Diferenční kryptoanalýza

Definice. Pro booleovskou funkci $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ definujeme *matici šíření diference* DP^f jako matici typu $2^m \times 2^n$ nad $\mathbb{R}$, kde pro $u \in \mathbb{F}_2^m$ a $v \in \mathbb{F}_2^n$ je

$$\mathrm{DP}^f_{u,v} \;=\; \mathrm{P}(f + f \circ \tau_v = u) \;=\; \frac{|\{w \in \mathbb{F}_2^n \,;\, f(w) + f(w+v) = u\}|}{2^n}$$

Vektor v se přitom nazývá *vstupní diference*, vektor u *výstupní diference* a hodnota $\mathrm{DP}^f_{u,v}$ *šíření diference (difference propagation) od v k u*. Příslušný jev budeme v tomto textu značit $\mathrm{A}^f_{u,v} = \{w \in \mathbb{F}_2^n \,;\, f(w) + f(w+v) = u\}$.

Poznámka. Zřejmě je $0 \le \mathrm{DP}^f_{u,v} \le 1$. Dále z definice plyne $\mathrm{DP}^f_{0,0} = 1$ a $\mathrm{DP}^f_{u,0} = 0$ pro $u \neq 0$. Pro f prostou funkci a $v \neq 0$ pak je také $\mathrm{DP}^f_{0,v} = 0$.
Tvar prvního sloupce DP^f je speciální případ obecnější vlastnosti. Pro každé $v \in \mathbb{F}_2^n$ platí:

$$\sum_{u \in \mathbb{F}_2^m} \mathrm{DP}^f_{u,v} = 1$$

Totiž jevy $\mathrm{A}^f_{u,v}$ jsou pro různé vektory $u \in \mathbb{F}_2^m$ disjunktní a jejich sjednocení je celý prostor $\mathbb{F}_2^n$.

Definice. Je-li $\mathrm{DP}^f_{u,v} \neq 0$ řekneme, že vstupní diference v a výstupní diference u jsou *kompatibilní v f*.

Definice. Pro booleovskou funkci f, vstupní diferenci v a výstupní diferenci u kompatibilní v f definujeme *váhu šíření diference* $\mathrm{w}^f_{u,v} = -\log_2 \mathrm{DP}^f_{u,v}$.

Lemma. Pro $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$, $v \in \mathbb{F}_2^n$ a $u \in \mathbb{F}_2^m$ kompatibilní v f platí $0 \le \mathrm{w}^f_{u,v} \le n-1$.

Důkaz. Váha šíření diference nabývá nejmenší možnou hodnotu pro $\mathrm{DP}^f_{u,v} = 1$. Pro horní odhad je třeba si uvědomit, že velikost jevu $\mathrm{A}^f_{u,v}$ je vždy sudé číslo. Víme, že $|\mathrm{A}^f_{0,0}| = 2^n$ a $|\mathrm{A}^f_{u,0}| = 0$ pro $u \neq 0$. Posunutí τ_v má pro $v \neq 0$ na prostoru $\mathbb{F}_2^n$ 2-prvkové orbity. Přitom platí $w \in \mathrm{A}^f_{u,v}$ právě když $w + v \in \mathrm{A}^f_{u,v}$. Jsou-li tedy diference v a u kompatibilní, pak $|\mathrm{A}^f_{u,v}| = 2k$, $0 \neq k \in \mathbb{N}$, a $\mathrm{DP}^f_{u,v} \ge \frac{1}{2^{n-1}}$. □

Můžeme říci, že váha $\mathrm{w}^f_{u,v}$ udává úbytek entropie jevu $\mathrm{A}^f_{u,v}$. Pro kompatibilní diference je $\mathrm{DP}^f_{u,v} = 2^{-\mathrm{w}^f_{u,v}}$ a $|\mathrm{A}^f_{u,v}| = 2^{n-\mathrm{w}^f_{u,v}}$. V tomto případě se uvádí také formulace: ‘vektory jevu $\mathrm{A}^f_{u,v}$ jsou určeny na $\mathrm{w}^f_{u,v}$ bitech’.

Pro matici šíření diference složení booleovských funkcí rovnost $\mathrm{DP}^{g \circ f} = \mathrm{DP}^g \cdot \mathrm{DP}^f$ obecně neplatí. Tato rovnost ale nastává v důležitém speciálním případě složení bijekcí, pokud je jedna z nich afinní zobrazení.

Lemma. Ať je $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ bijekce a $g : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Jsou-li pro všechna $v, \tilde{u} \in \mathbb{F}_2^n$ a všechna $u \in \mathbb{F}_2^m$ jevy $\mathrm{A}^f_{\tilde{u},v}$ a $f^{-1}\big(\mathrm{A}^g_{u,\tilde{u}}\big)$ nezávislé, pak je $\mathrm{DP}^{g \circ f} = \mathrm{DP}^g \cdot \mathrm{DP}^f$.

Důkaz. Jev $\mathrm{A}^{g \circ f}_{u,v}$ můžeme zapsat jako disjunktní sjednocení

$$\mathrm{A}^{g\circ f}_{u,v} = \bigsqcup_{\tilde{u}\in\mathbb{F}_2^n} \left(f^{-1}\big(\mathrm{A}^{g}_{u,\tilde{u}}\big) \cap \mathrm{A}^{f}_{\tilde{u},v} \right)$$

Pro šíření diference dostaneme:

$$\begin{aligned}
\mathrm{DP}^{g\circ f}_{u,v} &= \mathrm{P}\big(\mathrm{A}^{g\circ f}_{u,v}\big) \\
&= \mathrm{P}\left(\bigsqcup_{\tilde{u}\in\mathbb{F}_2^n} \left(f^{-1}\big(\mathrm{A}^{g}_{u,\tilde{u}}\big) \cap \mathrm{A}^{f}_{\tilde{u},v} \right) \right) \\
&= \sum_{\tilde{u}\in\mathbb{F}_2^n} \mathrm{P}(f^{-1}(\mathrm{A}^{g}_{u,\tilde{u}})) \cdot \mathrm{P}(\mathrm{A}^{f}_{\tilde{u},v}) \\
&= \sum_{\tilde{u}\in\mathbb{F}_2^n} \mathrm{P}(\mathrm{A}^{g}_{u,\tilde{u}}) \cdot \mathrm{P}(\mathrm{A}^{f}_{\tilde{u},v}) \\
&= \sum_{\tilde{u}\in\mathbb{F}_2^n} \mathrm{DP}^{g}_{u,\tilde{u}} \cdot \mathrm{DP}^{f}_{\tilde{u},v} \\
&= \big(\mathrm{DP}^{g} \cdot \mathrm{DP}^{f}\big)_{u,v}
\end{aligned}$$

□

Lemma. Booleovská funkce $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ je afinní bijekce právě když je DP^f permutační matice.

Důkaz. Afinní funkce má tvar $\tau \circ h$, kde h je lineární a τ je posunutí o pevný vektor. Pro $f = \tau \circ h$ platí $f(w) + f(w+v) = h(w) + h(w+v) = 2\,h(w) + h(v) = h(v)$. Je-li $u = h(v)$, pak $\mathrm{DP}^f_{u,v} = 1$, jinak je $\mathrm{DP}^f_{u,v} = 0$. Matice DP^f tedy obsahuje pouze hodnoty 0 a 1. Přitom $\mathrm{DP}^f_{h(v),v}$ je jediná jednotka sloupce v. Pokud je f bijekce, pak h je bijekce a $\mathrm{DP}^f_{u,h^{-1}(u)}$ je jediná jednotka řádku u.
Ať je DP^f permutační matice. Položme $h = \tau_{f(0)} \circ f$. Pro $v \in \mathbb{F}_2^n$ platí $f(0)+f(0+v) = h(v)$, tedy $\mathrm{DP}^f_{h(v),v} > 0$. Pak musí být $\mathrm{DP}^f_{h(v),v} = 1$. Pro každé $w \in \mathbb{F}_2^n$ pak platí $h(v) = f(w)+f(w+v) = h(w)+h(w+v)$, což dokazuje linearitu h.
Zbývá dokázat, že f je prostá. V řádcích DP^f je vždy jediná nenulová hodnota. Přitom víme, že $\mathrm{DP}^f_{h(v),v} \neq 0$ pro každé $v \in \mathbb{F}_2^n$. Z $h(v) = h(v')$ musí tedy plynout $v = v'$. □

Důsledek. Ať jsou $f, g : \mathbb{F}_2^n \to \mathbb{F}_2^n$ bijekce. Je-li f nebo g afinní, pak $\mathrm{DP}^{g\circ f} = \mathrm{DP}^{g} \cdot \mathrm{DP}^{f}$.

Důkaz. Jedna z matic DP^f, DP^g je permutační. V tomto případě jsou příslušné jevy buď prázdné, nebo zahrnují celý prostor. Jevy $\mathrm{A}^f_{\tilde{u},v}$ a $f^{-1}\big(\mathrm{A}^g_{u,\tilde{u}}\big)$ jsou tudíž vždy nezávislé. □

Kolo substitučně-permutační sítě obsahuje kromě vrstvy S-boxů dvě afinní vrstvy - přičtení klíče a permutační vrstvu. Matice šíření diference kola SPN je tedy podle předchozího tvrzení součinem matic šíření diference jeho vrstev (pro konkrétní hodnotu kolového klíče). Tvary matic šíření diference jednotlivých vrstev nyní popíšeme.

Přičtení klíče

Přičtení klíče τ_K je afinní bijekce. Matice DP^{τ_K} je permutační a v tomto případě platí $\tau_K(w) + \tau_K(w+v) = v$. Tedy $\mathrm{DP}^{\tau_K}_{v,v} = 1$ a matice DP^{τ_K} je identická. Pro bijekci g pak platí $\mathrm{DP}^{g\circ\tau_K} = \mathrm{DP}^{\tau_K\circ g} = \mathrm{DP}^{g}$.

Permutační vrstva

Šifrovací zobrazení permutační vrstvy je lineární bijekce. Pro f lineární platí $f(w)+f(w+v)=f(v)$. Je-li tedy f lineární bijekce, DP^f je permutační matice s jednotkovými vstupy $\mathrm{DP}^f_{f(v),v}$. Matice šíření diference složení $\mathrm{DP}^{\,g\circ f}$ pro bijekci g pak vznikne permutací sloupců (v opačném pořadí složení řádků) $\mathrm{DP}^{\,g}$.

Vrstva S-boxů

Ať jsou $f_i : \mathbb{F}_2^{n_i} \to \mathbb{F}_2^{l_i}$, $i = 1, \ldots, m$, $n = \sum_{i=1}^{m} n_i$, $l = \sum_{i=1}^{m} l_i$ a $f : \mathbb{F}_2^n \to \mathbb{F}_2^l$ je bricklayer funkce, tedy obraz $w = (w^{(1)}|\ldots|w^{(m)}) \in \mathbb{F}_2^n$, $w^{(i)} \in \mathbb{F}_2^{n_i}$, je $f(w) = (f_1(w^{(1)})|\ldots|f_m(w^{(m)})) \in \mathbb{F}_2^l$. Pro funkci f platí:

$$f(w) + f(w+v) = u \quad \Leftrightarrow \quad f_i(w^{(i)}) + f_i(w^{(i)} + v^{(i)}) = u^{(i)} \quad \forall\, i = 1, \ldots, m$$

Jinými slovy:

$$w \in \mathrm{A}^f_{u,v} \quad \Leftrightarrow \quad w^{(i)} \in \mathrm{A}^{f_i}_{u^{(i)},v^{(i)}} \quad \forall\, i = 1, \ldots, m$$

Jev $\mathrm{A}^f_{u,v}$ tedy můžeme zapsat jako kartézský součin $\mathrm{A}^{f_1}_{u^{(1)},v^{(1)}} \times \ \ldots \ \times \mathrm{A}^{f_m}_{u^{(m)},v^{(m)}}$. Pro šíření diference pak dostaneme:

$$\begin{aligned} \mathrm{DP}^f_{u,v} &= \frac{\left|\mathrm{A}^f_{u,v}\right|}{2^n} = \prod_{i=1}^{m} \frac{\left|\mathrm{A}^{f_i}_{u^{(i)},v^{(i)}}\right|}{2^{n_i}} = \prod_{i=1}^{m} \mathrm{DP}^{f_i}_{u^{(i)},v^{(i)}} \\ \mathrm{w}^f_{u,v} &= \sum_{i=1}^{m} \mathrm{w}^{f_i}_{u^{(i)},v^{(i)}} \end{aligned}$$

V dalším textu bude $f = f_N \circ \ldots \circ f_1$ složení booleovských funkcí $f_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $i = 1, \ldots, N$.

Definice. *Diferenční cesta* nad f je $(N+1)$-tice vektorů $U = (u^{(0)}, \ldots, u^{(N)})$, $u^{(i)} \in \mathbb{F}_2^n$, $i = 0, \ldots, N$, taková, že pro $i = 1, \ldots, N$ jsou diference $u^{(i-1)}$, $u^{(i)}$ kompatibilní v f_i. Dvojice $(u^{(i-1)}, u^{(i)})$ se nazývají *diferenční kroky* cesty U, *váha diferenčního kroku* je hodnota $\mathrm{w}^{f_i}_{u^{(i)},u^{(i-1)}}$. *Váha diferenční cesty* je

$$\mathrm{w}(U) = \sum_{i=1}^{N} \mathrm{w}^{f_i}_{u^{(i)},u^{(i-1)}}$$

Pokud diferenční cesta $U = (u^{(0)}, \ldots, u^{(N)})$ začíná vektorem $v = u^{(0)}$ a končí vektorem $u = u^{(N)}$, řekneme, že je to cesta od v k u.

Definice. *Pravděpodobnost diferenční cesty* $U = (u^{(0)}, \ldots, u^{(N)})$ nad f je hodnota

$$\mathrm{P}(U) = \frac{|\{w \in \mathbb{F}_2^n\,;\ \varphi_i(w) + \varphi_i(w + u^{(0)}) = u^{(i)} \ \ \forall\, i = 1, \ldots, N\}|}{2^n}$$

kde $\varphi_i = f_i \circ \ldots \circ f_1$, $i = 1, \ldots, N$.

Věta. Pro $u, v \in \mathbb{F}_2^n$ platí

$$\mathrm{DP}^f_{u,v} = \sum_{\substack{U \text{ dif. cesta nad } f \\ \text{od } v \text{ k } u}} \mathrm{P}(U)$$

Důkaz. Pro $w \in \mathrm{A}^f_{u,v}$ můžeme definovat diferenční cestu

$$(v,\, \varphi_1(w) + \varphi_1(w+v),\, \ldots\, ,\, \varphi_N(w) + \varphi_N(w+v) = u)$$

Šíření diference pak můžeme vyjádřit:

$$\begin{aligned}
\mathrm{DP}^f_{u,v} &= \frac{\left|\mathrm{A}^f_{u,v}\right|}{2^n} \\
&= \frac{1}{2^n} \cdot \left| \bigsqcup_{\substack{U = (u^{(0)}=v,\, \ldots\, ,u^{(N)}=u) \\ \text{dif. cesta nad } f}} \left\{w \in \mathbb{F}_2^n\,;\ \varphi_i(w) + \varphi_i(w+v) = u^{(i)}\ \ \forall\, i = 1, \ldots, N\right\} \right| \\
&= \frac{1}{2^n} \cdot \sum_{\substack{U = (u^{(0)}=v,\, \ldots\, ,u^{(N)}=u) \\ \text{dif. cesta nad } f}} \left|\left\{w \in \mathbb{F}_2^n\,;\ \varphi_i(w) + \varphi_i(w+v) = u^{(i)}\ \ \forall\, i = 1, \ldots, N\right\}\right| \\
&= \sum_{\substack{U \text{ dif. cesta nad } f \\ \text{od } v \text{ k } u}} \mathrm{P}(U)
\end{aligned}$$

□

Má-li diferenční cesta nad f od v k u významnou pravděpodobnost, pak totéž platí pro šíření diference $\mathrm{DP}^f_{u,v}$. Bez znalosti kolových klíčů ovšem neznáme chování zobrazení φ_i a pravděpodobnost diferenční cesty tak určit nemůžeme. Z pohledu útočníka je vhodným invariantem váha diferenční cesty.

Váha diferenční cesty nad klíč alternující šifrou. Šifrovací zobrazení klíč alternující šifry pro konkrétní hodnoty kolových klíčů je:

$$f = \left(\tau_{K_{N+1}} \circ\, \beta_N \circ\, \tau_{K_N}\right) \circ \left(\beta_{N-1} \circ\, \tau_{K_{N-1}}\right) \circ\, \ldots \circ \left(\beta_1 \circ\, \tau_{K_1}\right)$$

kde τ_{K_i}, $i = 1, \ldots, N+1$, jsou přičtení kolových klíčů a β_i, $i = 1, \ldots, N$, jsou bijekce nezávislé na klíčích. Matice šíření diference šifrovacích zobrazení kol:

$$\begin{aligned}
\mathrm{DP}^{\,\beta_i \circ \tau_{K_i}} &= \mathrm{DP}^{\,\beta_i} \cdot \mathrm{DP}^{\,\tau_{K_i}} = \mathrm{DP}^{\,\beta_i},\ \ i = 1, \ldots, N-1 \\
\mathrm{DP}^{\,\tau_{K_{N+1}} \circ \beta_N \circ \tau_{K_N}} &= \mathrm{DP}^{\,\tau_{K_{N+1}}} \cdot \mathrm{DP}^{\,\beta_N} \cdot \mathrm{DP}^{\,\tau_{K_N}} = \mathrm{DP}^{\,\beta_N}
\end{aligned}$$

Označíme-li $f_1, \ldots, f_N$ šifrovací zobrazení kol, pak pro diferenční cestu $U = (u^{(0)}, \ldots, u^{(N)})$ nad f dostaneme:

$$\mathrm{w}(U) = \sum_{i=1}^{N} \mathrm{w}^{f_i}_{u^{(i)}, u^{(i-1)}} = \sum_{i=1}^{N} \mathrm{w}^{\beta_i}_{u^{(i)}, u^{(i-1)}}$$

Váha diferenční cesty nad klíč alternující šifrou tedy nezávisí na hodnotách klíčů.

Diferenční útok na substitučně-permutační síť. Popíšeme diferenční útok na SPN, jehož cílem je získat část posledního kolového klíče. Postup útoku na N-kolovou verzi:

1. Konstrukce diferenční cesty $U = (u^{(0)}, \ldots, u^{(N-1)})$ nad prvními $N-1$ koly SPN s malou vahou. Označíme $v = u^{(0)}$, $u = u^{(N-1)}$.

2. Generování množiny vzorků $T = \{(x, \bar{x}, f(x), f(\bar{x}))\}$, kde f je šifrovací zobrazení N-kolové SPN (pro neznámé ale pevně dané klíče) a pro vzorky platí $x + \bar{x} = v$. Odhaduje se, že počet vzorků by měl zhruba odpovídat hodnotě $2^{\mathrm{w}(U)}$.

3. Na indexech těch S-boxů, na kterých je vektor u nenulový (na S-boxech, na kterých končí cesta U), tipujeme část posledního kolového klíče K_{N+1}. Pro každý takový tip $\tilde{K}$ spočítáme

$$\mathrm{DP}_{\tilde{K}} = \frac{\left|\left\{(x, \bar{x}, y, \bar{y}) \in T\,;\ \sigma^{-1}(y + \tilde{K}) + \sigma^{-1}(\bar{y} + \tilde{K}) = u\right\}\right|}{|T|}$$

   Pro korektní výpočet můžeme $\tilde{K}$ na zbylé S-boxy rozšířit libovolně. Na zbylých S-boxech je vektor u nulový, tedy na těchto S-boxech bude podmínka splněna právě když y a $\bar{y}$ jsou na nich shodné. Je-li tip na klíč správný, můžeme $\mathrm{DP}_{\tilde{K}}$ chápat jako aproximaci šíření diference $\mathrm{DP}^{f'}_{u,v}$ na množině vzorků, kde f' je šifrovací zobrazení prvních $N-1$ kol.

Tipy na část K_{N+1} s výraznou hodnotou $\mathrm{DP}_{\tilde{K}}$ jsou kandidáty na hledaný výsledek.

Poznámky. 1) K diferenčnímu útoku potřebujeme získat vzorky s pevně danou diferencí plaintextů. Pravděpodobnost nasbírání takové množiny vzorků při šifrování náhodných plaintextů je nízká. Útočník musí v tomto případě do generování vzorků aktivně zasahovat, jde tedy o *chosen plaintext* útok.

2) Při generování vzorků je vhodné vyřadit ty vzorky $(x, \bar{x}, y, \bar{y})$, u kterých je vektor y různý od $\bar{y}$ na S-boxech, na kterých je poslední vektor diferenční cesty nulový. Tyto vzorky totiž pro žádný tip na klíč podmínku šíření diference nesplňují. Jde o tzv. *filtrování vzorků*.

3) Podobně jako v lineárním případě můžeme takto útočit na oba krajní kolové klíče. Pro omezení počtu nalezených kandidátů je důležité, aby diferenční cesta končila v malém počtu S-boxů.

4) Zkonstruovaná diferenční cesta končí před poslední vrstvou S-boxů. Pouhé přičtení stejného tipu na klíč totiž výslednou diferenci nezmění. Spoléháme na 'náhodné' chování S-boxů, které může tipy na klíč dostatečně rozlišit. Úspěšnosti diferenčního útoku při náhodné volbě kolových klíčů se budeme věnovat v dalším textu.