Booleovské funkce - první část

Definice. Zobrazení $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ se nazývá *booleovská funkce*. V případě $m = 1$ mluvíme o *binární booleovské funkci*.

Podle definice je booleovská funkce libovolné zobrazení mocnin dvouprvkového tělesa. Tento obecný pojem zahrnuje zpravidla všechny stavební kameny symetrických blokových šifer: S-boxy, vrstvy kol, šifrovací zobrazení kol (pro daný kolový klíč) nebo celý šifrovací algoritmus (pro daný šifrovací klíč). Teorie booleovských funkcí je důležitým nástrojem kryptoanalýzy symetrických šifrovacích algoritmů.

Definice. Na množině všech binárních booleovských funkcí $\mathbb{F}_2^n \to \mathbb{F}_2$ můžeme pomocí operací dvouprvkového tělesa definovat sčítání a násobení (takzvaně 'po bodech'):

$$(f+g)(v) = f(v) + g(v)$$
$$(f \cdot g)(v) = f(v) \cdot g(v)$$

Získáme tím *okruh binárních booleovských funkcí*, který budeme značit R_n.

Lze přímočaře ověřit, že R_n je komutativní okruh, jehož nulový a jednotkový prvek jsou konstantní zobrazení const_0 resp. const_1.

Věta (*o algebraické normální formě*).

$$\mathrm{R}_n \ \simeq \ \mathbb{F}_2[x_1, \ldots, x_n]/\langle x_1 + x_1^2, \ldots, x_n + x_n^2 \rangle$$

Důkaz. Označme $I = \langle x_1 + x_1^2, \ldots, x_n + x_n^2 \rangle$ ideál okruhu $\mathbb{F}_2[x_1, \ldots, x_n]$. Pro každé $i = 1, \ldots, n$ platí $x_i \equiv_I x_i^2$. Předpokládejme, že $p \in \mathbb{F}_2[x_1, \ldots, x_n]$ obsahuje proměnnou x_i v mocnině vyšší než jedna, tedy $p = qx_i^j + r$ pro nějaká $q, r \in \mathbb{F}_2[x_1, \ldots, x_n]$, $j > 1$. Pak $p = qx_i^j + r = (qx_i^{j-2})x_i^2 + r \ \equiv_I \ qx_i^{j-1} + r$. Vidíme, že každý polynom je kongruentní modulo I s polynomem bez vyšších mocnin proměnných.
Definujme zobrazení okruhů φ:

$$\begin{aligned} \mathbb{F}_2[x_1, \ldots, x_n] \ &\xrightarrow{\varphi} \ \mathrm{R}_n \\ p \ &\mapsto \ f, \ f(v) = p(v) \ \ \forall v \in \mathbb{F}_2^n \end{aligned}$$

Obraz $\varphi(p)$ definujeme dosazováním vektorů z $\mathbb{F}_2^n$ do polynomu p, kde za proměnné dosazujeme příslušné složky vektoru. Z vlastností dosazování a z definice operací R_n snadno zjistíme, že φ je homomorfismus okruhů:

$$(\varphi(p+q))(v) = (p+q)(v) = p(v) + q(v) = \varphi(p)(v) + \varphi(q)(v) = (\varphi(p) + \varphi(q))(v)$$
$$(\varphi(p \cdot q))(v) = \ (p \cdot q)(v) \ = \ p(v) \cdot q(v) \ = \ \varphi(p)(v) \cdot \varphi(q)(v) \ = (\varphi(p) \cdot \varphi(q))(v)$$

Úplný vzor $\varphi^{-1}(0) = \mathrm{Ker}(\varphi)$ je tedy ideál okruhu $\mathbb{F}_2[x_1, \ldots, x_n]$. Přitom platí $\varphi(x_i + x_i^2)(v) = v_i + v_i^2 = 0$, tedy $\varphi(x_i + x_i^2) = \mathrm{const}_0$ a $I \subseteq \mathrm{Ker}(\varphi)$.
Naopak, zvome $p \in \mathrm{Ker}(\varphi)$. Víme, že existuje $\tilde{p} \equiv_I p$ bez vyšších mocnin proměnných. Je-li $\tilde{p} = 0$, pak $p \in I$. Pokud by $\tilde{p} \neq 0$, zvolíme q monočlen $\tilde{p}$ s nejnižším stupněm (nejmenším

počtem proměnných) a vektor $v \in \mathbb{F}_2^n$ tak, že $v_i = 1$ právě když $x_i \mid q$. Tím dostaneme $q(v) = 1$ a hodnota zbylých monočlenů $\tilde{p}$ bude přitom ve v nulová. Tedy $\tilde{p}(v) = 1$ a $\tilde{p} \notin \mathrm{Ker}(\varphi)$. Polynom p tedy nemůže ležet v jádru φ, což je spor.
Ukázali jsme, že $\mathrm{Ker}(\varphi) = I$. Navíc je vidět, že v každé třídě kongruence $\equiv_I$ leží právě jeden polynom bez vyšších mocnin proměnných. Rozdíl takovýchto polynomů je totiž prvek $\mathrm{Ker}(\varphi)$ a jako polynom bez vyšších mocnin proměnných tedy musí být nulový.
Indukovaný homomorfismus

$$\mathbb{F}_2[x_1, \ldots, x_n]/I \xrightarrow{\bar{\varphi}} \mathrm{R}_n$$

je prostý. Zbývá ukázat, že každá binární booleovská funkce je φ-obrazem nějakého polynomu. Označme nejprve pro $v \in \mathbb{F}_2^n$ funkci $f_v \in \mathrm{R}_n$ takovou, že $f_v(v) = 1$ a $f_v(w) = 0 \ \forall w \neq v$. Položme

$$q_v = \prod_{i=1}^{n} (x_i + v_i + 1)$$

Snadno ověříme, že $\varphi(q_v) = f_v$. Položíme-li pro $f \in \mathrm{R}_n$

$$p = \sum_{\substack{v \in \mathbb{F}_2^n \\ f(v)=1}} q_v$$

bude platit $\varphi(p) = \sum_{\substack{v \in \mathbb{F}_2^n \\ f(v)=1}} f_v = f.$ □

Poznámka. Surjektivitu homomorfismu φ lze odvodit také porovnáním velikostí okruhů. Velikost faktoru $\mathbb{F}_2[x_1, \ldots, x_n]/I$ odpovídá počtu polynomů bez vyšších mocnin proměnných, tedy je 2^{2^n}. Počet prvků R_n je stejný.

Definice. Polynom $p \in \mathbb{F}_2[x_1, \ldots, x_n]$ bez vyšších mocnin proměnných se nazývá *algebraická normální forma* funkce $f \in \mathrm{R}_n$, pokud platí $f(v) = p(v) \ \forall v \in \mathbb{F}_2^n$. V tomto případě polynom značíme $\mathrm{ANF}(f)$.

V předchozí větě jsme dokázali existenci a jednoznačnost algebraické normální formy.

Definice. *Algebraický stupeň* $\deg(f)$ funkce $f \in \mathrm{R}_n$ je stupeň její algebraické normální formy, tedy největší délka monočlenu $\mathrm{ANF}(f)$.

Například $\mathrm{ANF}(\mathrm{const}_0) = 0$ a $\mathrm{ANF}(\mathrm{const}_1) = 1$, tedy algebraický stupeň konstantních funkcí je (nejvýše) nula. Je-li $f \in \mathrm{R}_n$ lineární zobrazení, pak $\mathrm{ANF}(f) = \sum_{i=1}^{n} f(b^{(i)}) x_i$, kde $\{b^{(1)}, \ldots, b^{(n)}\}$ je kanonická báze $\mathbb{F}_2^n$. Algebraický stupeň nenulového lineárního zobrazení je tedy roven jedné. Funkce f_v v důkazu předchozí věty mají algebraický stupeň n.

Věta. Algebraický stupeň je afinně invariantní.

Důkaz. Tvrzení věty říká, že pro $f \in \mathrm{R}_n$ a afinní bijekci $h : \mathbb{F}_2^n \to \mathbb{F}_2^n$ platí $\deg(f) = \deg(f \circ h)$. Afinní bijekce $h = \tau_v \circ g$, kde g je lineární bijekce a τ_v posunutí o pevný vektor $v \in \mathbb{F}_2^n$. Větu tedy stačí dokázat v případech lineární bijekce a posunutí.
Ať je M matice lineárního zobrazení $g : \mathbb{F}_2^n \to \mathbb{F}_2^n$ vzhledem ke kanonické bázi. Položme $q = p\,(M \cdot (x_1, \ldots, x_n)^\top)$, kde $p = \mathrm{ANF}(f)$. Polynom q vznikne dosazením příslušných lineárních kombinací proměnných do p a pro $u \in \mathbb{F}_2^n$ bude platit:

$$q(u) = p\left(M \cdot (u_1, \ldots, u_n)^\top\right) = p(g(u)) = f(g(u)) = f \circ g(u)$$

Tedy $\deg(\mathrm{ANF}(f \circ g)) \leq \deg(q) \leq \deg(p)$ (za proměnné dosazujeme polynomy stupně nejvýše jedna). Pro lineární zobrazení g tedy platí nerovnost $\deg(\mathrm{ANF}(f \circ g)) \leq \deg(\mathrm{ANF}(f))$. Je-li g navíc bijekce, pak z této vlastnosti pro g^{-1} dostaneme $\deg(\mathrm{ANF}(f)) = \deg(\mathrm{ANF}((f \circ g) \circ g^{-1})) \leq \deg(\mathrm{ANF}(f \circ g))$.
Pro $v \in \mathbb{F}_2^n$ položme $q = p\,(x_1 + v_1, \ldots, x_n + v_n)$, kde $p = \mathrm{ANF}(f)$. Pak pro $u \in \mathbb{F}_2^n$ platí:

$$q(u) = p\,(u_1 + v_1, \ldots, u_n + v_n) = p(\tau_v(u)) = f(\tau_v(u)) = f \circ \tau_v(u)$$

V tomto případě je $q = \mathrm{ANF}(f \circ \tau_v)$ a $\deg(q) = \deg(p)$. □

Zkusme polynomiálním výrazem vyjádřit hodnotu v j-té složce zašifrovaného textu kola substitučně-permutační sítě. Označme $p = \mathrm{ANF}(\pi_{\pi_{\mathrm{P}}^{-1}(j)} \circ \sigma)$, kde σ je vrstva S-boxů a $\pi_{\pi_{\mathrm{P}}^{-1}(j)}$ je projekce na $\pi_{\mathrm{P}}^{-1}(j)$-tou složku, tedy zobrazení, které vektoru $u \in \mathbb{F}_2^{lm}$ přiřadí hodnotu $u_{\pi_{\mathrm{P}}^{-1}(j)}$. Pro vrstvu l-bitových S-boxů bude $\deg(p) \leq l$ a p bude obsahovat pouze proměnné na indexech příslušného S-boxu. Hodnotu v j-té složce výstupu kola SPN můžeme zapsat výrazem $p\,(t_1 + k_1, \ldots, t_{lm} + k_{lm})$, kde t_i jsou složky vstupního plaintextu a k_i složky kolového klíče. Dosazením těchto výrazů za složky vstupních plaintextů následujících kol postupně získáme polynomiální vyjádření složek zašifrovaného textu SPN. Toto vyjádření bude obsahovat složky vstupního plaintextu SPN a složky kolových klíčů. Known plaintext útokem pak můžeme sestavit soustavu polynomiálních rovnic, kde neznámé budou složky kolových klíčů.
Řešení takovéto soustavy je cílem *algebraického útoku*. Ovšem řešení soustavy polynomiálních rovnic nad konečným tělesem je známý obtížný problém a návrhy SPN se (silně) nelineárním S-boxem budou proti takovému útoku odolné.

Jinou možností útoku na iterované kryptosystémy je lineární nebo diferenční kryptoanalýza. Při lineární kryptoanalýze iterovaných šifer budeme používat takzvanou lineární aproximaci booleovské funkce příslušnou korelační maticí. Začneme definicí korelace binárních booleovských funkcí.

Definice. Pro $f, g \in \mathrm{R}_n$ definujeme *korelaci* $\mathrm{C}(f, g) = 2 \cdot \mathrm{P}(f = g) - 1$.

Hodnota korelace tedy odpovídá pravděpodobnosti jevu $f = g$:

$$\mathrm{C}(f, g) = 2 \cdot \frac{|\{u \in \mathbb{F}_2^n;\ f(u) = g(u)\}|}{2^n} - 1$$

Je-li $\mathrm{C}(f, g)$ nenulová, řekneme, že funkce f a g jsou korelovány. Pro kryptoanalytické využití přitom není podstatné znaménko korelace, ale velikost její odchylky od nuly.
Pro korelaci platí:

- $-1 \leq \mathrm{C}(f, g) \leq 1$
- $\mathrm{C}(f, g) = \mathrm{C}(g, f)$
- $\mathrm{C}(f, g) = \mathrm{C}(f + g, 0_{\mathrm{R}_n})$
- $\mathrm{C}(f, g) = 1 \quad \Leftrightarrow\ f = g$
- $\mathrm{C}(f, g) = -1 \Leftrightarrow\ f$ je všude různá od g

Definice. Pro funkci $f \in \mathrm{R}_n$ definujeme *znaménkovou funkci* $\widehat{f} : \mathbb{F}_2^n \to \mathbb{R}$, $\widehat{f}(u) = (-1)^{f(u)}$ pro $u \in \mathbb{F}_2^n$.

Zřejmě $\mathrm{Im}(\widehat{f}) \subseteq \{-1, 1\}$. Dále platí rovnost $\widehat{f+g} = \widehat{f} \cdot \widehat{g}$, kde součin znaménkových funkcí chápeme 'po bodech'.

Na množině všech zobrazení $\mathbb{F}_2^n \to \mathbb{R}$ můžeme zavést skalární součin. Pro $h, \tilde{h} : \mathbb{F}_2^n \to \mathbb{R}$ definujeme

$$(h, \tilde{h}) = \sum_{u \in \mathbb{F}_2^n} h(u) \cdot \tilde{h}(u)$$

Pokud prvky $\mathbb{F}_2^n$ interpretujeme jako n-tice koeficientů binárních zápisů celých čísel, získáme (pevně určenou) bijekci $\mathbb{F}_2^n \xrightarrow{\iota} \{0, \ldots, 2^n - 1\}$. Zobrazení $h : \mathbb{F}_2^n \to \mathbb{R}$ pak můžeme chápat jako vektor prostoru $\mathbb{R}^{2^n}$, kde $h_i = h(\iota^{-1}(i))$. V této představě je množina všech zobrazení $\mathbb{F}_2^n \to \mathbb{R}$ reálný vektorový prostor izomorfní $\mathbb{R}^{2^n}$ a zavedený skalární součin je součinem eukleidovského prostoru. Tento pohled budeme často využívat a se zobrazeními do reálných čísel budeme pracovat jako s reálnými vektory.
Také zde máme odvozenou normu $\| h \| = \sqrt{(h, h)}$. Pro znaménkové funkce platí $\| \widehat{f} \| = 2^{n/2}$.

Lemma. Pro $f, g \in \mathrm{R}_n$ platí:

$$\mathrm{C}(f, g) = \frac{(\widehat{f}, \widehat{g})}{\| \widehat{f} \| \cdot \| \widehat{g} \|}$$

Důkaz.

$$\begin{aligned}
\frac{(\widehat{f}, \widehat{g})}{\| \widehat{f} \| \cdot \| \widehat{g} \|} &= \frac{1}{2^n} \cdot (|\{u \in \mathbb{F}_2^n; f(u) = g(u)\}| - |\{u \in \mathbb{F}_2^n; f(u) \neq g(u)\}|) \\
&= \frac{1}{2^n} \cdot (|\{f = g\}| - (2^n - |\{f = g\}|)) \\
&= 2 \cdot \frac{|\{f = g\}|}{2^n} - 1
\end{aligned}$$

□

Korelace má tedy geometrický význam - rovná se kosinu úhlu, který svírají příslušné znaménkové funkce. Platí, že binární booleovské funkce nejsou korelovány právě když jsou příslušné znaménkové funkce na sebe kolmé.

Definice. Funkce $f \in \mathrm{R}_n$ je *balancovaná*, pokud $\mathrm{C}(f, 0_{\mathrm{R}_n}) = 0$, tedy pokud platí $|f^{-1}(0)| = |f^{-1}(1)|$.

Definice. Ať je $f \in \mathrm{R}_n$ lineární. Víme, že $\mathrm{ANF}(f) = \sum_{i=1}^{n} f(b^{(i)}) x_i$, kde $\{b^{(1)}, \ldots, b^{(n)}\}$ je kanonická báze $\mathbb{F}_2^n$. Položme $v = (f(b^{(1)}), \ldots, f(b^{(n)})) \in \mathbb{F}_2^n$. Funkci f budeme nazývat *parita* a značit p_v.

Parity jsou lineární formy nad dvouprvkovým tělesem. Můžeme říci, že $\mathrm{p}_v(u)$ udává paritu počtu jednotek na indexech vektoru u, kde je $v = 1$.

Lemma. Nenulové parity jsou balancované.

Důkaz. Zvolme $u \in \mathbb{F}_2^n \setminus \mathrm{Ker}(\mathrm{p}_v)$. Platí $\mathrm{p}_v^{-1}(1) = u + \mathrm{Ker}(\mathrm{p}_v)$, tedy $|\mathrm{p}_v^{-1}(0)| = |\mathrm{Ker}(\mathrm{p}_v)| = |u + \mathrm{Ker}(\mathrm{p}_v)| = |\mathrm{p}_v^{-1}(1)|$. □

Věta. Znaménkové funkce parit tvoří ortogonální bázi $\mathbb{R}^{2^n}$.

Důkaz. Množina všech parit odpovídá množině všech zobrazení pevně zvolené báze $\mathbb{F}_2^n$ do dvouprvkového tělesa. Počet parit je tedy 2^n (jinými slovy: duální prostor $(\mathbb{F}_2^n)^*$ má stejnou dimenzi). Znaménkové funkce jsou vždy nenulové. Stačí tedy dokázat, že znaménkové funkce různých parit jsou na sebe kolmé - tedy že různé parity nejsou korelované.
Pro korelaci platí $\mathrm{C}(\mathrm{p}_v, \mathrm{p}_w) = \mathrm{C}(\mathrm{p}_v + \mathrm{p}_w, 0_{\mathrm{R}_n})$. Je-li $\mathrm{p}_v \neq \mathrm{p}_w$ (tedy $v \neq w$), pak je $\mathrm{p}_v + \mathrm{p}_w$ nenulová parita. □

Každé zobrazení $h : \mathbb{F}_2^n \to \mathbb{R}$ můžeme tedy zapsat v bázi znaménkových funkcí parit:

$$h = \sum_{v \in \mathbb{F}_2^n} \frac{(h\,, \widehat{\mathrm{p}}_v)}{(\widehat{\mathrm{p}}_v\,, \widehat{\mathrm{p}}_v)} \cdot \widehat{\mathrm{p}}_v$$

Koeficienty tohoto zápisu v ortogonální bázi budou v případě znaménkové funkce:

$$\frac{(\widehat{f}\,, \widehat{\mathrm{p}}_v)}{(\widehat{\mathrm{p}}_v\,, \widehat{\mathrm{p}}_v)} = \frac{(\widehat{f}\,, \widehat{\mathrm{p}}_v)}{2^n} = \frac{(\widehat{f}\,, \widehat{\mathrm{p}}_v)}{\| \widehat{f} \| \cdot \| \widehat{\mathrm{p}}_v \|} = \mathrm{C}(f, \mathrm{p}_v)$$

Zápis znaménkové funkce:

$$\widehat{f} = \sum_{v \in \mathbb{F}_2^n} \mathrm{C}(f, \mathrm{p}_v) \cdot \widehat{\mathrm{p}}_v$$

Definice. *Walsh-Hadamardova transformace* prostoru všech zobrazení $\mathbb{F}_2^n \to \mathbb{R}$ je definována následujícím předpisem:

$$\begin{aligned} \{\mathbb{F}_2^n \to \mathbb{R}\} &\xrightarrow{\mathrm{W}} \{\mathbb{F}_2^n \to \mathbb{R}\} \\ h &\mapsto \mathrm{W}(h),\ \mathrm{W}(h)(v) = \frac{(h\,, \widehat{\mathrm{p}}_v)}{(\widehat{\mathrm{p}}_v\,, \widehat{\mathrm{p}}_v)} \end{aligned}$$

Walsh-Hadamardova transformace přiřazuje vektoru z $\mathbb{R}^{2^n}$ vektor jeho souřadnic v bázi znaménkových funkcí parit. Je to proto lineární bijekce, tedy automorfismus prostoru $\mathbb{R}^{2^n}$. Matice W vzhledem ke kanonické bázi má speciální tvar. Její řádky (sloupce) jsou navzájem kolmé, mají stejnou normu a zároveň je tato matice symetrická. Symetrie plyne z vlastnosti počítání s paritami: pro $u, v \in \mathbb{F}_2^n$ platí $\mathrm{p}_v(u) = \mathrm{p}_u(v)$ a tedy i $\widehat{\mathrm{p}}_v(u) = \widehat{\mathrm{p}}_u(v)$. Normalizací W vhodným skalárem lze získat ortogonální involutivní transformaci $\mathbb{R}^{2^n}$.

Definice. Pro $f \in \mathrm{R}_n$ se zobrazení $\mathrm{W}(\widehat{f})$ nazývá *spektrum* binární booleovské funkce f.

Věta (*Parseval*). Norma spektra je rovna jedné.

Důkaz. Pro $f \in \mathrm{R}_n$ postupujeme úpravami skalárního součinu $(\widehat{f}\,, \widehat{f}\,)$:

$$\begin{aligned} (\widehat{f}\,, \widehat{f}\,) &= \left(\sum_{v \in \mathbb{F}_2^n} \mathrm{W}(\widehat{f})(v) \cdot \widehat{\mathrm{p}}_v \ , \ \sum_{w \in \mathbb{F}_2^n} \mathrm{W}(\widehat{f})(w) \cdot \widehat{\mathrm{p}}_w \right) \\ &= \sum_{v \in \mathbb{F}_2^n} \sum_{w \in \mathbb{F}_2^n} \mathrm{W}(\widehat{f})(v) \cdot \mathrm{W}(\widehat{f})(w) \cdot (\widehat{\mathrm{p}}_v\,, \widehat{\mathrm{p}}_w) \\ &= \sum_{v \in \mathbb{F}_2^n} \mathrm{W}^2(\widehat{f})(v) \cdot (\widehat{\mathrm{p}}_v\,, \widehat{\mathrm{p}}_v) \\ &= 2^n \cdot \left(\mathrm{W}(\widehat{f}\,), \mathrm{W}(\widehat{f}\,) \right) \end{aligned}$$

Tvrzení plyne z rovnosti $(\widehat{f}\,,\widehat{f}\,) = 2^n$. □

Definice. Pro $f \in \mathrm{R}_n$ a $v \in \mathbb{F}_2^n$ se hodnota $\mathrm{W}^2(\widehat{f}\,)(v) = \mathrm{C}^2(f, \mathrm{p}_v)$ nazývá *korelační potenciál* f *ve* v.

Podle předchozí věty je součet všech korelačních potenciálů dané binární booleovské funkce roven jedné.