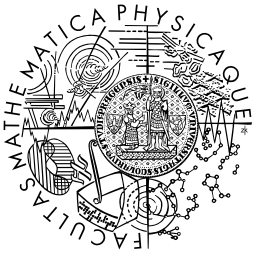

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Jana Hrúzová

Zobecněná integrální vlastnost

Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. et Mgr. Jan Žemlička, Ph.D.

Studijní program: Matematika

Studijní obor: Matematika pro informační technologie

Praha 2020

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ....

Jana Hrúzová

Děkuji vedoucímu mé práce panu doc. Mgr. et Mgr. Janu Žemličkovi, Ph.D. za cenné připomínky a čas věnovaný konzultacím.

Název práce: Zobecněná integrální vlastnost

Autor: Jana Hrúzová

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., Katedra algebry

Abstrakt: Tato bakalářská práce vychází z odborného článku C. Boura a A. Canteaut, Another View of the Division Property, který pojednává o dělící vlastnosti množin z $\mathbb{F}_2^n$. V této práci nejprve zopakujeme důležité pojmy a tvrzení o booleovských funkcích, polynomech a Reed-Mullerových kódech. Následně definujeme množinu parit množiny z $\mathbb{F}_2^n$. Pomocí množiny parit zjednodušíme dělící vlastnost a ukážeme, jak vypadají množiny splňující různé stupně dělící vlastnosti. Díky tomu budeme moci určit, jak se dělící vlastnost šíří substitučně-permutační sítí.

Klíčová slova: dělící vlastnost, množina parit, substitučně-permutační síť, booleovské funkce

Title: Generalized integral property

Author: Jana Hrúzová

Department: Department of Algebra

Supervisor: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., Department of Algebra

Abstract: This thesis is based on an article C. Boura and A. Canteaut, Another View of the Division Property, which is focused on division property of sets from $\mathbb{F}_2^n$. In this thesis we introduce important definitions and propositions about boolean function, polynomials and Reed-Muller codes at the beginning. Then we define parity set of a set from $\mathbb{F}_2^n$, which helps us to simplify the division property. We also show how sets, which satisfy division property of certain order, look like. From that we could follow how the division property propagate through the substitution-permutation network.

Keywords: division property, parity set, substitution-permutation network, boolean function

Obsah

Úvod

Blokové šifry jsou častým příkladem symetrického šifrování. Otevřený text zpracovávají po úsecích určené délky, po tak zvaných blocích. Výstupem je stejně dlouhý blok šifrového textu.

V této práci uvedeme článek autorů Boura a Canteaut (2016), který se zabývá dělící vlastností množin z $\mathbb{F}_2^n$ a tím, jak se tato vlastnost šíří v blokových šifrách.

Dělící vlastnost byla poprvé definována v článku Todo (2015) jako zobecnění dříve zkoumané takzvané integrální vlastnosti. Z toho názvu je lehce patrnější motivace, proč takovou vlastnost množin z $\mathbb{F}_2^n$ zkoumat.

Tou motivací k zkoumání dělící vlastnosti je možnost integrální kryptoanalýzy na blokových šifrách. Integrální útok se skládá z nalezení rozlišovače a hádání klíče.

Nejdříve se vezme N otevřených textů a jim odpovídajících šifrových textů tak, aby v předposlední rundě platilo $\sum_{x \in X} x = 0$, kde X je množina všech odpovídajících výstupů předposlední rundy.

Následně se hádá poslední rundovní klíč a ze šifrových textů se dopočtou výstupy předposlední rundy, ty označme X'. Pokud pro tyto výstupy $\sum_{x \in X'} x \neq 0$, pak je použitý rundovní klíč nesprávný. Naopak pokud danou rovnost splňují, pak se použitý rundovní klíč přidává do kandidátů na správný klíč. Takto se postupně hádají rundovní klíče celé šifry.

V této práci ukážeme, že dělící vlastnost množiny je vhodný rozlišovač pro integrální útoky. To znamená, že pokud množina X splňuje dělící vlastnost stupně alespoň 2, pak platí $\sum_{x \in X} x = 0$.

První kapitolu věnujeme opakování ze samoopravných kódů, převážně booleovským polynomům, funkcím a základům z Reed-Mullerových kódů.

Ve druhé kapitole definujeme množinu parit pro množinu z $\mathbb{F}_2^n$ a ukážeme, že jednoznačně určuje danou množinu. Dále pomocí množiny parit budeme moci lépe zformulovat dělící vlastnost a prozkoumat, jak vypadají množiny splňující dělící vlastnost určitého stupně.

Třetí kapitola se zabývá tím, jak vypadají množiny parit při průchodu dané množiny substitučně permutační sítí s bijektivními S-boxy. To nám pak pomůže zjistit, jestli dané množiny po určitém počtu rund splňují dělící vlastnost.

1. Úvod do booleovských funkcí

Sekce o booleovských funkcích, polynomech a Reed-Mullerových kódech převážně vychází ze skript profesora Drápala, kde je možné dohledat důkazy ke zde vyřčeným tvrzením. Zároveň je to shrnutí základních pojmů a tvrzení, které budeme dále v práci používat.

1.1 Značení

V textu značí **0** nulový vektor z $\mathbb{F}_2^n$, **1** vektor obsahující samé jedničky z $\mathbb{F}_2^n$ a e_i i-tý vektor kanonické báze $\mathbb{F}_2^n$.

Vektor $x \in \mathbb{F}_2^n$ nazýváme n-bitové slovo.

Hammingova váha vektoru z $\mathbb{F}_2^n$ je počet nenulových souřadnic v daném vektoru. Pro $a \in \mathbb{F}_2^n$ i-tou souřadnici značíme a_i a Hammingovu váhu $wt(a)$ spočítáme jako $wt(a) = \sum_{i=1}^{n} a_i$.

Support vektoru $\mathbb{F}_2^n$ je množina indexů nenulových souřadnic daného vektoru.

Definice 1 (Afinní podprostor)**.** *Nechť V je vektorový prostor nad tělesem T. Afinním podprostorem prostoru V je neprázdná množina tvaru $a + U = \{a + u \mid u \in U\}$, kde $a \in V$ a $U \subseteq V$ je vektorový podprostor.*

1.2 Booleovské polynomy

Něchť F je komutativní těleso. Polynomy v neznámých x_1,...,x_n tvoří okruh polynomů $F[x_1,...,x_n]$. Každý polynom f lze zapsat jako formální sumu

$$\sum a_{i_1,...,i_m} x_1^{i_1} ... x_m^{i_m},$$

kde i_1,...,i_m jsou celá nezáporná čísla a kde $a_{i_1,...,i_m} \in F$ je nenulové jen pro konečně mnoho m-tic $(i_1,...,i_m)$.

Definice 2 (Algebraický stupeň)**.** *Stupeň polynomu $f \in F[x_1,...,x_n]$ je*

$$deg(f) = \max_{\substack{(i_1,...,i_m) \\ a_{i_1,...,i_m} \neq 0}} (i_1 + ... + i_m).$$

Stupeň nulového polynomu definujeme jako -1.

Polynom nazveme booleovský, je-li $F = \mathbb{F}_2$ a současně $a_{i_1,...,i_m} = 0$ kdykoliv $i_j \geq 2$ pro některé j od 1 do m.

Používáme následující značení pro monomy s n proměnnými, kde $u \in \mathbb{F}_2^n$

$$x^u = \prod_{i=1}^{n} x_i^{u_i}.$$

Každý booleovský polynom v proměných x_1,...,x_n lze jednoznačně zapsat jako $\sum_{u \in M} x^u$, kde M je nějaká podmnožina $\mathbb{F}_2^n$.

Booleovské polynomy v proměnných x_1,...,x_n tvoří komutativní okruh se standardním sčítáním a s násobením určeným podmínkou $x^u \cdot x^v = x^w$, kde $w_i = 1 \Leftrightarrow u_i = 1$ nebo $v_i = 1$.

Příklad. Mějme booleovské polynomy

$$f = x_1x_2x_4 = x^{(1,0,1,1)}$$
$$g = x_1x_3x_4 = x^{(1,1,0,1)}.$$

Jejich součin je roven $fg = x_1x_2x_3x_4 = x^{(1,1,1,1)}$.

1.3 Booleovské funkce

Booleovská funkce n proměnných je zobrazení z $\mathbb{F}_2^n$ do $\mathbb{F}_2$. Každému polynomu $f \in \mathbb{F}_2[x_1,...,x_n]$ můžeme přiřadit booleovskou funkci $\overline{f}$ n proměnných tak, že funkční hodnota v bodě $u = (u_1,...,u_n)$ se spočítá dosazením u_i za x_i, $1 \leq i \leq n$. Je tedy rovna $f(u) = f(u_1,...,u_n)$.

Příklad. Mějme booleovský polynom $f = x_1 + x_3 + x_2x_3$. Pak booleovskou funkci dostaneme jako zobrazení $\mathbb{F}_2^3 \to \mathbb{F}_2$, které $(u_1,u_2,u_3) \mapsto u_1 + u_3 + u_2u_3$.

Pro přehlednější značení indexů vektorů a matic bude prvek $(u_1,...,u_m) \in \mathbb{F}_2^n$ reprezentovat:

- vektor z $\mathbb{F}_2^n$
- číslo v binárním zápisu, jehož hodnotou v desítkové soustavě je $\sum_{i=1}^{n} u_i 2^{n-i}$

Touto jeho číselnou hodnotou jsou prvky uspořádány vzestupně v lexikografickém pořadí. Počítáme-li od nuly, tak j-tým prvkem je vektor, jehož souřadnice vyjadřují binární zápis čísla j.

Příklad. Reprezentace v $\mathbb{F}_2^3$ je následující.

Vektor	Číselná hodnota
(0,0,0)	0
(0,0,1)	1
(0,1,0)	2
(0,1,1)	3
(1,0,0)	4
(1,0,1)	5
(1,1,0)	6
(1,1,1)	7

Definice 3 (Algebraická normální forma)**.** *Algebraickou normální formou booleovské funkce $f : \mathbb{F}_2^n \to \mathbb{F}_2$ nazveme booleovský polynom $p \in \mathbb{F}_2[x_1,...,x_n]$ splňující $f = \overline{p}$.*

Následující tvrzení nám říká, že algebraická normální forma booleovské funkce je určena jednoznačně.

Tvrzení 1. *Každou booleovskou funkci n proměnných lze jednoznačně vyjádřit booleovským polynomem z $\mathbb{F}_2[x_1,...,x_n]$.*

Výše zmíněné nám dává dvě reprezentace booleovských funkcí. Buď se používá algebraická normální forma (ANF), nebo 2^n-bitový vektor zvaný vektor hodnot.

Příklad. Algebraická normální forma $f = x_1 + x_3 + x_2x_3$ nám dá následující vektor hodnot $v = (0,1,0,1,1,1,0,1)$, kde v_i získáme jako funkční hodnotu $f(i)$.

Definice 4. *Stupeň booleovské funkce definujeme jako stupeň algebraické normální formy funkce.*

Definice 5 (Incidenční vektor)**.** *Nechť $X \subseteq \mathbb{F}_2^n$. Incidenční vektor v_X množiny X je 2^n-bitový vektor, který má na pozici $x \in \mathbb{F}_2^n$ jedničku právě tehdy, když $x \in X$.*

Příklad. Mějme množinu $X = \{(0,0,1),(0,1,0),(0,1,1),(1,1,1)\}$. Incidenční vektor $v_X = (0,1,1,1,0,0,0,1)$.

Definice 6. *Nechť x, u jsou n-bitová slova. Pro ně definujeme $u \preceq x$ jako $u_i \leq x_i$ pro všechna $1 \leq i \leq n$.*

Předchozí vztah mezi n-bitovými slovy je částečné uspořádání. Tedy je

reflexivní: $x \preceq x$

slabě antisymetrické: $x \preceq u \wedge u \preceq x \Rightarrow x = u$

tranzitivní: $x \preceq u \wedge u \preceq v \Rightarrow x \preceq v$.

Jestliže $u \preceq x$, pak je support u obsažen v supportu x. To znamená, že všechny nenulové složky u jsou nenulové i v x.

Tento vztah mezi n-bitovými slovy budeme využívat na vyhodnocování monomů v bodě.

Lemma 2. *Nechť x a u jsou dvě n-bitová slova. Pak $x^u = 1$ právě tehdy, když $u \preceq x$.*

Důkaz. $\Rightarrow$ Rozepíšeme si $x^u = \prod_{i=1}^n x_i^{u_i} = 1$. Z toho plyne, že $x_i^{u_i} = 1$ pro všechna i.

$$x_i^{u_i} = 1 \Rightarrow \begin{cases} x_i = 1 & \Rightarrow u_i = 1 \text{ nebo } u_i = 0, \\ x_i = 0 & \Rightarrow u_i = 0. \end{cases}$$

Celkem $u_i \leq x_i \ \forall i \Rightarrow u \preceq x$.

$\Leftarrow$ Stejně tak $u \preceq x \Rightarrow \forall i \ u_i \leq x_i$.

$$x_i^{u_i} = \left.\begin{cases} x_i = 1 & \Rightarrow u_i = 1 \text{ nebo } u_i = 0 \\ x_i = 0 & \Rightarrow u_i = 0 \end{cases}\right\} = 1.$$

Tedy $\forall i \ x_i^{u_i} = 1 \Rightarrow x^u = 1$. □

Lemma 3. *Nechť x,y a u jsou tři n-bitová slova. Pak*

$$(x+y)^u = \sum_{v \preceq u} x^v y^{u+v}.$$

Důkaz. Z definice $(x+y)^u = \prod_{i=1}^n (x_i + y_i)^{u_i}$. Podíváme se na jednotlivé souřadnice $(x_i + y_i)^{u_i}$.

$$\begin{aligned}(x_i + y_i)^{u_i} &= \begin{cases} x_i + y_i = x_i^1 y_i^0 + x_i^0 y_i^1 & \text{pokud } u_i = 1, \\ 1 = x_i^0 y_i^0 & \text{pokud } u_i = 0, \end{cases} \\ &= \sum_{v_i \leq u_i} x_i^{v_i} y_i^{v_i + u_i}.\end{aligned}$$

Tím jsme dostali $\prod_{i=1}^n (\sum_{v_i \leq u_i} x_i^{v_i} y_i^{v_i+u_i})$, což nám z definice dává $\sum_{v \preceq u} x^v y^{u+v}$. □

Definice 7. *Nechť $u \in \mathbb{F}_2^n$. Pak definujeme*

$$\begin{aligned}\mathrm{Prec}(u) &= \{x \in \mathbb{F}_2^n : x \preceq u\}\\ \mathrm{Succ}(u) &= \{x \in \mathbb{F}_2^n : u \preceq x\}.\end{aligned}$$

$\mathrm{Prec}(u)$ je podprostor $\mathbb{F}_2^n$ dimenze $wt(u)$, protože $\mathrm{Prec}(u) \subseteq \mathbb{F}_2^n$ a zároveň je uzavřeno na sčítání a na násobení skalárem. Bázi $\mathrm{Prec}(u)$ tvoří právě ta slova váhy 1, neboli vektory kanonické báze, jejichž support leží v supportu u. Těch je přesně $wt(u)$.

Zatímco $\mathrm{Succ}(u)$ je tvaru $u+\mathrm{Prec}(\mathbf{1}-u)$, kde $\mathrm{Prec}(\mathbf{1}-u)$ je vektorový podprostor $\mathbb{F}_2^n$ a tedy $\mathrm{Succ}(u)$ je afinní podprostor $\mathbb{F}_2^n$. Z předchozího odstavce dostáváme, že dimenze $\mathrm{Succ}(u)$ je $n - wt(u)$.

Příklad. Mějme $u = (1,0,1,0)$, pak

$$\begin{aligned}\mathrm{Prec}(u) &= LO(e_1,e_3)\\ &= \{(0,0,0,0),(0,0,1,0),(1,0,0,0),(1,0,1,0)\}\\ \mathrm{Succ}(u) &= (1,0,1,0) + LO(e_2,e_4)\\ &= \{(1,0,1,0),(1,0,1,1),(1,1,1,0),(1,1,1,1)\}.\end{aligned}$$

1.4 Reed-Mullerovy kódy

Definice 8 (Minimální váha)**.** *Minimální váha nenulového lineárního kódu C se rozumí* $\min\{wt(u) \mid u \in C, u \neq 0\}$.

Definice 9 (Minimální vzdálenost)**.** *Minimální vzdálenost kódu C definujeme jako* $\min\{wt(u-v) \mid u,v \in C, u \neq v\}$.

Pro nenulové lineární kódy je minimální váha kódu rovna minimální vzdálenosti.

Definice 10 (Reed-Mullerův kód)**.** *Nechť $n, r \in \mathbb{Z}$ takové, že $0 \leq r \leq n$. Reed-Mullerovův kód $\mathcal{R}(r,n)$ je binární kód stupně r a délky 2^n, který je tvořen vektory hodnot všech booleovských funkcí n proměnných stupně nejvýše r:*

$$\mathcal{R}(r,n) = \{(f(x), x \in \mathbb{F}_2^n), f : \mathbb{F}_2^n \to \mathbb{F}_2, \text{ kde } deg(f) \leq r\}.$$

Na incidenční vektor množiny $X \subseteq \mathbb{F}_2^n$ můžeme pohlížet jako na kódové slovo z Reed-Mullerových kódů. Tento pohled v dalších sekcích využijeme.

Tvrzení 4. *Buď $0 \leq r \leq n$. Pak $\mathcal{R}(r,n)$ je lineární binární kód délky 2^n dimenze $\binom{n}{0} + \ldots + \binom{n}{r}$ a minimální vzdálenosti 2^{n-r}.*

Navíc bázi tvoří vektory hodnot booleovských funkcí s algebraickou normální formou x^u, kde $wt(u) \leq r$.

Definice 11 (Generující matice $\mathcal{R}(r,n)$)**.** *Označme k dimenzi Reed-Mullerova kódu $\mathcal{R}(r,n)$. Generující matice je matice $k \times 2^n$, jejíž řádky tvoří bázi $\mathcal{R}(r,n)$.*

Tvrzení 5. *Reed-Mullerovi kódy $\mathcal{R}(r,n)$ a $\mathcal{R}(n-r-1,n)$ jsou navzájem duální, tzn.*

$$\mathcal{R}(r,n)^\perp = \mathcal{R}(n-r-1,n).$$

Následují tvrzení je převzato z knihy MacWilliams a Sloane (1977) (strana 380, Tvrzení 8).

Tvrzení 6. *Kódová slova $\mathcal{R}(r,n)$ minimální váhy jsou právě incidenční vektory afinních podprostorů dimenze $n - r$.*

2. Dělící vlastnost

V této kapitole budeme zpracovávat teorii ze článku Boura a Canteaut (2016), kterou doplňuji o vlastní příklady.

2.1 Množina parit dané množiny

Definice 12 (Množina parit)**.** *Nechť X je možina prvků z $\mathbb{F}_2^n$. Množina parit X je podmožina $\mathbb{F}_2^n$ a je definována jako*

$$\mathcal{U}(X) = \{u \in \mathbb{F}_2^n, \sum_{x \in X} x^u = 1\}.$$

Ukážeme, že množina parit jednoznačně určuje danou množinu a naopak. To se nám v další sekci bude hodit při vyjádření dělící vlastnosti dané množiny.

Definice 13. *Nechť G je binární matice $2^n \times 2^n$. Prvky této matice jsou indexovány podle číselných hodnot n-bitových vektorů a jsou definovány jako*

$$G_{u,a} = a^u, a,u \in \mathbb{F}_2^n.$$

V následujícím textu bude G značit výhradně tuto matici.

Lemma 7. *Řádky G odpovídající vektorům u váhy nejvýše r tvoří generující matici Reed-Mullerova kódu stupně r a délky 2^n.*

Důkaz. Indukcí přes r.

Pro $r = 0$. Vektor váhy 0 je pouze jeden, a to $u = \mathbf{0}$. Z lemmatu 2 obsahuje matice G na řádku u samé 1. Taková matice generuje $\mathcal{R}(0,n)$.

Pro $r+1$. Z indukčího předpokladu máme, že řádky G odpovídající vektorům u váhy nejvýše r tvoří generující matici $\mathcal{R}(r,n)$. Díky tvrzení 4 už nám jen zbývá dokázat, že řádky G odpovídající vektorům u, pro které $wt(u) = r + 1$, generují vektory hodnot booleovských funkcí a ANF x^u pro $wt(u) = r + 1$.

Monomy stupně $r+1$ jsou generovány x^u přes všechny u splňující $wt(u) = r+1$. Pak vektor hodnot $(x^u, x \in \mathbb{F}_2^n)$ je přesně u-tý řádek matice G. Tedy u-té řádky G pro $wt(u) \leq r + 1$ generují $\mathcal{R}(r + 1,n)$. □

Důsledek. Matice G je generující matice Reed-Mullerova kódu stupně n a délky 2^n.

Lemma 8. *Pak pro každou podmnožinu $X \subseteq \mathbb{F}_2^n$ je incidenční vektor $\mathcal{U}(X)$ roven součinu G s incidenčním vektorem X.*

Důkaz. Gv_X je roven součtu právě těch sloupců, jejichž index je prvkem supportu v_X, tj. indexy jež jsou prvky X:

$$(Gv_X)_u = \sum_{x \in X} G_{u,x} = \sum_{x \in X} x^u.$$

Množina parit $\mathcal{U}(X)$ je rovna $\{u \in \mathbb{F}_2^n, \sum_{x \in X} x^u = 1\}$. Tedy support $v_{\mathcal{U}(X)}$ je množina všech u takových, že $\sum_{x \in X} x^u = (Gv_X)_u = 1$. □

Věta 9. *G je regulární matice a $G^{-1} = G$. Proto pro každou podmnožinu $U \subseteq \mathbb{F}_2^n$ existuje právě jedna množnina $X \subseteq \mathbb{F}_2^n$ taková, že $\mathcal{U}(X) = U$.*

Důkaz. G je podle lemmatu 7 generující matice Reed-Mullerova kódu délky 2^n a stupně n. Tento kód má podle tvrzení 4 dimenzi $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ tj. G je regulární. Navíc pro u,$w \in \mathbb{F}_2^n$ máme

$$(G \cdot G)_{u,w} = \sum_{v \in \mathbb{F}_2^n} G_{u,v} G_{v,w} = \sum_{v \in \mathbb{F}_2^n} v^u w^v$$

Lemma 2 nám říká, že $x^y = 1 \Leftrightarrow y \preceq x$. Z toho dostáváme:

$$\begin{aligned} \sum_{v \in \mathbb{F}_2^n} v^u w^v &= |\{v \in \mathbb{F}_2^n : u \preceq v \text{ a } v \preceq w\}| \bmod 2 \\ &= \begin{cases} 2^{wt(w)-wt(u)} \bmod 2 & \text{pokud } u \preceq w, \\ 0 & \text{jinak.} \end{cases} \end{aligned}$$

Dále pokud $wt(w) - wt(u) > 0$, pak $2^{wt(w)-wt(u)} \bmod 2 = 0$. Tedy $(G \cdot G)_{u,w} = 1$, pouze pokud $wt(w) - wt(u) = 0$ pro $u \preceq w$. Což je pouze právě tehdy, když $u = w$, tj. $(G \cdot G) = I$. Tedy $G = G^{-1}$.
Díky lemmatu 8 dostáváme, že zobrazení $v_X \mapsto v_{\mathcal{U}(X)}$ je automorfismus vektorových prostorů $\mathbb{F}_2^{2^n} \to \mathbb{F}_2^{2^n}$. □

Předchozí věta nám dává snadnou cestu, jak nalézt množinu X odpovídající dané množině parit U.

Důsledek. Nechť X je podmnožina $\mathbb{F}_2^n$. Pak

- $\mathcal{U}(X)$ je prázdná množina právě tehdy, když X je prázdná množina.
- $\mathcal{U}(X) = \mathrm{Prec}(x)$ právě tehdy, když $X = \{x\}$.
- $\mathcal{U}(X) = \{u\}$ právě tehdy, když $X = \mathrm{Prec}(u)$.
- $\mathcal{U}(X) = \{\mathbf{1}\}$ právě tehdy, když $X = \mathbb{F}_2^n$.

Příklad. Konkrétní příklady na převod množiny z $\mathbb{F}_2^3$ na jí odpovídající množinu parit a naopak.

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Nalezneme pro množiny X pomocí G jejich množiny parit.

- Množina $X = \{(1,0,0),(0,0,1)\}$, její incidenční vektor $v_X = (0,1,0,0,1,0,0,0)$.
  $v_{\mathcal{U}(X)} = G v_X = (0,1,0,0,1,0,0,0)$.
  Množina parit $\mathcal{U}(X) = \{(1,0,0),(0,0,1)\}$.

- Množina $X = \{(1,1,0),(0,0,1)\}$, její incidenční vektor $v_X = (0,1,0,0,0,0,1,0)$.
  $v_{\mathcal{U}(X)} = Gv_X = (0,1,1,0,1,0,1,0)$.
  Množina parit $\mathcal{U}(X) = \{(1,0,0),(0,1,0),(1,1,0),(0,0,1)\}$.

A naopak pro množiny parit U nalezneme jím odpovídající množiny X.

- $\mathcal{U}(X) = \{(1,0,0),(1,0,1)\}$, její incidenční vektor $v_{\mathcal{U}(X)} = (0,0,0,0,1,1,0,0)$.
  $v_X = Gv_{\mathcal{U}(X)} = (0,1,0,0,0,1,0,0)$.
  Z toho dostaneme, že množina $X = \{(1,0,1),(0,0,1)\}$.

- Množina parit $\mathcal{U}(X) = \{(0,1,0),(1,0,1),(1,1,1)\}$ a její incidenční vektor $v_{\mathcal{U}(X)} = (0,0,1,0,0,1,0,1)$.
  $v_X = Gv_{\mathcal{U}(X)} = (1,0,0,1,0,0,1,1)$.
  Z toho dostaneme, že množina $X = \{(0,0,0),(0,1,1),(1,1,0),(1,1,1)\}$.

2.2 Dělící vlastnost pomocí množiny parit

Definice 14 (Dělící vlastnost)**.** *Nechť $X \subseteq \mathbb{F}_2^n$ a $0 \leq k \leq n$. Řekneme, že X má dělící vlastnost stupně k, značíme $\mathcal{D}_k^n$, pokud*

$$\sum_{x \in X} x^u = 0 \text{ pro všechny } u \in \mathbb{F}_2^n \text{ takové, že } wt(u) < k.$$

Příklad. Mějme množinu $X = \{(0,0,1),(0,1,1),(1,0,1),(1,1,1)\}$.

	$(0,0,1)^u$	$(0,1,1)^u$	$(1,0,1)^u$	$(1,1,1)^u$	$\sum x^u$
$u = (0,0,0)$	1	1	1	1	0
$u = (0,0,1)$	1	1	1	1	0
$u = (0,1,0)$	0	1	0	1	0
$u = (0,1,1)$	0	1	0	1	0
$u = (1,0,0)$	0	0	1	1	0
$u = (1,0,1)$	0	0	1	1	0
$u = (1,1,0)$	0	0	0	1	1
$u = (1,1,1)$	0	0	0	1	1

Pro všechny u splňující $wt(u) < 2$ platí, že $\sum_{x \in X} x^u = 0$, tedy množina X splňuje dělící vlastnost $\mathcal{D}_2^3$.

Nyní znovu zformulujeme dělící vlastnost stupně k množiny X pomocí vlastnosti $\mathcal{U}(X)$.

Tvrzení 10. *Množina X prvků z $\mathbb{F}_2^n$ splňuje dělící vlastnost stupně k, $\mathcal{D}_k^n$, právě tehdy, když všechny prvky z $\mathcal{U}(X)$ mají váhu alespoň k, tj.*

$$\mathcal{U}(X) \subseteq \{u \in \mathbb{F}_2^n : wt(u) \geq k\}.$$

Důkaz. $\Leftarrow$ Rozepíšeme si definici množiny parit

$$\mathcal{U}(X) = \{u \in \mathbb{F}_2^n : \sum_{x \in X} x^u = 1\} \subseteq \{u \in \mathbb{F}_2^n : wt(u) \geq k\}.$$

Z toho vidíme, že když $\sum_{x \in X} x^u = 1$, pak $wt(u) \geq k$. Naopak pro všechny $wt(u) < k$ je součet $\sum_{x \in X} x^u = 0$. Tedy X splňuje dělící vlastnost stupně k.

$\Rightarrow$ Nechť X splňuje $\mathcal{D}_k^n$, pak $\sum_{x\in X} x^u = 0\ \forall u \in \mathbb{F}_2^n$ takové, že $wt(u) < k$. To znamená, že

$$\mathcal{U}(X) \subset \mathbb{F}_2^n \setminus \{u \in \mathbb{F}_2^n \mid wt(u) < k\} = \{u \in \mathbb{F}_2^n \mid wt(u) \geq k\}.$$

□

Z toho vidíme, že pokud množina splňuje dělící vlastnost stupně k, pak také splňuje dělící vlastnost stupně l pro každé $l < k$.

Příklad. Mějme množinu $X = \{(0,0,1),(0,1,1),(1,0,1),(1,1,1)\}$ z minulého příkladu. Ze vztahů z lemmatu 8 spočteme množinu parit $\mathcal{U}(X)$

$$v_X = (0,1,0,1,0,1,0,1) \Rightarrow v_{\mathcal{U}(X)} = Gv_X = (0,0,0,0,0,0,1,1).$$

Množina parit $\mathcal{U}(X) = \{(1,1,0),(1,1,1)\} \subseteq \{u \in \mathbb{F}_2^n : wt(u) \geq 2\}$. Tím jsme došli ke stejnému výsledku a to, že X splňuje dělící vlastnost $\mathcal{D}_2^3$.

Následující tvrzení nám definuje vztah mezi Reed-Mullerovými kódy a množinou splňující dělící vlastnost.

Tvrzení 11. *Nechť X je množina prvků z $\mathbb{F}_2^n$ a k je celé číslo takové, že $1 \leq k \leq n$. Pak jsou následující tvrzení ekvivalentní.*

(1) *X splňuje dělící vlastnost stupně k, $\mathcal{D}_k^n$.*

(2) *Incidenční vektor X patří k Reed-Mullerovu kódu délky 2^n stupně $(n-k)$, tedy $v_X \in \mathcal{R}(n-k,n)$.*

(3) *Incidenční vektor X patří do duálu k Reed-Mullerovu kódu délky 2^n stupně $(k-1)$, tedy $v_X \in \mathcal{R}(k-1,n)^\perp$.*

Důkaz. Označme G' restrikci G na řádky s indexem u pro $wt(u) \leq k-1$. Pak podle lemmatu 7 je G' generující matice Reed-Mullerova kódu délky 2^n stupně $(k-1)$.

(3) $\Rightarrow$ (1): Bod (3) nám říká, že $v_X \in \mathcal{R}(k-1,n)^\perp$. Tedy $G'v_X = \mathbf{0}$. Takže incidenční vektor $\mathcal{U}(X)$ bude nulový na všech pozicích u, kde $wt(u) \leq k-1$. To znamená, že množina parit $\mathcal{U}(X)$ obsahuje pouze prvky, jejichž Hammingova váha je větší nebo rovna k. Tím pádem $\mathcal{U}(X)$ spňuje podmínku v tvrzení 10.

(1) $\Rightarrow$ (3): Z toho, že množina X splňuje $\mathcal{D}_k^n$ dostáváme, že incidenční vektor $v_{\mathcal{U}(X)}$ obsahuje 1 pouze na indexech i, pro které platí $wt(i) \geq k$. Pak podle lemmatu 8 $G'v_X = \mathbf{0}$.

Navíc je množina všech v_X splňujících $G'v_X = \mathbf{0}$ duální k $\mathcal{R}(k-1,n)$. Tedy $v_X \in \mathcal{R}(k-1,n)^\perp$.

(2) $\Leftrightarrow$ (3): Z tvrzení 5 máme, že duál k $\mathcal{R}(n-k,n)$ je $\mathcal{R}(k-1,n)$. Tedy incidenční vektor v_X patří do $\mathcal{R}(n-k,n)$ právě tehdy, když v_X patří do duálu k $\mathcal{R}(k-1,n)$. □

Tvrzení 12. *Nechť X je neprázdná podmnožina $\mathbb{F}_2^n$ splňující $\mathcal{D}_k^n$. Pak*

$$|X| \geq 2^k.$$

Navíc množina X velikosti 2^k splňuje $\mathcal{D}_k^n$ právě tehdy, když X je afinní podprostor dimenze k.

Důkaz. Využijeme tvrzení 11, že X splňuje $\mathcal{D}_k^n$ právě tehdy, když v_X patří do $\mathcal{R}(n-k,n)$. Podle tvrzení 4 minimální vzdálenost $\mathcal{R}(n-k,n)$ je $2^{n-(n-k)} = 2^k$. Tedy $wt(v_X) \geq 2^k$. Zároveň $wt(v_X) = |X|$, takže celkem dostáváme $|X| \geq 2^k$.

Tvrzení 6 nám říká, že kódová slova s minimální váhou v $\mathcal{R}(n-k,n)$ jsou incidenční vektory afinních podprostorů dimenze k. Z toho vyplývá, že množina velikosti 2^k splňuje $\mathcal{D}_k^n$ právě tehdy, když je afinním podprostorem dimenze k. □

2.3 Stupeň dělící vlastnosti

Nejdříve se podíváme, jak vypadá Reed-Mullerův kód stupně 0

$$\mathcal{R}(0,n) = \{(f(x), x \in \mathbb{F}_2^n) : \deg(f) = 0\} = \{\mathbf{0},\mathbf{1}\}.$$

Pak podle tvrzení 11 dostáváme:

$$\begin{aligned} \text{Množina } X \text{ splňuje } \mathcal{D}_1^n &\Leftrightarrow v_X \in \mathcal{R}(0,n)^\perp \\ &\Leftrightarrow \mathbf{1}v_X = \mathbf{0} \\ &\Leftrightarrow \text{počet 1 v incidenčním vektoru } v_X \text{ je sudý.} \end{aligned}$$

Důsledek. Z předešlého nám plyne následující poznatek

- Množina X splňuje $\mathcal{D}_1^n$ právě tehdy, když je její mohutnost sudá

Tvrzení 13. *Nechť $X \subseteq \mathbb{F}_2^n$. Pak jsou následující podmínky ekvivalentní.*

(1) *X splňuje dělící vlastnost stupně k, $\mathcal{D}_k^n$.*

(2) *Pro libovolnou množinu souřadnic $\{i_1,...,i_t\} \subseteq \{1,...,n\}$ velikosti $t < k$ a konstantu $\alpha \in \mathbb{F}_2^t$ je počet prvků v X takových, že $x_{i_j} = \alpha_j$ pro všechny $1 \leq j \leq t$, sudý.*

(3) *Pro libovolnou množinu souřadnic $\{i_1,...,i_t\} \subseteq \{1,...,n\}$ velikosti $t < k$ je počet prvků v X takových, že $x_{i_j} = 0$ pro všechny $1 \leq j \leq t$, sudý.*

Důkaz. (1) ⇒ (2): Nechť $I = \{i_1,...,i_t\}$ je množina velikosti $t < k$ a u je vektor z $\mathbb{F}_2^n$ pro který platí $\text{supp}(u) = I$. Dále definujeme $\beta \in \mathbb{F}_2^n$ následovně: $\beta_{i_j} = (\alpha_j + 1)$ pro $1 \leq j \leq t$ a $\beta_i = 0$ pro $i \notin I$. Pak

$$\{x \in X : x_{i_j} = \alpha_j, 1 \leq j \leq t\} = \{x \in X : (x+\beta) \succeq u\}.$$

Důkaz rovnosti těchto množin:
⊆ Nechť $x \in \{x \in X : x_{i_j} = \alpha_j, 1 \leq j \leq t\}$. Pak

$$(x+\beta) = \begin{cases} x_{i_j} + \alpha_j + 1 = x_{i_j} + x_{i_j} + 1 = 1 & \text{pokud } 1 \leq j \leq t, \\ x_{i_j} + 0 = x_{i_j} & \text{jinak.} \end{cases}$$

Stejně tak z toho, že $\text{supp}(u) = I = \{i_1,...,i_t\}$ máme

$$u = \begin{cases} u_{i_j} = 1 & \text{pokud } 1 \leq j \leq t, \\ u_{i_j} = 0 & \text{jinak.} \end{cases}$$

Z toho plyne, že $(x+\beta) \succeq u \Rightarrow x \in \{x \in X : (x+\beta) \succeq u\}$.

$\supseteq$ Naopak nechť $x \in \{x \in X : (x+\beta) \succeq u\}$. Zároveň $\mathrm{supp}(u) = I = \{i_1,...,i_t\}$. Tedy

$$(x+\beta) = \begin{cases} x_{i_j} + \alpha_j + 1 \leq 1 & \text{pokud } 1 \leq j \leq t, \\ x_{i_j} \geq 0 & \text{jinak.} \end{cases}$$

Takže $x_{i_j} = \alpha_j$ pro všechna $1 \leq j \leq t \Rightarrow x \in \{x \in X : x_{i_j} = \alpha_j, 1 \leq j \leq t\}$.

Déle z lemmatu 2 a lemmatu 3 dostáváme

$$\begin{aligned} \mid \{x \in X : (x+\beta) \succeq u\} \mid \mod 2 &= \sum_{x \in X} (x+\beta)^u = \sum_{x \in X} \sum_{v \preceq u} x^v \beta^{u+v} \\ &= \sum_{v \preceq u} \beta^{u+v} (\sum_{x \in X} x^v) \end{aligned}$$

X splňuje dělící vlastnost stupně k a $wt(v) \leq wt(u) < k$, tedy $\sum_{x \in X} x^v = 0$ pro všechny $v \preceq u$.

(2) $\Rightarrow$ (3): Po zvolení nulového vektoru za α dostaneme bod (3).

(3) $\Rightarrow$ (1): Nechť $u \in \mathbb{F}_2^n$ a $wt(u) < k$. Pak

$$\begin{aligned} \sum_{x \in X} x^u &= \sum_{x \in X} ((x+u)+u)^u \\ &= \sum_{v \preceq u} \sum_{x \in X} (x+u)^v u^{u+v} \\ &= \sum_{v \preceq u} \sum_{x \in X} (x+u)^v \\ &= \sum_{v \preceq u} \mid \{x \in X : x_i = 0, \forall i \in \mathrm{supp}(v)\} \mid \mod 2. \end{aligned}$$

Ve druhé rovnosti jsme použili lemma 3.

Ve třetí rovnosti jsme použili, že pokud $v \preceq u$, pak i $u + v \preceq u$ a lemma 2, podle kterého pro všechny $u + v \preceq u$ platí $u^{u+v} = 1$.

Podle bodu (3) mají množiny $\{x \in X : x_i = 0, \forall i \in \mathrm{supp}(v)\}$ sudou velikost, protože $wt(v) \leq wt(u) < k$. Z toho dostáváme, že $\sum_{x \in X} x^u = 0$ a tedy X splňuje dělící vlastnost stupně k. □

Z tvrzení 13 máme, že X splňuje $\mathcal{D}_2^n$ právě tehdy, když je počet prvků, pro které platí $x_i = 1$ pro libovolné i, sudý. To znamená, že $\sum_{x \in X} x_i = 0$ pro všechna i.

Dále X splňuje $\mathcal{D}_3^n$ pokud platí předcházející a navíc libovolná dvojice (i,j) splňuje, že počet prvků majících $x_i = x_j = 1$ je sudý. Vytvořme podmnožiny $M_i = \{x \in X : x_i = 1\} \subset X$. Pak pro libovolné j je počet prvků $x_j = 1$ v množině M_i sudý pro fixní i.

Důsledek. To nám dává charakteristiku množiny $X \subseteq \mathbb{F}_2^n$ splňující dělící vlastnost stupně 2 a 3.

- Množina X splňuje $\mathcal{D}_2^n$ právě tehdy, když je její mohutnost sudá a zároveň $\sum_{x \in X} x = 0$.

- Množina X splňuje dělící vlastnost $\mathcal{D}_3^n$ právě tehdy, když $\sum_{x \in X} x = 0$ a zároveň pro všech n podmnožin $M_i = \{x \in X : x_i = 1\}$, kde $i = \{1,...,n\}$, platí $\sum_{x \in M_i} x = 0$.

Podle tvrzení 10 množina $X \subseteq \mathbb{F}_2^n$ splňuje dělící vlastnost maximálního stupně $\mathcal{D}_n^n$ právě tehdy, když platí

$$\mathcal{U}(X) \subseteq \{u \in \mathbb{F}_2^n : wt(u) \geq n\}.$$

To může nastat, jen když $\mathcal{U}(X)$ je buď prázdná množina, nebo $\mathcal{U}(X) = \{\mathbf{1}\}$. Z důsledku na konci sekce 2.1 vidíme, že to odpovídá tomu, že X je buď prázdná množina, nebo se rovná celému $\mathbb{F}_2^n$.

3. Substitučně permutační síť

V této kapitole budeme interpretovat výsledky ze článku Boura a Canteaut (2016) doplněné o ilustrující příklady.

SPN neboli substitučně permutační síť je struktura blokové šifry. Ta obsahuje rundovní funkci, která se skládá ze substituční vrsty a permutační vrsty. Bloková šifra pak vzniká iterováním této rundovní funkce.

Rundovní klíč je pro každou rundu jiný a všechny vznikají z hlavního klíče při takzvané expanzi klíče. Substituční vrsta je konkatenace několika S-boxů. Každý z nich je nelineární funkce z $\mathbb{F}_2^n$ do $\mathbb{F}_2^m$ a často jsou implementovány jako vyhledávací tabulka. Permutační vrstva je bijekce na bitech.

Dále v textu budeme uvažovat SPN pouze s bijektivními S-boxy z $\mathbb{F}_2^n$ do $\mathbb{F}_2^n$.

Definice 15. *Nechť S je permutace na $\mathbb{F}_2^n$, $S_1,...,S_n : \mathbb{F}_2^n \to \mathbb{F}_2$ jsou projekce do složek S a $x = (x_1,...,x_n)$, $u = (u_1,...,u_n)$ jsou vektory z $\mathbb{F}_2^n$. Definujeme*

$$S^u(x) = \prod_{i=1}^{n} S_i(x)^{u_i}.$$

Ukážeme šíření informace na množině parit výstupních množin skrz po sobě jdoucích rund substitučně permutační sítě.

3.1 Přidání klíče

Následující tvrzení nám říká, jak se změní množina parit původní množiny po přidání klíče $k \in \mathbb{F}_2^n$. Přidání klíče se nejčastěji provádí pomocí operace XOR po složkách, tedy sčítáním ve vektorovém prostoru $\mathbb{F}_2^n$.

Tvrzení 14. *Nechť X je podmnožina $\mathbb{F}_2^n$ a $\mathcal{U}(X)$ je množina parit X. Pak pro každé $k \in \mathbb{F}_2^n$ množina parit $\mathcal{U}(k+X)$ splňuje*

$$\mathcal{U}(k+X) \subseteq \bigcup_{u \in \mathcal{U}(X)} \mathrm{Succ}(u).$$

Důkaz. Z definice $\mathcal{U}(k+X) = \{u \in \mathbb{F}_2^n : \sum_{x\in X}(k+x)^u = 1\}$.

Použijeme lemma 3, které říká, že

$$(x+k)^u = \sum_{v \preceq u} x^v k^{v+u}.$$

Pak

$$\sum_{x\in X}(x+k)^u = \sum_{x\in X}\sum_{v\preceq u} x^v k^{v+u} = \sum_{v\preceq u} k^{v+u}(\sum_{x\in X} x^v).$$

Nechť $u \in \mathcal{U}(k+X)$, pak $\sum_{v\preceq u} k^{v+u}(\sum_{x\in X} x^v) = 1$. Pokud se tato suma se rovná jedné, pak existuje aspoň jedno v takové, že $\sum_{x\in X} x^v = 1$. Z definice množiny parit $\sum_{x\in X} x^v = 1 \Leftrightarrow v \in \mathcal{U}(X)$.

Celkem $u \in \mathcal{U}(k+X) \Rightarrow$ existuje v takové, že $v \preceq u$ a $v \in \mathcal{U}(X)$. Takže

$$\mathcal{U}(k+X) \subseteq \bigcup_{v\in\mathcal{U}(X)} \{u \in \mathbb{F}_2^n : v \preceq u\} = \bigcup_{v\in\mathcal{U}(X)} \mathrm{Succ}(v).$$

□

3.2 Substituční a permutační vrstva

V této sekci ukážeme, jak se množina parit šíří permutací (např. bijektivním S-boxem nebo lineární permutací).

Definice 16. *Nechť S je permutace na $\mathbb{F}_2^n$. Pro $u \in \mathbb{F}_2^n$ definujeme*

$$V_S(u) = \{v \in \mathbb{F}_2^n : \textit{algebraická normální forma } S^v(x) \textit{ obsahuje člen } x^u\}.$$

Tvrzení 15. *Nechť S je permutace na $\mathbb{F}_2^n$ a $X \subseteq \mathbb{F}_2^n$. Pak platí,*

$$\mathcal{U}(S(X)) \subseteq \bigcup_{u \in \mathcal{U}(X)} V_S(u).$$

Důkaz.

$$\mathcal{U}(S(X)) = \{v \in \mathbb{F}_2^n : \sum_{x \in X} S^v(x) = 1\}.$$

Ze sekce 1.2 o booleovských funkcích víme, že booleovskou funkci S^v lze jednoznačně vyjádřit algebraickou normální formou, tj. polynomem $\sum_{u \in M} x^u$ pro nějaké $M \subseteq \mathbb{F}_2^n$.

Pro pevné S označme $M_v \subseteq \mathbb{F}_2^n$ množinu exponentů, pro které platí $u \in M_v$ právě tehdy, když ANF $S^v(x)$ obsahuje člen x^u. V tomto značení je množina $V_S(u) = \{v \in \mathbb{F}_2^n : u \in M_v\}$.

Díky tomu můžeme součet $\sum_{x \in X} S^v(x)$ napsat jako

$$\begin{aligned}\sum_{x \in X} S^v(x) &= \sum_{x \in X} \sum_{u \in M_v} x^u \\ &= \sum_{u \in M_v} (\sum_{x \in X} x^u).\end{aligned}$$

Pokud se tento součet rovná jedné, pak existuje aspoň jedno $u \in M_v$ takové, že $\sum_{x \in X} x^u = 1$. Tedy ANF $S^v(x)$ obsahuje člen x^u pro $u \in \mathcal{U}(X)$, kde

$$\mathcal{U}(X) = \{u \in \mathbb{F}_2^n : \sum_{x \in X} x^u = 1\}.$$

Celkem

$$\mathcal{U}(S(X)) \subseteq \bigcup_{u \in \mathcal{U}(X)} \{v \in \mathbb{F}_2^n : u \in M_v\} = \bigcup_{u \in \mathcal{U}(X)} V_S(u).$$

□

Příklad. Rozebereme si, jak to vypadají množiny V_S pro šifru PRESENT. Algebraická normální forma PRESENT S-boxu je následující

$$\begin{aligned}S_1(x_1,x_2,x_3,x_4) &= x_1 + x_3 + x_4 + x_2x_3 \\ S_2(x_1,x_2,x_3,x_4) &= x_2 + x_4 + x_2x_4 + x_3x_4 + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 \\ S_3(x_1,x_2,x_3,x_4) &= 1 + x_3 + x_4 + x_1x_2 + x_1x_4 + x_2x_4 + x_1x_2x_4 + x_1x_3x_4 \\ S_4(x_1,x_2,x_3,x_4) &= 1 + x_1 + x_2 + x_4 + x_2x_3 + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4.\end{aligned}$$

	$V_S(u)$															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	x				x				x				x			
1		x				x			x				x			
2			x				x		x				x			
3				x	x	x	x			x	x	x	x			
4		x			x					x			x			
5						x				x			x			
6		x					x		x	x	x		x			
7			x	x			x		x	x		x		x		
8		x	x	x	x				x				x			
9				x	x	x	x				x				x	
a			x		x	x		x		x	x	x		x	x	x
b			x	x	x		x	x	x		x		x	x		x
c			x	x						x			x			
d			x		x			x	x	x	x				x	
e						x		x				x		x	x	x
f																x

Pozn: x značí prvky, které leží v množině $V_S(u)$ pro dané u.

Tabulka 3.1: $V_S(u)$ pro 4-bitová slova u a S-box ze šifry PRESENT

Z definice vektor $v \in V_S(u)$ právě tehdy, když ANF $S^v(x)$ obsahuje monom x^u. V našem případě $S^v(x) = S_1^{v_1}(x)S_2^{v_2}(x)S_3^{v_3}(x)S_4^{v_4}(x)$. Vezmeme u = (0,0,1,1) a v = (0,0,1,0). Pak

$$\begin{aligned} S^v(x) &= S_1^0(x)S_2^1(x)S_3^0(x)S_4^0(x) \\ &= x_2 + x_4 + x_2x_4 + x_3x_4 + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4. \end{aligned}$$

Tento polynom neobsahuje $x^u = x_1x_2$, tedy $v \notin V_S(u)$.

Naopak pro v = (0,0,1,1) máme

$$\begin{aligned} S^v(x) &= S_1^1(x)S_2^1(x)S_3^0(x)S_4^0(x) \\ &= x_1x_2 + x_1x_2x_3 + x_4 + x_1x_4 + x_1x_2x_4 + x_3x_4. \end{aligned}$$

Vidíme, že ANF $S^v(x)$ obsahuje polynom $x^u = x_1x_2$ a tedy $v \in V_S(u)$.

Tabulka 3.1 ukazuje zbylé množiny $V_S(u)$ pro všechna 4-bitová slova u a S-box ze šifry PRESENT. 4-bitová slova jsou zde v hexadecimálním zápise.

3.3 Šíření skrz rundu

Uvažujme SPN s bijektivními S-boxy, kde každá vrstva S-boxů následuje po přidání rundovního klíče. Z předchozích tvrzení dostáváme:

$$\mathcal{U}(S(X+k)) \subseteq \bigcup_{u \in \mathcal{U}(X+k)} V_S(u) \subseteq \bigcup_{u \in \mathcal{U}(X)} \left(\bigcup_{v \in \mathrm{Succ}(u)} V_S(v) \right).$$

Pro zjednodušení zavedeme následující značení.

Definice 17. *Nechť S je permutace na $\mathbb{F}_2^n$ a $u \in \mathbb{F}_2^n$. Pak definujeme*

$$\mathcal{V}_S(u) = \bigcup_{v \in \mathrm{Succ}(u)} V_S(v).$$

Pak máme

$$\mathcal{U}(S(X+k)) \subseteq \bigcup_{u \in \mathcal{U}(X)} \mathcal{V}_S(u).$$

Tedy šíření informace, v našem případě váhy prvků v množině, z $\mathcal{U}(X)$ do $\mathcal{U}(S(X+k))$ zahrnuje množiny $\mathcal{V}_S(u)$, které závisí pouze na S-boxech.

Příklad. Využijeme příkladu z předešlé sekce a ukážeme si, jak vypadá množina $\mathcal{V}_S$ pro šifru PRESENT a $u = (0011) = 0x3$.

Množina $\mathrm{Succ}(0x3) = \{(0011),(0111),(1011),(1111)\} = \{0x3,0x7,0xb,0xf\}$. Takže

$$\mathcal{V}_S(0x3) = V_S(0x3) \cup V_S(0x7) \cup V_S(0xb) \cup V_S(0xf).$$

Z tabulky 3.1 vidíme, že

$$\begin{aligned} V_S(0x3) &= \{0x3,0x4,0x5,0x6,0x9,0xa,0xb,0xc\} \\ V_S(0x7) &= \{0x2,0x3,0x6,0x8,0x9,0xb,0xd\} \\ V_S(0xb) &= \{0x2,0x3,0x4,0x6,0x7,0x8,0xa,0xc,0xd,0xf\} \\ V_S(0xf) &= \{0xf\}. \end{aligned}$$

Celkem $\mathcal{V}_S(0x3) = \{0x2,0x3,0x4,0x5,0x6,0x7,0x8,0x9,0xa,0xb,0xc,0xd,0xf\}$.

3.4 Rozlišovač na SPN

Označme E_K šifrovací funkci substitučně-permutační sítě s klíčem K. Zde si ukážeme pouze základní myšlenku tvoření rozlišovače pro danou funkci E_K pomocí množiny parit. Chceme zvolit vstup X takový, že množina parit odpovídajícího výstupu $E_K(X)$ má dělící vlastnost stupně 2 pro jakýkoli výběr klíče K. Tj. platí

$$\mathcal{U}(E_K(X)) \subseteq \{u \in \mathbb{F}_2^n : wt(u) \geq 2\}.$$

Dále pokud množina $E_K(X)$ spňuje dělící vlastnost stupně 2, pak podle důsledku v sekci 2.3 platí $\sum_{x \in E_K(X)} x = 0$ a mohutnost X je sudá. Tím jsou splněny podmínky na rozlišovač pro integrální útok tak, jak jsou uvedeny v motivaci v úvodu. Díky tomu lze postupně zjistit rundovní klíče dané šifry.

Příklad. Mějme blokovou šifru, kde za vstup jsou 4-bitová slova a klíč $K = (k_1,k_2,k_3)$, kde k_1,k_2,k_3 jsou rundovní klíče odvozené z K.

Šifrovací funkce $E_K(x) = k_3 + S(k_2 + S(k_1 + x))$, kde S je S-box ze šifry PRESENT. Chceme uhádnout rundovní klíč k_3.

Najdeme množinu $\mathcal{U}(S(k_1 + X))$, tak aby splňovala dělící vlastnost stupně 2. Pro takovou množinu díky tomu, že mohutnost $S(k_1 + X)$ je sudá, platí

$$\sum_{x \in (k_2 + S(k_1+X))} x = \sum_{x \in S(k_1+X)} x + k_2 = 0.$$

Dále víme, že

$$\mathcal{U}(S(k_1 + X)) \subseteq \bigcup_{u \in \mathcal{U}(X)} \mathcal{V}_S(u).$$

Takže hledáme u, pro která platí

$$\mathcal{V}_S(u) \subseteq \{u \in \mathbb{F}_2^n : wt(u) \geq 2\}.$$

Z tabulky 3.1 dohledáme, že slova v splňující $V_S(v) \subseteq \{u \in \mathbb{F}_2^n : wt(u) \geq 2\}$ jsou pouze $0x5, 0x9, 0xe, 0xf$.

Zároveň $\mathcal{V}_S(u) = \bigcup_{v \in \mathrm{Succ}(u)} V_S(v)$, takže odpovídající u jsou pouze $0xe$ nebo $0xf$.

Vybereme si $0xe$, tzn. $\mathcal{U}(X) = \{0xe\}$. Ze vztahu $v_X = Gv_{\mathcal{U}(X)}$ dostaneme, že množina $X = \{0x0, 0x2, 0x4, 0x6, 0x8, 0xa, 0xc, 0xe\}$.

Nyní každé slovo z X zašifrujeme funkcí E_K pro konkrétní klíč. Dále budeme tipovat k_3 a spočteme $Y = \{S^{-1}(E_K(x) + k_3) : x \in X\}$. Pokud platí $\sum_{y \in Y} y = 0$, pak jsme rundovní klíč k_3 tipnuli správně.

Závěr

V této práci jsme představili článek Boura a Canteaut (2016) o dělící vlastnosti. Ten jsme rozšířili o ilustrativní příklady a doplnili o důkazy, popřípadě je lépe zpracovali.

Zadefinovali jsme množinu parit množiny z $\mathbb{F}_2^n$ a následně vyjádřili dělící vlastnost množiny z $\mathbb{F}_2^n$ pomocí její množiny parit. To nám umožnilo lépe prozkoumat šíření této dělící vlastnosti skrz blokové šifry.

Motivací pro zkoumání dělící vlastnosti dané množiny je možnost integrální kryptoanalýzy na blokových šifrách jak bylo zmíněno v úvodu. Ale v této práci se dál praktickému využití nevěnuji, to by mohlo být námětem dalšího zkoumání.

Seznam použité literatury

Boura, C. a Canteaut, A. (2016). Another view of the division property. *Advances in Cryptology - CRYPTO 2016, LNCS vol. 9814, Springer, Heidelberg (2016)*, pages 654–682.

Drápal, A. *Samoopravné kódy.* URL `http://www.karlin.mff.cuni.cz/~holub/soubory/drapal_kody.pdf`.

MacWilliams, F. a Sloane, N. (1977). *The theory of Error-Correcting Codes.* North-Holland, Secaucus.

Todo, Y. (2015). Structural evaluation by generalized integral property. *Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 287–314. Springer, Heidelberg (2015)*, pages 112–127.