hilfssatz 2 mit dem Korollar 1 in 3.1 und weil die Punkte $(u, 0)$ nichts am Maximum ändern. $\diamond$

Da das Linearitätsprofil $\lambda_f = \frac{1}{2^{2n}}\hat{\vartheta}_f^2$ ist, folgt daraus für das lineare Potenzial:

Korollar 1 (i) $\sigma_f = 2^{n-1} \cdot (1 - \sqrt{\Lambda_f}), \quad \Lambda_f = \left(1 - \frac{1}{2^{n-1}}\sigma_f\right)^2$.

(ii) (Meier/Staffelbach, Eurocrypt 89, im Fall $q = 1$)

$$\sigma_f \leq 2^{n-1} - 2^{\frac{n}{2}-1},$$

mit Gleichheit genau dann, wenn f krumm ist.

(iii) *Ist f bijektiv, so $\sigma_{f^{-1}} = \sigma_f$.*

Insbesondere ist die Nichtlinearität kein wirklich neues Maß. (In Wirklichkeit ist sie das ältere Maß.)

Da σ_f stets ganzzahlig sein muss, ergeben sich für kleine n folgende Schranken (die für beliebiges q gelten):

n	1	2	3	4	5	6	7	8	9
$\sigma_f \leq$	0	1	2	6	13	28	58	120	244

Daraus ergibt sich für $n = 3$ die schärfere untere Schranke $\Lambda_f \geq \frac{1}{4}$. Für $n = 5, 7, \ldots$ werden die entsprechend verschärften unteren Schranken $\frac{9}{256}, \frac{9}{1024}, \ldots$ zunehmend uninteressanter.

Ist n gerade und f nicht krumm, so haben wir entsprechend die Schranken

n	2	4	6	8
$\sigma_f \leq$	0	5	27	119
$\Lambda_f \geq$	1	$\frac{9}{64}$	$\frac{25}{1024}$	$\frac{81}{16384}$

Da $\chi_f(u) = \pm 2^{n/2}$, wenn f eine krumme Funktion ist, folgt aus dem Korollar 2 in 2.1:

Korollar 2 *Ist f krumme Funktion, α affin, so*

$$d(f, \alpha) = 2^{n-1} \pm 2^{\frac{n}{2}-1}.$$

Korollar 3 *Ist f krumme Funktion, so hat f genau $2^{n-1} \pm 2^{\frac{n}{2}-1}$ Nullstellen; insbesondere ist f nicht balanciert.*

Beweis. $d(f, 0) = 2^{n-1} \pm 2^{\frac{n}{2}-1} \neq 2^{n-1}$. $\diamond$

Korollar 4 *Ist n gerade, so gibt es eine balancierte Funktion $f \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ mit Nichtlinearität $\sigma_f = 2^{n-1} - 2^{\frac{n}{2}}$ und linearem Potenzial $\Lambda_f = \frac{1}{2^{n-2}}$.*

Beweis. Man nehme eine krumme Funktion und ändere sie an $2^{\frac{n}{2}-1}$ Stellen. Da dann

$$\Lambda_f = \left(1 - \frac{1}{2^{n-1}}\sigma_f\right)^2 = \left(1 - 1 + \frac{1}{2^{\frac{n}{2}-1}}\right)^2 = \frac{1}{2^{n-2}},$$

folgt auch die zweite Aussage. $\diamond$

Beispiele

1. Im Fall $n = 2$, $q = 1$, $f(x_1, x_2) = x_1x_2$, ist $\sigma_f = 2 - 1 = 1$, da f krumm.
2. Im Fall $n = 3$, $f = T_1T_2T_3 + T_1T_2 + T_3$, ist $\sigma_f = 1$.
3. Ist $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ quadratische Form vom Rang r, so

$$\sigma_f = 2^{n-1} \cdot (1 - \frac{1}{2^{r/2}}) = 2^{n-1} - 2^{n-\frac{r}{2}-1}.$$

Ist $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ direkte Summe (siehe 2.8) von $g : \mathbb{F}_2^r \longrightarrow \mathbb{F}_2$ und $h\colon \mathbb{F}_2^s \longrightarrow \mathbb{F}_2$, so ist

$$\begin{aligned} 2^n - 2\sigma_f &= \max|\hat{\chi}_f| = \max|\hat{\chi}_g| \cdot \max|\hat{\chi}_h| = (2^r - 2\sigma_g)(2^s - 2\sigma_h) \\ &= 2^n - 2^r \cdot 2\sigma_h - 2^s \cdot 2\sigma_g + 4\sigma_g\sigma_h. \end{aligned}$$

Korollar 5 *Ist f direkte Summe von g und h, so*

$$\begin{aligned} \sigma_f &= 2^s \cdot \sigma_g + 2^r \cdot \sigma_h - 2\sigma_g\sigma_h, \\ \sigma_f &\geq 2^r \cdot \sigma_h, \\ \sigma_f &\geq 2^s \cdot \sigma_g. \end{aligned}$$

Beweis. Die erste Aussage wurde in der Vorbemerkung gezeigt. Die Abschätzungen folgen, da etwa $2\sigma_g \leq 2^r$. $\diamond$

Bemerkungen

3. Ist f direkte Summe von g und h, und ist h affin, so $\sigma_h = 0$, also $\sigma_f = 2^s\sigma_g$.
4. Als Spezialfall der Bemerkung 3 folgt: Ist $\breve{f} : \mathbb{F}_2^{n+1} \longrightarrow \mathbb{F}_2$ einfache Erweiterung von $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$, so $\sigma_{\breve{f}} = 2\sigma_f$ und $\Lambda_{\breve{f}} = (1 - \frac{1}{2^n}2\sigma_f)^2 = \Lambda_f$.

Startet man für ungerade Dimension n mit einer krummen Funktion $g\colon \mathbb{F}_2^{n-1} \longrightarrow \mathbb{F}_2$, so folgt durch einfache Erweiterung von g:

Korollar 6 *Für jede ungerade Dimension n gibt es eine balancierte Funktion $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ mit $\sigma_f = 2^{n-1} - 2^{\frac{n-1}{2}}$, $\Lambda_f = \frac{1}{2^{n-1}}$.*