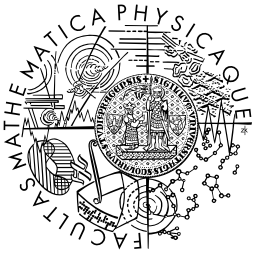


MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Kieu Trang Phamová

Integrální útok na blokové šifry Simon

Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. et Mgr. Jan Žemlička, Ph.D.
Studijní program: Matematika
Studijní obor: Matematika pro informační technologie

Praha 2021

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 ....

Podpis autora

Děkuji vedoucímu mé práce panu doc. Mgr. et Mgr. Janu Žemličkovi, Ph.D. za cenné připomínky a čas věnovaný konzultacím. Také chci poděkovat své rodině a svému manželovi Milanovi za neustálou podporu během studia. Děkuji svým kamarádkám za korekci práce a psychickou podporu.

Název práce: Integrální útok na blokové šifry Simon

Autor: Kieu Trang Phamová

Katedra: Katedra algebry

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

Abstrakt: Tato bakalářská práce pojednává o bitové dělící vlastnosti se třemi podmnožinami. Nejprve představíme důležité pojmy jako bloková šifra, integrální útok a standardní dělící vlastnost. Potom zavedeme definici bitové dělící vlastnosti se třemi podmnožinami a dokážeme tři souvislá tvrzení pravidla propagace: funkce kopírování, AND-komprese a XOR-komprese. V kryptografii využíváme tyto funkce často, proto v této práci dokážeme, jak se šíří bitová dělící vlastnost se třemi podmnožinami po aplikaci těchto funkcí.

Klíčová slova: Dělící vlastnost, Simon šifry, Integrální útok

Title: Integral attack to Simon Family block ciphers

Author: Kieu Trang Phamová

Department: Department of Algebra

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

Abstract: This thesis is focused on bit based division property using three subsets. Firstly, we introduce important definitions such as block cipher, integral attack and conventional division property. Then we define bit based division property using three subsets and prove its propagation rules: copy, AND-compression and XOR-compression. We often use these functions in cryptography, therefore in this thesis we will prove how bit based division property with three subsets propagates after the application of these functions.

Keywords: Division property, Simon family, Integral attack

Obsah

Úvod **2**

1 Základní definice **3**
1.1 Značení 3
1.2 Bloková šifra, rundová funkce 3
1.3 Integrální útok 4
1.4 Blokové šifry SIMON 5
1.5 Integrální útok na SIMON32 6

2 Standardní dělící vlastnost **7**
2.1 Dělící vlastnost 7
2.2 Pravidla propagace dělící vlastnosti 8

3 Bitová dělící vlastnost **10**
3.1 Propagace pro jádro rundové funkce šifry SIMON 10

4 Bitová dělící vlastnost se třemi podmnožinami **13**
4.1 Motivační příklad 13
4.2 Bitová dělící vlastnost se třemi podmnožinami 14
4.3 Pravidla propagace pro bitovou dělící vlastnost se třemi podmnožinami 15

Závěr **24**

Seznam použité literatury **25**

Seznam obrázků **26**

Úvod

Jeden z častých typů symetrických šifer jsou šifry blokové, například DES, AES, SIMON2n. Tyto šifry zašifrují otevřený text po úsecích pevné délky, takzvaných blocích. Vstup do šifrovacího algoritmu a jeho výstup jsou stejně dlouhé. Šifrovací algoritmus můžeme chápat jako složení rundových funkcí. Z hlavního klíče generujeme posloupnost rundových klíčů. Rundová funkce přijímá na vstupu rundový klíč a výstup předchozí rundy.

V článku Todo (2015) autor poprvé zavedl pojem dělící vlastnosti jako nového způsobu, jak najít integrální charakteristiku k útoku blokových šifer. Pomocí této vlastnosti lze dokázat devítirundovou integrální charakteristiku pro blokovou šifru SIMON32. Nicméně v experimentu na SIMON32 ve své práci Wang a kol. (2014) ukázali charakteristiku až na 15 rundách, ale bez důkazu. Todo a Morii (2016) potom ve svém článku zavedli pojem dělící vlastnosti se třemi podmožinami, s jejíž pomocí dokázali 15 rundovou charakteristiku pro SIMON32 obecně.

Bitovou dělící vlastnost můžeme chápat jako speciální případ dělící vlastnosti s bloky délky jeden bit. V článku Todo (2015) standardní dělící vlastnost pracuje s celými bloky šifry a teprve v práci Todo a Morii (2016) autoři začali zkoumat, jak se dělící vlastnost šíří po bitech.

V první kapitole se věnujeme opakování blokových šifer, definujeme rundovou funkci a popíšeme integrální útok s příkladem. Integrální útok využívá integrální charakteristiku dané šifry k odhalení tajného klíče.

Ve druhé kapitole uvedeme definici standardní dělící vlastnosti a její související tvrzení pravidla propagace.

Ve třetí kapitole popíšeme pravidla propagace pro jádro rundové funkce šifry SIMON. Formulujeme tvrzení, jak se šíří standardní dělící vlastnost po funkci jádra rundové funkce, a dokážeme ho.

Ve čtvrté kapitole zavedeme množinu $U_{\mathbb{K}}$, s jejíž pomocí definujeme bitovou dělící vlastnost se třemi podmožinami a dokážeme tvrzení pravidel propagace. V kryptografii využíváme často funkce kopírování, AND-komprese a XOR-komprese, proto v této práci dokážeme, jak se šíří bitová dělící vlastnost se třemi podmnožinami po aplikaci těchto funkcí.

1. Základní definice

1.1 Značení

- Operaci sčítání na $\mathbb{F}_2^n$ označím jako $\oplus$, a sčítání na $\mathbb{Z}$ jako $+$.
- Operaci bitové rotace doleva o j bitů na množině $\mathbb{F}_2^n$ označíme jako $<<< j$. Např. v $\mathbb{F}_2^4$ rotujeme doleva o 1 bit: $(1110)^{<<<1} = (1101)$.
- Pro každý vektor $u \in \mathbb{F}_2^n$ označíme $u[i]$ nebo u_i jeho i-tou složku.
- Pro libovolné $u, v \ \in \mathbb{F}_2^n$ označíme jako $u \odot v$ operaci násobení vektorů po složkách, tj. $u \odot v \ = w \in \mathbb{F}_2^n$, kde $w[i] = u[i] \cdot v[i]$.
- Pro každý prvek $a \in \mathbb{F}_2^n$ definujeme Hammingovu váhu vektoru a předpisem $w(a) = \sum_{i=1}^{n} a[i]$.
- Pro každý prvek $\mathbf{a} \in (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$ definujeme **vektorovou Hammingovou váhu** a následovně

$$W(\mathbf{a}) = (w(a_1), w(a_2), \ldots, w(a_m)) \in \mathbb{Z}^m.$$

- Pro libovolné prvky $\mathbf{k,l} \in \mathbb{Z}^m$ definujeme uspořádání:

$$\mathbf{k} \succeq \mathbf{l} \Leftrightarrow \forall i : k[i] \geq l[i].$$

  Jinak $\mathbf{k} \not\succeq \mathbf{l}$.

1.2 Bloková šifra, rundová funkce

V této práci uvažujeme pouze případy, kdy obě komunikační strany využívají stejný klíč pro šifrování a dešifrování zprávy.

Definice 1 (Bloková šifra)**.** *Bloková šifra S je pětice (P, C, K, E, D), kde*
$P \subseteq \mathbb{F}_2^n$ je množina otevřených textů pro $n \in \mathbb{N}$,
$C \subseteq \mathbb{F}_2^n$ je množina šifrových textů pro $n \in \mathbb{N}$,
$K \subseteq \mathbb{F}_2^m$ je množina klíčů pro $m \in \mathbb{N}$,
$E : K \times P \to C$ je šifrovací funkce,
$D : K \times C \to P$ je dešifrovací funkce,
splňující $\forall k \in K, \forall p \in P : D(k, E(k, p)) = p$.

Jinak řečeno, šifra S je bloková, pokud se pracuje s bloky a klíči pevně dané délky. Funkce E a D zobrazí vstup délky n bitů s klíčem délky m bitů na výstup délky n bitů.

Definice 2 (Rundová funkce blokové šifry)**.** *Mějme blokovou šifru $S = (P, C, K, E, D)$, kde P,C $\subseteq \mathbb{F}_2^n, K \subseteq \mathbb{F}_2^m$. Pro libovolný klíč $k \in K$ definujeme i-tý rundový klíč jako*

$$k_i = h(k_{i-1}), \text{ až na první klíč } k_1 = h(g(k)),$$

kde g a h jsou nějaké funkce $g : \mathbb{F}_2^m \to \mathbb{F}_2^d$, $h : \mathbb{F}_2^d \to \mathbb{F}_2^d$. Řekneme, že

$$F : \mathbb{F}_2^d \times \mathbb{F}_2^n \to \mathbb{F}_2^n$$

je rundová funkce šifry S, pokud existuje $r \in \mathbb{N}$, pro které platí:

$$\forall k \in K, \forall p \in P : E(k,p) = F(k_r, F(k_{r-1}, F(\dots F(k_1,p)\dots),$$

takovou šifru S s rundovou funkcí F nazýváme r-rundová bloková šifra.

1.3 Integrální útok

Odesílatel chce poslat utajenou zprávu tím, že zašifroval zprávu s tajným klíčem k a poslal zašifrovanou zprávu na veřejném kanálu. Tuto zašifrovanou zprávu si může přečíst kdokoliv, ale pouze příjemci, kteří mají správný tajný klíč k, ji umí dešifrovat. Odesílatel a příjemci se mohou předem domluvit na tajném klíči k třeba přes zabezpečený kanál.

V takovém případě bezpečnost informace spočívá v náročnosti uhádnutí správného tajného klíče k a nikoliv v utajení šifrovacího schématu. Šifrovácí schéma a návrh rundových klíčů jsou veřejné. Snahou útočníka je nalezení tajného klíče k z analýzy šifrovaných textů, šifrovacího schématu, nebo pomocí nějaké speciální vlastnosti dané šifry.

Ve zbytku sekce uvažujme r-rundovou blokovou šifru $S = (P, C, K, E, D)$ s rundouvou funkcí F, kde $P = C = \mathbb{F}_2^n$. Pro hlavní klíč $k \in K$ generujeme i-tý rundový klíč jako

$$k_i = h(k_{i-1}), \text{ až na první klíč } k_1 = h(g(k)),$$

kde $g : \mathbb{F}_2^m \to \mathbb{F}_2^d$ a $h : \mathbb{F}_2^d \to \mathbb{F}_2^d$ jsou funkce generující rundové klíče.

Nyní popíšeme obecné schéma integrálního útoku. Předpokládejme, že útočník umí získat šifrovaný text pro libovolný otevřený text bez znalosti hlavního klíče k. Jeho cílem je jej zjistit.

Krok 1. Útočník musí nejdříve analyzovat rundovou funkci F a nalézt integrální charakteristiku, která je specifická pro konkrétní šifru.

Krok 2. Útočník připraví N otevřených textů a zašifruje je po m-rundách, tedy od první do m-té rundy.

Krok 3. Útočník ověří, zda množina zašifrovaných textů splňuje podmínku integrální charakteristiky. Pokud ji splňuje, potom útočník dokáže uhodnout hlavní klíč nebo nějakou jeho část.

Poznamenejme, že integrální útok je vždy specifický pro konkrétní šifru. Kroky útoku se musí přizpůsobit dané šifře.

Poznámka (Ke **Kroku 2**). U některých šifer v kroku 2 generuje hlavní klíč, u jiných generuje jen rundový klíč a pomocí integrální charakteristiky se zjišťuje, zda je správný. Potom ze znalosti rundového klíče lze hrubou silou zjistit hlavní klíč k. Z'aba a kol. (2008) v sekci 2.3 uvádí například šifry Noekeon, Serpent nebo PRESENT.

Nyní uvedeme dva příklady integrální charakteristiky pro lepší pochopení problematiky.

Příklad. V článku Knudsen a Wagner (2002), sekce 2, je uveden příklad integrální charakteristiky pro množinu vektorů $M \subset P$ tak, že šifrovali všechny její vektory po prvích m rund. Řekneme, že množina M má integrální charakteristiku, pokud je splněn alespoň jeden z případů:

Případ 1. Všechny výstupní vektory po m rundách mají na nějaké i-té složce konstantní hodnotu.

Případ 2. Výstupní vektory po m rundách jsou navzájem různé.

Případ 3. XOR-součet všech výstupů po m rundách se rovná konstantě.

Příklad (Integrální charakteristika pro SIMON2n). Pro šifru SIMON2n řekneme, že má m-rundovou integrální charakteristiku s N vybranými otevřenými texty, pokud XOR všech šifrovaných textů po m rundách má na některých pevně zvolených pozicích nulový bit.

1.4 Blokové šifry SIMON

Blokové šifry SIMON byly navrženy tak, aby byly jednoduché a mohly být přímo implementovány v hardwaru. Blokovou šifru SIMON s délkou bloku $2n$ bitů, kde typicky $n \in \{16, 24, 32, 48, 64, \dots\}$, značíme SIMON2n. Délka klíče SIMON2n je typicky $m \cdot n$ pro $m \in \{2, 3, 4, \dots\}$. V literatuře se také označuje jako SIMON2n/nm.

Definice 3 (Blokové šifry SIMON)**.** *SIMON2n/nm je 2n-bitová bloková šifra* (P, C, K, E, D) *taková, že* $P, C \subseteq \mathbb{F}_2^{2n}$ *a* $K \subseteq \mathbb{F}_2^{mn}$*. Nechť* $k \in K$ *je hlavní klíč, nechť* g, h *jsou funkce generující rundové klíče, kde*

$$g : \mathbb{F}_2^{mn} \to (\mathbb{F}_2^n)^m,$$

$$g(k) = (k_m, k_{m-1}, \dots, k_2, k_1),$$

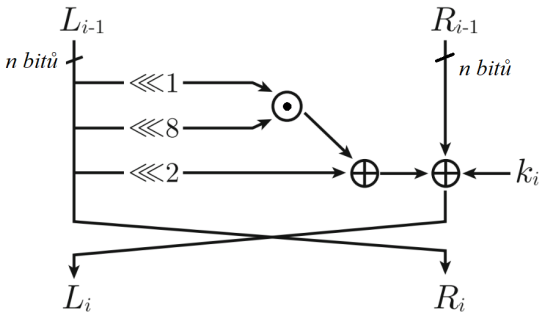
$$h : (\mathbb{F}_2^n)^m \to \mathbb{F}_2^n,$$

$$h(k_i, \dots, k_{i+m}) = k_{i+m+1}.$$

Pro i-tý rundový klíč $k_i \in \mathbb{F}_2^n$ *definujeme rundovou funkci šifry SIMON2n jako* $F_{k_i} : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n \times \mathbb{F}_2^n$ *předpisem:*

$$F_{k_i}(L_{i-1}, R_{i-1}) = ((L_{i-1}^{<<<1} \odot L_{i-1}^{<<<8}) \oplus L_{i-1}^{<<<2} \oplus R_{i-1} \oplus k_i, L_{i-1}),$$

kde (L_0, R_0) je vstupní otevřený text, neboli $L_0||R_0 \in P$, (L_i, R_i) je výstup i-té rundové funkce a současně i vstup do (i+1)-té rundové funkce, kde L_i je levá polovina a R_i je pravá polovina. Každá polovina má n bitů, viz Obrázek 1.1.



Obrázek 1.1: Schéma rundové funkce u SIMON2n.

1.5 Integrální útok na SIMON32

Zavedeme si pojem, který nám usnadní popis útoku.

Definice 4 (Balancovaná složka)**.** *Mějme množinu vektorů $\mathbb{V} \subset \mathbb{Z}_2^{32}$. Řekneme, že i-tá složka výsledku $\bigoplus_{\mathbf{v}\ \in \mathbb{V}} \mathbf{v}$ je balancovaná, jestliže $\bigoplus_{\mathbf{v}\ \in \mathbb{V}} \mathbf{v}[i] = 0$.*

V experimentu Wang a kol. (2014) v sekci 3.1. a 3.2. je popsán **integrální útok na SIMON32/64** s použitím 15 rundové integrální charakteristiky.

Krok 1. Algoritmus nalezení integrální chrakteristiky.

i. Vezměme množinu 2^t vektorů z $\mathbb{Z}_2^{32}$ $(32 > t \geq 16)$ takových, že jsou výstupy první rundy SIMON32 a splňují, že všech 16 pravých složek a některých $(t - 16)$ levých složek je libovolných a ostatní složky jsou konstantní.

ii. Zvolme náhodně hlavní klíč $k \in \mathbb{Z}_2^{64}$. Zašifrujeme 2^t vektorů od druhé do 14. rundy a kontrolujeme, zda jsou nějaké složky balancované. Pokud ano, necháme zvolený klíč jako integrálního kandidáta. Opakujeme tento krok 2^{13} krát, dokud nenajdeme nějakého kandidáta.

iii. Pokud najdeme integrálního kandidáta pro všechny možnosti množin 2^t vektorů s t složkami s libovolnými hodnotami, pak tvrdíme, že SIMON32 má 15 rundovou integrální charakteristiku.

Krok 2. Příprava výstupů první rundy. Vezmeme 2^{31} vektorů z $\mathbb{Z}_2^{32}$ s 31 složkami s libovolnými hodnotami jako výstupy první rundy. Zašifrujeme vektory po dalších 14 rundách.

Krok 3. Ověření integrální charakteristiky v kroku 1. Těchto 2^{31} vektorů má 3 balancované složky po 15 rundách. Více detailů, jak nalézt klíč k, viz sekce 3.2 v článku Wang a kol. (2014).

2. Standardní dělící vlastnost

V této kapitole zopakujeme definici dělící vlastnosti a související tvrzení, viz Todo (2015).

2.1 Dělící vlastnost

Nejdříve definujeme funkci bitového součinu, který budeme potřebovat v definici dělící vlastnosti.

Definice 5. *Pro každé $u, x \in \mathbb{F}_2^n$ definujeme funkci $\pi_u : \mathbb{F}_2^n \to \mathbb{F}_2$ předpisem:*

$$\pi_u(x) := \prod_{i=1}^{n} x[i]^{u[i]}.$$

Snadno nahlédneme, že $x[i]^1 = x[i]$ a $x[i]^0 = 1$, tedy stačí spočítat $x[i]$, jestliže $u[i] = 1$.

Příklad. Mějme $u = (0,1), x = (1,0)$, potom $\pi_u(x) = 1^0 \cdot 0^1 = 0^1$

Zobecníme definici pro $\mathbf{u}$ jako vektor vektorů:

Definice 6. *Pro každé $\mathbf{u}, \mathbf{x} \in (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$ definujeme funkci*

$$\pi_{\mathbf{u}} : (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m}) \to \mathbb{F}_2$$

předpisem:

$$\pi_{\mathbf{u}}(\mathbf{x}) := \prod_{i=1}^{m} \pi_{u[i]}(x[i]).$$

Příklad. Mějme $\mathbf{u} \in (\mathbb{F}_2^2 \times \mathbb{F}_2^3)$, $\mathbf{u} = ((01)(101)), \mathbf{x} = ((11)(110))$, potom

$$\pi_{\mathbf{u}}(\mathbf{x}) = \pi_{(01)}((11)) \cdot \pi_{(101)}((110)) = 1^1 \cdot (1^1 \cdot 0^1) = 0.$$

Definice 7. *Nechť $\mathbb{K} \subseteq \mathbb{Z}_{n_1+1} \times \mathbb{Z}_{n_2+1} \times \cdots \times \mathbb{Z}_{n_m+1}$. Nechť $\mathbf{u} \in (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$. Definujeme množinu*

$$U_{\mathbb{K}} = \{\mathbf{u} | \forall \mathbf{k} \in \mathbb{K} : W(\mathbf{u}) \not\geq \mathbf{k}\}.$$

Definice 8 (Dělící vlastnost)**.** *Nechť $\mathbb{X}$ je multimnožina s prvky z množiny $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$. Nechť $\mathbf{u} \in (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$. Řekneme, že $\mathbb{X}$ má dělící vlastnost $\mathcal{D}_{\mathbb{K}}^{n_1,n_2,\ldots,n_m}$, kde $\mathbb{K} \subseteq \mathbb{Z}_{n_1+1} \times \mathbb{Z}_{n_2+1} \times \cdots \times \mathbb{Z}_{n_m+1}$, jestliže pro všechna $\mathbf{u} \in U_{\mathbb{K}}$ platí:*

$$\bigoplus_{\mathbf{x} \in \mathbb{X}} \pi_{\mathbf{u}}(\mathbf{x}) = 0.$$

2.2 Pravidla propagace dělící vlastnosti

Pravidla propagace dělící vlastnosti jsou tvrzení, která byla dokázána v literatuře Todo (2015) jako důkaz tvrzení B1-B5. Zde následující tvrzení připomínáme pro srovnání s dokazovanými pravidly tvrzení 4, 5 a 6 v sekci 4.3. Uveďme pomocné značení, které používáme v této sekci.

Značení:

- Zápisem $\mathbb{K} \leftarrow k$ označíme, že množinu $\mathbb{K}$ nahradíme množinou $\mathbb{K} \cup \{k\}$.
- Zápisem $\min_{(k_1,k_2)\in\mathbb{K}}\{k_1 + k_2\}$ označíme nejmenší prvek množiny $\{k_1 + k_2 | \forall (k_1,k_2) \in \mathbb{K}\}$.

Pravidlo 1. (Substituce) Nechť F je funkce, která se skládá z m S-boxů, kde i-tý S-box má délku n_i bitů a jeho algebraický stupeň je d_i. Označíme vstupní a výstupní multimnožiny $\mathbb{X}$, $\mathbb{Y}$, jejichž prvky jsou prvky množiny $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$. Pokud multimnožina $\mathbb{X}$ má dělící vlastnost $\mathcal{D}_{\mathbb{K}}^{n_1,n_2,\ldots,n_m}$, potom multimnožina $\mathbb{Y}$ bude mít dělící vlastnost $\mathcal{D}_{\mathbb{K}'}^{n_1,n_2,\ldots,n_m}$, kde

$$\mathbb{K}' \leftarrow \left(\left\lceil \frac{k_1}{d_1} \right\rceil, \left\lceil \frac{k_2}{d_2} \right\rceil \ldots \left\lceil \frac{k_m}{d_m} \right\rceil\right), \forall k \in \mathbb{K}.$$

Pokud i-tý S-box je bijektivní a $k_i = n_i$, i-tý element vlastnosti propagace bude n_i, nikoliv $\left\lceil \frac{n_i}{d_i} \right\rceil$.

Pravidlo 2. (Kopírování) Nechť $\mathbb{X}$ je multimnožina z $\mathbb{F}_2^n$ a $\mathbb{Y}$ je multimnožina z $\mathbb{F}_2^n \times \mathbb{F}_2^n$. Definujeme funkce kopírování $F : \mathbb{X} \to \mathbb{Y}$ takové, že pro každý $x \in \mathbb{X}$: $F(x) = (x,x)$. Pokud $\mathbb{X}$ má $\mathcal{D}_k^n$, potom $\mathbb{Y}$ má $\mathcal{D}_{\mathbb{K}'}^{n,n}$, kde

$$\mathbb{K}' \leftarrow (k - i,i) \text{ ,kde } 0 \leq i \leq k.$$

Pravidlo 3. (XOR-komprese) Nechť $\mathbb{X}$ je multimnožina z $\mathbb{F}_2^n \times \mathbb{F}_2^n$ a $\mathbb{Y}$ je multimnožina z $\mathbb{F}_2^n$. Definujeme funkci XOR-komprese $F : \mathbb{X} \to \mathbb{Y}$ takovou, že $F(x_1,x_2) = x_1 \oplus x_2$. Pokud $\mathbb{X}$ má $\mathcal{D}_{\mathbb{K}}^{n,n}$, potom $\mathbb{Y}$ má $\mathcal{D}_{k'}^n$, kde

$$k' \leftarrow \min_{(k_1,k_2)\in\mathbb{K}}\{k_1 + k_2\}.$$

Konkatenace. Označíme operaci konkatenace $||$. Pro libovolné 2 vektory

$$a = (a_1, \ldots,a_n) \in \mathbb{F}_2^n, \quad b = (b_1, \ldots,b_m) \in \mathbb{F}_2^m$$

definujeme konkatenaci vektorů a a b

$$a||b := (a_1, \ldots, a_n,b_1, \ldots, b_m) \in \mathbb{F}_2^{n+m}.$$

Pravidlo 4. (Rozdělení) Nechť $\mathbb{X}$ je multimnožina z $\mathbb{F}_2^n$ a $\mathbb{Y}$ je multimnožina z $\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n-n_1}$. Definujeme funkci rozdělení $F : \mathbb{X} \to \mathbb{Y}$ takové, že

$$\forall x = (x_1, \ldots, x_n) \in \mathbb{X} : F(x) = (x_1, \ldots, x_{n_1})||(x_{n_1+1}, \ldots, x_n).$$

Pokud $\mathbb{X}$ má $\mathcal{D}_k^n$, potom $\mathbb{Y}$ má $\mathcal{D}_{\mathbb{K}'}^{n_1,n-n_1}$, kde

$$\mathbb{K}' \leftarrow (k-i,i) \text{,kde } 0 \leq i \leq k.$$

Platí, že $(k-i) \leq n_1, i \leq n-n_1$.

Pravidlo 5. (Konkatenace) Nechť $\mathbb{X}$ je multimnožina z $\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2}$ a $\mathbb{Y}$ je multimnožina z $\mathbb{F}_2^{n_1+n_2}$. Definujeme funkci konkatenace $F : \mathbb{X} \to \mathbb{Y}$ takovou, že

$$\forall (x_1,x_2) \in \mathbb{X} : F((x_1,x_2)) = x_1||x_2.$$

Pokud $\mathbb{X}$ má $\mathcal{D}_{\mathbb{K}}^{n_1,n_2}$, potom $\mathbb{Y}$ má $\mathcal{D}_{k'}^{n_1+n_2}$, kde

$$k' \leftarrow \min_{(k_1,k_2)\in\mathbb{K}} \{k_1+k_2\}.$$

3. Bitová dělící vlastnost

V této kapitole uvažujeme *bitovou dělící vlastnost* $\mathcal{D}_{\mathbb{K}}^{1^n}$ jako speciální případ dělící vlastnosti. Pro jednoduchost lze chápat bitovou dělící vlastnost jako dělící vlastnost jen u jednoho bitu. Můžeme použít přímo pět pravidel propagace dělící vlatnosti.

3.1 Propagace pro jádro rundové funkce šifry SIMON

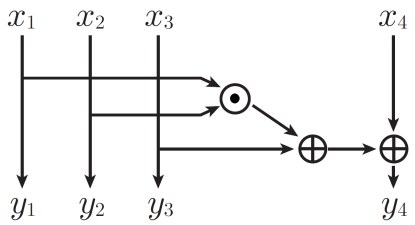
Analyzujeme SIMON2n pomocí bitové dělící vlastnosti. Soustředíme se pouze na jeden bit pravé poloviny v šifře SIMON2n. Jádro rundové funkce je funkce

$$C : \mathbb{F}_2^4 \to \mathbb{F}_2^4$$

s předpisem

$$C((x_1,x_2,x_3,x_4)) = (x_1,x_2,x_3, x_1 \cdot x_2 \oplus x_3 \oplus x_4).$$

Funkce C je reprezentována na obrázku 3.1. Vstup i výstup mají délku čtyř bitů. Používáme dělící vlastnost $\mathcal{D}_{\mathbb{K}}^{1^4}$. Uvažujeme jednu aplikaci funkce C na nějaký vstup (x_1,x_2,x_3,x_4), jejíž výstup označíme (y_1,y_2,y_3,y_4).



Obrázek 3.1: Jádro rundové funkce šifry SIMON2n.

Na následujícím příkladu si přiblížíme pojem dělící vlastnosti.

Příklad. Ukážeme, že vstupní multimnožina $\mathbb{X} = \{(1,1,1,0), (1,1,1,1)\}$ má dělící vlastnost $\mathcal{D}_{(0,0,0,1)}^{1^4}$. To znamená, že musíme ověřit podmínku $\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{\mathbf{u}}(\mathbf{x}) = 0, \forall \mathbf{u}$ tak, že $W(\mathbf{u}) \not\succeq (0,0,0,1)$. Rozepíšeme podmínku dle definice následovně

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{\mathbf{u}}(\mathbf{x}) = \bigoplus_{\mathbf{x}\in\mathbb{X}} \prod_{i=1}^{4} \pi_{u[i]}(x[i]) = \bigoplus_{\mathbf{x}\in\mathbb{X}} \prod_{i=1}^{4} x[i]^{u[i]}.$$

Z definice vektorové Hamingovy váhy a navíc faktu, že $\mathbf{u} \in \mathbb{F}_2^4$, neboli $u[i] \in \mathbb{F}_2$, platí $W(\mathbf{u}) = (w(u[1]), w(u[2]),w(u[3]),w(u[4])) = (u[1],u[2],u[3],u[4]) = \mathbf{u}$. Tedy chceme najít všechna $\mathbf{u} \not\succeq (0,0,0,1)$. Označme $\mathbf{k} = (0,0,0,1)$ a $U_{\mathbf{k}} = \{\mathbf{u} : W(\mathbf{u}) \not\succeq \mathbf{k}\}$. Protože $W(\mathbf{u}) = \mathbf{u}$, pak $U_{\mathbf{k}} = \{\mathbf{u} : \mathbf{u} \not\succeq \mathbf{k}\}$. Platí, že

$$\mathbf{u} \not\succeq \mathbf{k} \Leftrightarrow \exists i : u[i] < k[i].$$

Nicméně první 3 bity vektoru $\mathbf{k}$ jsou nuly, tedy musí platit $u[4] = 0 < k[4]$.

Všechna možná $\mathbf{u}$ budou prvky množiny $U_\mathbf{k} = \{(u[1],u[2],u[3],0), u[i] \in \mathbb{F}_2\}$. Tedy

$$U_\mathbf{k} = \{(0,0,0,0),(0,0,1,0),(0,1,0,0),(0,1,1,0),\\ (1,0,0,0),(1,0,1,0),(1,1,0,0),(1,1,1,0)\}.$$

Ověříme, že $\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_\mathbf{u}(\mathbf{x}) = 0$ pro všechny $\mathbf{u} \in U_\mathbf{k}$:

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_\mathbf{u}(\mathbf{x}) = \bigoplus_{\mathbf{x}\in\mathbb{X}} \prod_{i=1}^{4} x[i]^{u[i]} = \bigoplus_{\mathbf{x}\in\mathbb{X}} 1^{u[1]} \cdot 1^{u[2]} \cdot 1^{u[3]} \cdot x[4]^0 = 1 \oplus 1 = 0.$$

Tedy multimnožina $\mathbb{X}$ skutečně má $\mathcal{D}^{14}_{(0,0,0,1)}$.

Tvrzení 1. *Nechť vstupní multimnožina $\mathbb{X}$ má dělící vlastnost $\mathcal{D}^{14}_{(k_1,k_2,k_3,1)}$, kde $k_i \in \mathbb{F}_2$. Nechť C je jádro rundové funkce SIMON2n. Označme výstupní množinu po propagaci C jako*

$$\mathbb{Y} = \{(x_1, x_2, x_3, x_1 \cdot x_2 \oplus x_3 \oplus x_4); (x_1, x_2, x_3, x_4) \in \mathbb{X}\}.$$

Potom multimnožina $\mathbb{Y}$ má stejnou dělící vlastnost jako vstupní multimnožina $\mathbb{X}$, neboli $\mathbb{Y}$ má $\mathcal{D}^{14}_{(k_1,k_2,k_3,1)}$.

Důkaz. Označme $U_\mathbf{k} = \{\mathbf{u} : W(\mathbf{u}) \not\succeq (k_1,k_2,k_3,1)\}$. Multimnožina $\mathbb{X}$ má dělící vlastnost $\mathcal{D}^{14}_{(k_1,k_2,k_3,1)}$ což znamená, že

$$\forall \mathbf{u} \in U_\mathbf{k} : \bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_\mathbf{u}(\mathbf{x}) = \bigoplus_{\mathbf{x}\in\mathbb{X}} \prod_{i=1}^{4} x_i^{u_i} = 0.$$

Uvědomme si, že pro každou trojici $(u_1,u_2,u_3) \in \mathbb{F}_2^3$ leží vektor $(u_1,u_2,u_3,0)$ v U_k, protože platí $(u_1,u_2,u_3,0) \not\succeq (k_1,k_2,k_3,1)$. Proto pro každou trojici (u_1,u_2,u_3):

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \prod_{i=1}^{3} x_i^{u_i} = \bigoplus_{\mathbf{x}\in\mathbb{X}} \prod_{i=1}^{3} x_i^{u_i} \cdot x_4^0 = 0. \tag{3.1}$$

Potom spočítáme pro všechna $(u_1,u_2,u_3,0) \in U_k$, že

$$\bigoplus_{\mathbf{y}\in\mathbb{Y}} \pi_\mathbf{u}(\mathbf{y}) = \bigoplus_{\mathbf{y}\in\mathbb{Y}} \prod_{i=1}^{4} y_i^{u_i} = \bigoplus_{\mathbf{x}\in\mathbb{X}} \prod_{i=1}^{3} x_i^{u_i} = 0.$$

díky rovnosti 3.1.

Nakonec s využitím distributivity a faktu, že $x_i^1 = x_i^2$, protože $x_i \in \mathbb{F}_2$, spočítáme pro všechna $(u_1,u_2,u_3,1) \in U_k$:

$$\bigoplus_{\mathbf{y}\in\mathbb{Y}} \pi_\mathbf{u}(\mathbf{y}) = \bigoplus_{\mathbf{y}\in\mathbb{Y}} \prod_{i=1}^{4} y_i^{u_i} = \bigoplus_{\mathbf{x}\in\mathbb{X}} (\prod_{i=1}^{3} x_i^{u_i} \cdot (x_1 \cdot x_2 \oplus x_3 \oplus x_4)) =$$

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} (x_1^{u_1+1} x_2^{u_2+1} x_3^{u_3}) \oplus \bigoplus_{\mathbf{x}\in\mathbb{X}} (x_1^{u_1} x_2^{u_2} x_3^{u_3+1}) \oplus \bigoplus_{\mathbf{x}\in\mathbb{X}} (x_1^{u_1} x_2^{u_2} x_3^{u_3} x_4) =$$

$$\bigoplus_{\mathbf{x}\in\mathbb{X}}(x_1x_2x_3^{u_3}) \oplus \bigoplus_{\mathbf{x}\in\mathbb{X}}(x_1^{u_1}x_2^{u_2}x_3) \oplus \bigoplus_{\mathbf{x}\in\mathbb{X}}(x_1^{u_1}x_2^{u_2}x_3^{u_3}x_4^{u_4}) = 0.$$

kde první dvě sumy přes $\mathbb{X}$ jsou nulové podle 3.1 a poslední je nulová z předpokladu. Navíc, $x_i^{u_i+1} = x_i$ pro všechna $u_i \in \mathbb{F}_2$, protože pro $u_i = 0 : x_i^{0+1} = x_i$, jinak pro $u_i = 1 : x_i^{1+1} = x_i^2 = x_i$ dle faktu. Tedy

$$\forall \mathbf{u} \in U_{\mathbf{k}} : \bigoplus_{\mathbf{y}\in\mathbb{Y}} \pi_{\mathbf{u}}(\mathbf{y}) = 0,$$

neboli multimnožina $\mathbb{Y}$ má dělící vlastnost $\mathcal{D}^{1^4}_{(k_1,k_2,k_3,1)}$ stejně jako multimnožina $\mathbb{X}$.

□

Z tvrzení 1 plyne, že vstupní a výstupní multimnožiny po propagaci jádra rundové funkce SIMON2n mají stejnou dělící vlastnost $\mathcal{D}^{1^4}_{\mathbf{k}}$, pokud čtvrtý bit vektoru $\mathbf{k}$ je 1. Nyní se zaměříme na příklad, kdy vstupní multimnožina $\mathbb{X}$ má dělící vlastnost $\mathcal{D}^{1^4}_{(1,0,0,0)}$, neboli čtvrtý bit vektoru $\mathbf{k}$ je 0. Zajímá nás, jak bude vypadat dělící vlastnost výstupní množiny po propagaci jádra rundové funkce SIMON2n.

Příklad. Ukažme, že vstupní multimnožina $\mathbb{X} = \{(0,0,1,0),(1,0,1,0)\}$ má dělící vlastnost $\mathcal{D}^{1^4}_{(1,0,0,0)}$. Toto lze ověřit podle definice 8 tak, že $\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{\mathbf{u}}(\mathbf{x}) = 0$ pro všechna možná $\mathbf{u} \in \{(0,0,0,0),(0,0,0,1),(0,0,1,0),(0,0,1,1),(0,1,0,0),$
$(0,1,0,1),(0,1,1,0),(0,1,1,1)\}$.

Po propagaci jádra rundové funkce SIMON2n příslušná výstupní multimnožina je $\mathbb{Y} = \{(0,0,1,1),(1,0,1,1)\}$. Všimněme si, že pro $\mathbf{u} = (0,0,1,1)$ platí

$$(0^0 \cdot 0^0 \cdot 0^1 \cdot 1^1) \oplus (1^0 \cdot 0^0 \cdot 1^1 \cdot 1^1) = 0 \oplus 1 = 1.$$

Tedy $\mathbb{Y}$ má jinou dělící vlastnost než $\mathbb{X}$.

Všimněme si, že tento příklad můžeme zobecnit. Pokud vstupní multimnožina má dělící vlastnost $\mathcal{D}^{1^4}_{(k_1,k_2,k_3,0)}$ s alespoň jedním $k_i = 1$, potom výstupní multimnožina po propagaci jádra rundové funkce SIMON2n nemusí mít stejnou dělící vlastnost jako vstupní multimnožina.

V sekci 3.2 článku Todo a Morii (2016) je bez důkazu uvedeno tvrzení, jak z dělící vlastnosti vstupu zjistit dělící vlasnosti výstupu po propagaci jádra rundové funkce SIMON32.

4. Bitová dělící vlastnost se třemi podmnožinami

Nejprve ukážeme motivační příklad a potom zadefinujeme bitovou dělící vlastnost se třemi podmnožinami. Dokážeme souvislá tvrzení pravidla propagace pro funkce kopírování, XOR-kompresi a AND-kompresi.

4.1 Motivační příklad

Standardní dělící vlastnost dělí množinu vektorů $\mathbf{u} \in U_K$ podle toho, zda $\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{\mathbf{u}}(\mathbf{x})$ nabývá 0, viz definice 8. Na jednoduchém příkladu ukážeme, že existuje vlastnost, kterou standardní bitová dělící vlastnost nedokáže najít.

Nechť $\mathbb{X} = \{(0,0,0,0), (0,1,0,0), (1,0,0,0), (1,1,1,0)\}$ je multimnožina s $\mathcal{D}^{1^4}_{(1,1,0,0),(0,0,1,0)}$. Nechť $\mathbb{Y} = \{(0,0,0,0), (0,1,0,0), (1,0,0,0), (1,1,1,0)\}$ je multimnožina s $\mathcal{D}^{1^4}_{(1,1,0,0),(0,0,1,0),(0,0,0,1)}$. Nechť $C : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ je funkce jádra rundové funkce SIMON2n. Všimněme si, že platí $\mathbb{Y} = C(\mathbb{X})$. Označme $K = \{(1,1,0,0), (0,0,1,0)\}$ a $K_1 = \{(1,1,0,0), (0,0,1,0), (0,0,0,1)\}$. Potom $U_{K_1} = \{(0,0,0,0), (0,1,0,0), (1,0,0,0)\}$.

Podle definice standardní dělící vlastnosti zkoumáme, zda pro vektory $\mathbf{u} \in U_{K_1}$ platí $\bigoplus_{\mathbf{y}\in\mathbb{Y}} \pi_{\mathbf{u}}(\mathbf{y}) = 0$.

Ukážeme, že vektor $(0,0,0,1) \notin U_{K_1}$, ale $\bigoplus_{\mathbf{y}\in\mathbb{Y}} \pi_{(0,0,0,1)}(\mathbf{y}) = 0$. Neboli výstupní množina $\mathbb{Y}$ má silnější dělící vlastnost.

Všimněme si, že $\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(1,1,0,0)}(\mathbf{x}) = 1$ a $\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(0,0,1,0)}(\mathbf{x}) = 1$. Potom platí:

$$\begin{aligned}
\bigoplus_{\mathbf{y}\in\mathbb{Y}} \pi_{(0,0,0,1)}(\mathbf{y}) &= \bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(0,0,0,1)}(C(\mathbf{x})) \\
&= \bigoplus_{\mathbf{x}\in\mathbb{X}} x_1^0 \cdot x_2^0 \cdot x_3^0 \cdot (x_1 \cdot x_2 \oplus x_3 \oplus x_4)^1 \\
&= \bigoplus_{\mathbf{x}\in\mathbb{X}} (x_1 \cdot x_2 \oplus x_3 \oplus x_4) \\
&= \bigoplus_{\mathbf{x}\in\mathbb{X}} (x_1 \cdot x_2) \bigoplus_{\mathbf{x}\in\mathbb{X}} (x_3) \bigoplus_{\mathbf{x}\in\mathbb{X}} (x_4) \\
&= \bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(1,1,0,0)}(\mathbf{x}) \bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(0,0,1,0)}(\mathbf{x}) \bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(0,0,0,1)}(\mathbf{x}) \\
&= 1 \oplus 1 \oplus 0 \\
&= 0.
\end{aligned}$$

Tudíž $\bigoplus_{\mathbf{y}\in\mathbb{Y}} \pi_{(0,0,0,1)}(\mathbf{y}) = 0$. Ukážeme, že multimnožina $\mathbb{Y}$ bude mít silnější dělící vlastnost $\mathcal{D}^{1^4}_{(1,1,0,0),(0,0,1,0),(0,1,0,1),(1,0,0,1)}$, nikoliv jen $\mathcal{D}^{1^4}_{(1,1,0,0),(0,0,1,0),(0,0,0,1)}$.

$\mathcal{D}^{1^4}_{(1,1,0,0),(0,0,1,0),(0,1,0,1),(1,0,0,1)}$ má příslušnou množinu

$$U_{K_2} = \{(0,0,0,0), (0,0,0,1), (0,1,0,0), (1,0,0,0)\},$$

tedy je opravdu silnější než $\mathcal{D}^{1^4}_{(1,1,0,0),(0,0,1,0),(0,0,0,1)}$, která má příslušnou

$$U_{K_1} = \{(0,0,0,0), (0,1,0,0), (1,0,0,0)\}.$$

4.2 Bitová dělící vlastnost se třemi podmnožinami

Poznámka. V této kapitole uvažujme, že $\mathbb{Z}_2^m$ je podmnožina množiny $\mathbb{N}_0^m$. Na $\mathbb{N}_0^m$ uvažujme po složkách definované operace $+$ a $\odot$ a na množině $\mathbb{Z}_2^m$ uvažujme obdobně definovanou operaci $\vee$. Všimněme si, že množina $\mathbb{Z}_2^m$ je sice uzavřená na operaci násobení, ale na operaci $+$ uzavřená není.

Definice 9. *Mějme množinu $\mathbb{K} \subseteq \mathbb{Z}_2^m$, kde $m \in \mathbb{N}$. Nechť $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$. Definujeme množinu*

$$U_{\mathbb{K}} = \{\mathbf{u} \in \mathbb{Z}_2^m | \forall \mathbf{k} \in \mathbb{K} : W(\mathbf{u}) \not\succeq \mathbf{k}\}.$$

Lemma 2. *Mějme množinu $\mathbb{K} \subseteq \mathbb{Z}_2^m$. Platí, že množina*

$$U_{\mathbb{K}} = \mathbb{Z}_2^m \setminus \bigcup_{\mathbf{k} \in \mathbb{K}} \{\mathbf{v} \in \mathbb{Z}_2^m | \mathbf{v} \succeq \mathbf{k}\}.$$

Důkaz. Všimněme si, že pro vektor $\mathbf{u} \in \mathbb{Z}_2^m$ platí, že $W(\mathbf{u}) = \mathbf{u}$. Potom množina

$$U_{\mathbb{K}} = \{\mathbf{u} \in \mathbb{Z}_2^m | \forall \mathbf{k} \in \mathbb{K} : \mathbf{u} \not\succeq \mathbf{k}\}.$$

Dokážeme dvě inkluze.

1. Nejprve dokážeme, že $U_{\mathbb{K}} \subseteq \mathbb{Z}_2^m \setminus \bigcup_{\mathbf{k} \in \mathbb{K}} \{\mathbf{v} \in \mathbb{Z}_2^m | \mathbf{v} \succeq \mathbf{k}\}$. Pokud vektor $\mathbf{u} \in U_{\mathbb{K}}$, potom pro všechna $\mathbf{k} \in \mathbb{K}$ platí, že $\mathbf{u} \not\succeq \mathbf{k}$. Z toho plyne, že vektor $\mathbf{u}$ není prvkem sjednocení $\bigcup_{\mathbf{k} \in \mathbb{K}} \{\mathbf{v} \in \mathbb{Z}_2^m | \mathbf{v} \succeq \mathbf{k}\}$, a proto platí, že $\mathbf{u} \in \mathbb{Z}_2^m \setminus \bigcup_{\mathbf{k} \in \mathbb{K}} \{\mathbf{v} \in \mathbb{Z}_2^m | \mathbf{v} \succeq \mathbf{k}\}$.

2. Dále dokážeme, že $\mathbb{Z}_2^m \setminus \bigcup_{\mathbf{k} \in \mathbb{K}} \{\mathbf{v} \in \mathbb{Z}_2^m | \mathbf{v} \succeq \mathbf{k}\} \subseteq U_{\mathbb{K}}$. Pokud vektor $\mathbf{u} \in \mathbb{Z}_2^m \setminus \bigcup_{\mathbf{k} \in \mathbb{K}} \{\mathbf{v} \in \mathbb{Z}_2^m | \mathbf{v} \succeq \mathbf{k}\}$, potom pro všechna $\mathbf{k} \in \mathbb{K}$ platí, že $\mathbf{u} \not\succeq \mathbf{k}$. Tedy platí, že $\mathbf{u} \in U_{\mathbb{K}}$.

Tím je lemma dokázáno.

□

Definice 10 (Bitová dělící vlastnost se třemi podmnožinami)**.** *Nechť $\mathbb{X}$ je multimnožina s prvky z množiny $\mathbb{F}_2^m$. Mějme množiny $\mathbb{K}, \mathbb{L} \subseteq \mathbb{F}_2^m$. Řekneme, že $\mathbb{X}$ má bitovou dělící vlastnost se třemi podmnožinami $\mathcal{D}_{\mathbb{K},\mathbb{L}}^{1^m}$, jestliže pro všechna $\mathbf{u} \in U_{\mathbb{K}}$ platí*

$$\bigoplus_{\mathbf{x} \in \mathbb{X}} \pi_{\mathbf{u}}(\mathbf{x}) = \begin{cases} 1, & \text{pokud } \exists \boldsymbol{\ell} \in \mathbb{L} : W(\mathbf{u}) = \boldsymbol{\ell} \\ 0, & \text{jinak.} \end{cases} \tag{4.1}$$

Poznámka. Je důležité si uvědomit, že nás nezajímají případy vektoru $\mathbf{u}$, pro něž existuje $\mathbf{k} \in \mathbb{K}$ splňující $W(\mathbf{u}) \succeq \mathbf{k}$.

Poznámka. Všimněme si, že pro vektory $\mathbf{u} \in U_{\mathbb{K}}$ a množiny $\mathbb{K}, \mathbb{L} \subseteq \mathbb{F}_2^m$ platí, že $W(\mathbf{u}) = \mathbf{u}$. Potom lze podmínku, že $\exists \boldsymbol{\ell} \in \mathbb{L} : W(\mathbf{u}) = \boldsymbol{\ell}$, přepsat na podmínku $\mathbf{u} \in \mathbb{L}$.

4.3 Pravidla propagace pro bitovou dělící vlastnost se třemi podmnožinami

Vyslovíme tři tvrzení bitové dělící vlastnosti se třemi podmnožinami. Tato tvrzení jsou obdobou tvrzení o standardní dělící vlastnosti. Nejdříve dokážeme pomocné lemma.

Lemma 3. *Nechť $x \in \mathbb{F}_2$ a $v_1, v_2 \in \mathbb{Z}_2^m \subseteq \mathbb{N}_0^m$. Potom platí, že $x^{v_1+v_2} = x^{v_1 \vee v_2}$.*

Důkaz.

Všimněme si faktu, že pro všechna $x \in \mathbb{F}_2$ platí $x^1 = x^2$. Potom pro $x, v_1, v_2 \in \mathbb{F}_2$ platí

v_1	v_2	$v_1 + v_2$	$v_1 \vee v_2$	$x^{v_1+v_2}$	$x^{v_1 \vee v_2}$
1	1	2	1	$x^2 = x$	x
1	0	1	1	x	x
0	1	1	1	x	x
0	0	0	0	1	1

Z tabulky vyplývá, že platí $x^{v_1+v_2} = x^{v_1 \vee v_2}$.

□

Tvrzení 4 (Pravidlo kopírování)**.** *Nechť $\mathbb{X}$ je multimnožina s prvky z $\mathbb{F}_2^m$ a $\mathbb{Y}$ je multimnožina s prvky z $\mathbb{F}_2^{m+1}$, definujme funkci kopírování $F : \mathbb{F}_2^m \to \mathbb{F}_2^{m+1}$ tak, že pro každé $(x_1,x_2,\ldots,x_m)$ máme*

$$F((x_1,x_2,\ldots,x_m)) = (x_1,x_1,x_2,\ldots,x_m).$$

Pokud $\mathbb{X}$ má $\mathcal{D}^{1^m}_{\mathbb{K},\mathbb{L}}$, potom $\mathbb{Y} = F(\mathbb{X})$ má $\mathcal{D}^{1^{m+1}}_{\mathbb{K}',\mathbb{L}'}$, kde

$$\mathbb{K}' = \{(0,0,\mathbf{k}_{2..m}) | (0,\mathbf{k}_{2..m}) \in \mathbb{K}\} \cup \{(1,0,\mathbf{k}_{2..m}),(0,1,\mathbf{k}_{2..m}) | (1,\mathbf{k}_{2..m}) \in \mathbb{K}\},$$
$$\mathbb{L}' = \{(0,0,\boldsymbol{\ell}_{2..m}) | (0,\boldsymbol{\ell}_{2..m}) \in \mathbb{L}\} \cup \{(a,b,\boldsymbol{\ell}_{2..m}) | (a,b) \neq (0,0), (1,\boldsymbol{\ell}_{2..m}) \in \mathbb{L}\},$$

kde $\mathbf{k}_{2..m}$ značí složky $k_2,k_3,\ldots,k_m$, a $\boldsymbol{\ell}_{2..m}$ značí složky $\ell_2,\ell_3,\ldots,\ell_m$.

Důkaz. Předpokládejme, že multimnožina $\mathbb{X}$ má $\mathcal{D}^{1^m}_{\mathbb{K},\mathbb{L}}$. Vyhodnotíme výraz $\bigoplus_{\mathbf{y}\in\mathbb{Y}} \pi_{\mathbf{v}}(\mathbf{y})$ pro každý vektor $\mathbf{v} \in U_{\mathbb{K}'}$:

$$\begin{aligned}\bigoplus_{\mathbf{y}\in\mathbb{Y}} \pi_{\mathbf{v}}(\mathbf{y}) &= \bigoplus_{\mathbf{x}\in\mathbb{X}} (\pi_{\mathbf{v}} \circ F)(\mathbf{x}) \\ &= \bigoplus_{\mathbf{x}\in\mathbb{X}} (x_1^{v_1} x_1^{v_2} x_2^{v_3} x_3^{v_4} \ldots x_m^{v_{m+1}}) \\ &= \bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(v_1 \vee v_2, v_3, \ldots, v_{m+1})}(\mathbf{x}). \end{aligned} \tag{4.2}$$

První dvě rovnosti v (4.2) jsou přímé dosazení do definice funkce kopírování. K důkazu třetí rovnosti využijeme lemmatu 3.

Podle definice dělící vlastnosti platí, že pro všechna $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) \in U_{\mathbb{K}}$ platí:

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(v_1\vee v_2, v_3, \ldots, v_{m+1})}(\mathbf{x}) = \begin{cases} 1, & \text{pokud } (v_1 \vee v_2, v_3, \ldots, v_{m+1}) \in \mathbb{L} \\ 0, & \text{jinak.} \end{cases} \tag{4.3}$$

Nejdřív dokážeme, že pokud $(v_1, v_2, v_3, \ldots, v_{m+1}) \in U_{\mathbb{K}'}$, potom platí $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) \in U_{\mathbb{K}}$. Dokážeme obměnu implikace, že pokud $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) \notin U_{\mathbb{K}}$, potom platí $(v_1, v_2, v_3, \ldots, v_{m+1}) \notin U_{\mathbb{K}'}$.

Pokud $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) \notin U_{\mathbb{K}}$, potom podle definice $U_{\mathbb{K}}$ platí, že

$$\exists \mathbf{k} = (k_1, k_2, \ldots, k_m) \in \mathbb{K} \text{ takové, že } (v_1 \vee v_2, v_3, \ldots, v_{m+1}) \succeq (k_1, k_2, \ldots, k_m).$$

Z toho plyne, že $\forall i \in \{3, 4, \ldots, m+1\} : v_i \geq k_{i-1}$ a $v_1 \vee v_2 \geq k_1$. Máme dva případy.

1. Pokud $k_1 = 0$, potom platí $v_1 \geq k_1$ a současně $v_2 \geq k_1$. Potom platí, že

   $$(v_1, v_2, v_3, \ldots, v_{m+1}) \succeq (0{,}0{,}k_2, \ldots, k_m).$$

   Podle konstrukce $\mathbb{K}'$ platí, že $(0{,}0{,}k_2, \ldots, k_m) \in \mathbb{K}'$. Z toho plyne, že $(v_1, v_2, v_3, \ldots, v_{m+1}) \notin U_{\mathbb{K}'}$.

2. Pokud $k_1 = 1$, potom z konstrukce $\mathbb{K}'$ platí, že $(1{,}0{,}k_2, \ldots, k_m), (0, 1, k_2, \ldots, k_m) \in \mathbb{K}'$. Protože $v_1 \vee v_2 \geq k_1$, máme tři případy:

   (a) pokud $v_1 = 1$ a $v_2 = 1$, potom platí, že

   $$(v_1, v_2, v_3, \ldots, v_{m+1}) \succeq (1{,}0{,}k_2, \ldots, k_m),$$

   (b) pokud $v_1 = 1$ a $v_2 = 0$, potom platí, že

   $$(v_1, v_2, v_3, \ldots, v_{m+1}) \succeq (1{,}0{,}k_2, \ldots, k_m),$$

   (c) pokud $v_1 = 0$ a $v_2 = 1$, potom platí, že

   $$(v_1, v_2, v_3, \ldots, v_{m+1}) \succeq (0{,}1{,}k_2, \ldots, k_m).$$

   Tedy existuje $\mathbf{k}' \in \mathbb{K}'$ takové, že $(v_1, v_2, v_3, \ldots, v_{m+1}) \succeq \mathbf{k}'$. Z toho plyne, že $(v_1, v_2, v_3, \ldots, v_{m+1}) \notin U_{\mathbb{K}'}$.

Tím jsme dokázali implikaci, že pokud $(v_1, v_2, v_3, \ldots, v_{m+1}) \in U_{\mathbb{K}'}$, potom platí $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) \in U_{\mathbb{K}}$.

Dále dokážeme, že pro všechna $\mathbf{v} \in U_{\mathbb{K}'}$ je podmínka $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) \in \mathbb{L}$ ekvivalentní s podmínkou $(v_1, v_2, v_3, \ldots, v_{m+1}) \in \mathbb{L}'$. Nejdřív dokážeme první implikaci: $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) \in \mathbb{L}$ implikuje, že $(v_1, v_2, v_3, \ldots, v_{m+1}) \in \mathbb{L}'$. Předpokládejme, že máme $\boldsymbol{\ell} \in \mathbb{L}$, pro které $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) = \boldsymbol{\ell}$. Máme dva případy, buď $\ell_1 = 0$, nebo $\ell_1 = 1$.

1. Pokud $\ell_1 = 0$, potom $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) = (0, \ell_2, \ldots, \ell_m)$. Neboli platí, že $v_1 \vee v_2 = 0$. A to platí právě tehdy, když $v_1 = v_2 = 0$.
   Tedy $(v_1, v_2, v_3, \ldots, v_{m+1}) = (0, 0, \ell_2, \ldots, \ell_m)$. Protože $(0, \ell_2, \ldots, \ell_m) \in \mathbb{L}$, potom $(0, 0, \ell_2, \ldots, \ell_m) \in \mathbb{L}'$.
   Tedy $(v_1, v_2, v_3, \ldots, v_{m+1}) \in \mathbb{L}'$.

2. Pokud $\ell_1 = 1$, potom $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) = (1, \ell_2, \ldots, \ell_m)$. Neboli platí, že $v_1 \vee v_2 = 1$. Tedy dvojice (v_1,v_2) může být buď (0,1), (1,0) nebo (1,1). Protože $(1, \ell_2, \ldots, \ell_m) \in \mathbb{L}$, potom $(1, 0, \ell_2, \ldots, \ell_m)$, (0,1,$\ell_2, \ldots, \ell_m$), (1,1,$\ell_2, \ldots, \ell_m$) $\in \mathbb{L}'$.
   Tedy $(v_1, v_2, v_3, \ldots, v_{m+1}) \in \mathbb{L}'$.

Tím jsme dokázali první implikaci.

Nyní dokážeme druhou implikaci: $(v_1, v_2, v_3, \ldots, v_{m+1}) \in \mathbb{L}'$ implikuje, že $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) \in \mathbb{L}$.

Předpokládejme, že máme $\boldsymbol{\ell'} \in \mathbb{L}'$, pro které $(v_1, v_2, v_3, \ldots, v_{m+1}) = \boldsymbol{\ell'}$. Máme dva případy, buď $(\ell'_1, \ell'_2) = (0,0)$, nebo $(\ell'_1, \ell'_2) \in \{(1,0), (0,1), (1,1)\}$.

1. Pokud $(\ell'_1, \ell'_2) = (0,0)$, potom $(v_1, v_2, v_3, \ldots, v_{m+1}) = (0, 0, \ell_2, \ldots, \ell_m)$. Tedy $v_1 = v_2 = 0$, z toho plyne, že $v_1 \vee v_2 = 0$.
   Tedy $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) = (0, \ell_2, \ldots, \ell_m)$. Protože $(0, 0, \ell_2, \ldots, \ell_m) \in \mathbb{L}'$, potom $(0, \ell_2, \ldots, \ell_m) \in \mathbb{L}$.
   Tedy $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) \in \mathbb{L}$.

2. Pokud $(\ell'_1, \ell'_2) \in \{(1,0), (0,1), (1,1)\}$, potom $v_1 = \ell'_1, v_2 = \ell'_2$. Potom platí, že $v_1 \vee v_2 = 1$. Neboli $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) = (1, \ell_2, \ldots, \ell_m)$. Protože (1,0,$\ell_2, \ldots, \ell_m$) nebo (0,1,$\ell_2, \ldots, \ell_m$) nebo (1,1,$\ell_2, \ldots, \ell_m$) jsou prvky $\mathbb{L}'$, potom $(1, \ell_2, \ldots, \ell_m) \in \mathbb{L}$.
   Tedy $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) \in \mathbb{L}$.

Tím jsme dokázali ekvivalenci.

Nyní dokážeme, že $\mathbb{Y}$ bude mít $\mathcal{D}^{1^{m+1}}_{\mathbb{K}',\mathbb{L}'}$. Z rovnosti (4.2) dostaneme, že pro každý vektor $\mathbf{v} \in U_{\mathbb{K}'}$ platí, že

$$\bigoplus_{\mathbf{y} \in \mathbb{Y}} \pi_{(v_1, v_2, v_3, \ldots, v_{m+1})}(\mathbf{y}) = \bigoplus_{\mathbf{x} \in \mathbb{X}} \pi_{(v_1 \vee v_2, v_3, \ldots, v_{m+1})}(\mathbf{x}).$$

Dokázali jsme, že $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) \in U_{\mathbb{K}}$. Tedy máme 2 případy:

(a) $(v_1, v_2, v_3, \ldots, v_{m+1}) \in \mathbb{L}'$. Dokázali jsme, že je to ekvivalentní s podmínkou, že $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) \in \mathbb{L}$. Z toho plyne, že

$$\bigoplus_{\mathbf{x} \in \mathbb{X}} \pi_{(v_1 \vee v_2, v_3, \ldots, v_{m+1})}(\mathbf{x}) = 1.$$

(b) $(v_1, v_2, v_3, \ldots, v_{m+1}) \notin \mathbb{L}'$. Potom platí, že $(v_1 \vee v_2, v_3, \ldots, v_{m+1}) \notin \mathbb{L}$. Z toho plyne, že

$$\bigoplus_{\mathbf{x} \in \mathbb{X}} \pi_{(v_1 \vee v_2, v_3, \ldots, v_{m+1})}(\mathbf{x}) = 0.$$

Tedy pokud multimnožina $\mathbb{X}$ má $\mathcal{D}^{1^m}_{\mathbb{K},\mathbb{L}}$, potom platí, že výstupní množina $\mathbb{Y}$ má dělící vlastnost $\mathcal{D}^{1^{m+1}}_{\mathbb{K}',\mathbb{L}'}$.

□

Tvrzení 5 (Pravidlo AND-komprese)**.** *Nechť $\mathbb{X}$ je multimnožina s prvky z $\mathbb{F}_2^m$ a $\mathbb{Y}$ je multimnožina z $\mathbb{F}_2^{m-1}$, definujme funkci AND-komprese $F : \mathbb{F}_2^m \to \mathbb{F}_2^{m-1}$ tak, že*

$$F((x_1,x_2,\ldots,x_m)) = (x_1 \cdot x_2, x_3, \ldots, x_m).$$

Pokud $\mathbb{X}$ má $\mathcal{D}^{1^m}_{\mathbb{K},\mathbb{L}}$, potom $\mathbb{Y} = F(\mathbb{X})$ má $\mathcal{D}^{1^{m-1}}_{\mathbb{K}',\mathbb{L}'}$, kde

$$\mathbb{K}' = \{(k_1 \vee k_2,k_3,k_4,\ldots,k_m) | (k_1,k_2,\ldots,k_m) \in \mathbb{K}\},$$

$$\mathbb{L}' = \{(\ell_1 \vee \ell_2,\ell_3,\ell_4,\ldots,\ell_m) | \ell_1 = \ell_2, (\ell_1,\ell_2,\ldots,\ell_m) \in \mathbb{L}\}.$$

Důkaz. Přepokládejme, že multimnožina $\mathbb{X}$ má $\mathcal{D}^{1^m}_{\mathbb{K},\mathbb{L}}$. Vyhodnotíme výraz $\bigoplus_{\mathbf{y}\in\mathbb{Y}} \pi_{\mathbf{v}}(\mathbf{y})$ pro každý vektor $\mathbf{v} \in U_{\mathbb{K}'}$:

$$\begin{aligned}\bigoplus_{\mathbf{y}\in\mathbb{Y}} \pi_{\mathbf{v}}(\mathbf{y}) &= \bigoplus_{\mathbf{x}\in\mathbb{X}} (\pi_{\mathbf{v}} \circ F)(\mathbf{x}) \\ &= \bigoplus_{\mathbf{x}\in\mathbb{X}} ((x_1 \cdot x_2)^{v_1} x_3^{v_2} \ldots x_m^{v_{m-1}}) \\ &= \bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(v_1,v_1,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}). \end{aligned} \tag{4.4}$$

Podle definice dělící vlastnosti platí, že pro všechna $(v_1, v_1, v_3, \ldots, v_{m-1}) \in U_{\mathbb{K}}$ platí:

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(v_1,v_1,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}) = \begin{cases} 1, & \text{pokud } (v_1, v_1, v_2, v_3, \ldots, v_{m-1}) \in \mathbb{L} \\ 0, & \text{jinak.} \end{cases}$$

Nejdřív dokážeme, že pokud $(v_1, v_2, v_3, \ldots, v_{m-1}) \in U_{\mathbb{K}'}$, potom platí $(v_1, v_1, v_2, v_3, \ldots, v_{m-1}) \in U_{\mathbb{K}}$. Dokážeme obměnu implikace, že pokud $(v_1, v_1, v_2, v_3, \ldots, v_{m-1}) \notin U_{\mathbb{K}}$, potom platí $(v_1, v_2, v_3, \ldots, v_{m-1}) \notin U_{\mathbb{K}'}$. Pokud $(v_1, v_1, v_2, v_3, \ldots, v_{m-1}) \notin U_{\mathbb{K}}$, potom podle definice $U_{\mathbb{K}}$ platí, že

$$\exists \mathbf{k} = (k_1, k_2, \ldots, k_m) \in \mathbb{K} \text{ takové, že } (v_1, v_1, v_2, v_3, \ldots, v_{m-1}) \succeq (k_1, k_2, \ldots, k_m).$$

Z toho plyne, že $v_1 \geq k_1$ a současně $v_1 \geq k_2$. A z toho plyne, že $v_1 \geq k_1 \vee k_2$. Protože $(v_1, v_1, v_2, v_3, \ldots, v_{m-1}) \succeq (k_1, k_2, \ldots, k_m)$, potom pro všechna $i \in \{2, \ldots, m-1\}$ platí $v_i \geq k_{i+1}$.
Z toho plyne, že $(v_1, v_2, v_3, \ldots, v_{m-1}) \succeq (k_1 \vee k_2, k_3, \ldots, k_m)$. A z definice $\mathbb{K}'$ plyne, že vektor $(k_1 \vee k_2, k_3, \ldots, k_m) \in \mathbb{K}'$. Jinak řečeno, že

$$\exists (k_1 \vee k_2, k_3, \ldots, k_m) \in \mathbb{K}' : (v_1, v_2, v_3, \ldots, v_{m-1}) \succeq (k_1 \vee k_2, k_3, \ldots, k_m).$$

Z toho plyne, že $(v_1, v_2, v_3, \ldots, v_{m-1}) \notin U_{\mathbb{K}'}$.

Dále dokážeme, že pro všechna $\mathbf{v} \in U_{\mathbb{K}'}$ je podmínka $(v_1, v_1, v_2, v_3, \ldots, v_{m-1}) \in \mathbb{L}$ ekvivalentní s podmínkou $(v_1, v_2, v_3, \ldots, v_{m-1}) \in \mathbb{L}'$.

Nejdříve dokážeme první implikaci: $(v_1, v_1, v_2, v_3, \ldots, v_{m-1}) \in \mathbb{L}$ implikuje, že $(v_1, v_2, v_3, \ldots, v_{m-1}) \in \mathbb{L}'$. Předpokládejme, že máme $\boldsymbol{\ell} = (\ell_1,\ell_2, \ldots,\ell_m) \in \mathbb{L}$, pro které $(v_1, v_1, v_2, v_3, \ldots, v_{m-1}) = (\ell_1,\ell_2, \ldots,\ell_m)$. Z toho plyne, že $\ell_1 = v_1 = \ell_2$. Protože $(\ell_1,\ell_2, \ldots,\ell_m) \in \mathbb{L}$ a $\ell_1 = \ell_2$, potom $(\ell_1 \vee \ell_2, \ldots,\ell_m) \in \mathbb{L}'$.

Platí, že $(v_1, v_2, v_3, \ldots, v_{m-1}) = (v_1 \vee v_1, v_2, v_3, \ldots, v_{m-1}) = (\ell_1 \vee \ell_2, \ldots,\ell_m)$. Z toho plyne, že $(v_1, v_2, v_3, \ldots, v_{m-1}) \in \mathbb{L}'$.

Tím jsme dokázali první implikaci.

Nyní dokážeme druhou implikaci: $(v_1, v_2, v_3, \ldots, v_{m-1}) \in \mathbb{L}'$ implikuje, že $(v_1, v_1, v_2, \ldots, v_{m-1}) \in \mathbb{L}$.
Předpokládejme, že máme $\boldsymbol{\ell'} \in \mathbb{L}'$, pro které $(v_1, v_2, v_3, \ldots, v_{m+1}) = \boldsymbol{\ell'}$. Potom existuje $(\ell_1, \ell_2, \ldots, \ell_m) \in \mathbb{L}$ takové, že $\ell_1 = \ell_2$, a platí, že $\boldsymbol{\ell'} = (\ell_1 \vee \ell_2,\ell_3, \ldots,\ell_m)$. Z toho plyne, že

$$\exists \boldsymbol{\ell} \in \mathbb{L} : (v_1, v_2, v_3, \ldots, v_{m+1}) = (\ell_1 \vee \ell_2,\ell_3,\ell_4, \ldots,\ell_m)\,.$$

Z toho plyne, že pro všechna $i \in \{2,3, \ldots, m-1\}$ platí $v_i = \ell_{i+1}$ a také $v_1 = \ell_1 \vee \ell_2$. Protože $\ell_1 = \ell_2$, potom $v_1 = \ell_1 = \ell_2$. Z toho plyne, že

$$(v_1, v_1, v_2, \ldots, v_{m-1}) = (\ell_1,\ell_2, \ell_3, \ldots,\ell_m).$$

Tedy $(v_1, v_1, v_2, \ldots, v_{m-1}) \in \mathbb{L}$. Tím jsme dokázali ekvivalenci.

Nyní dokážeme, že $\mathbb{Y}$ má $\mathcal{D}^{1^{m-1}}_{\mathbb{K}',\mathbb{L}'}$. Z rovnosti (4.4) dostaneme, že pro každý vektor $\mathbf{v} \in U_{\mathbb{K}'}$ platí, že

$$\bigoplus_{\mathbf{y}\in\mathbb{Y}} \pi_{(v_1,v_2,v_3,\ldots,v_{m-1})}(\mathbf{y}) = \bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(v_1,v_1,v_2,\ldots,v_{m-1})}(\mathbf{x}).$$

Dokázali jsme, že $(v_1, v_1, v_2, v_3, \ldots, v_{m-1}) \in U_{\mathbb{K}}$. Tedy máme 2 případy:

(a) $(v_1, v_2, v_3, \ldots, v_{m-1}) \in \mathbb{L}'$. Dokázali jsme, že je to ekvivalentní s podmínkou, že existuje $(v_1, v_1, v_2, \ldots, v_{m-1}) \in \mathbb{L}$. Z toho plyne, že

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(v_1,v_1,v_2,\ldots,v_{m-1})}(\mathbf{x}) = 1.$$

(b) $(v_1, v_2, v_3, \ldots, v_{m-1}) \notin \mathbb{L}'$. Potom platí, že $(v_1, v_1, v_2, \ldots, v_{m-1}) \notin \mathbb{L}$. Z toho plyne, že

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(v_1,v_1,v_2,\ldots,v_{m-1})}(\mathbf{x}) = 0.$$

Tedy pokud multimnožina $\mathbb{X}$ má $\mathcal{D}^{1^m}_{\mathbb{K},\mathbb{L}}$, potom platí, že výstupní množina $\mathbb{Y}$ má dělící vlastnost $\mathcal{D}^{1^{m-1}}_{\mathbb{K}',\mathbb{L}'}$.

□

Tvrzení 6 (Pravidlo XOR-komprese)**.** *Nechť $\mathbb{X}$ je multimnožina s prvky z $\mathbb{F}_2^m$ a $\mathbb{Y}$ je multimnožina z $\mathbb{F}_2^{m-1}$, definujme funkci XOR-komprese $F : \mathbb{F}_2^m \to \mathbb{F}_2^{m-1}$ tak, že*

$$F((x_1,x_2, \ldots, x_m)) = (x_1 \oplus x_2,x_3, \ldots, x_m).$$

Pokud $\mathbb{X}$ *má* $\mathcal{D}^{1^m}_{\mathbb{K},\mathbb{L}}$, *potom* $\mathbb{Y} = F(\mathbb{X})$ *má* $\mathcal{D}^{1^{m-1}}_{\mathbb{K}',\mathbb{L}'}$, *kde*

$$\mathbb{K}' = \{(k_1 \vee k_2, \mathbf{k}_{3..m}) | (k_1,k_2) \neq (1,1), (k_1,k_2,\mathbf{k}_{3..m}) \in \mathbb{K}\},$$

$\mathbb{L}' = \{(0,\boldsymbol{\ell}_{3..m}) | (0,0,\boldsymbol{\ell}_{3..m}) \in \mathbb{L}\}$
$\cup \{(1,\boldsymbol{\ell}_{3..m}) | \exists (\ell_1,\ell_2) \in \{(1,0),(0,1)\} : (\ell_1,\ell_2,\boldsymbol{\ell}_{3..m}) \in \mathbb{L} \wedge (\ell_2,\ell_1,\boldsymbol{\ell}_{3..m}) \notin \mathbb{L}\}$,

kde $\mathbf{k}_{3..m}$ *značí složky* $k_3,k_4,\ldots,k_m$, *a* $\boldsymbol{\ell}_{3..m}$ *značí složky* $\ell_3,\ell_4,\ldots,\ell_m$.

Důkaz. Přepokládejme, že multimnožina $\mathbb{X}$ má $\mathcal{D}^{1^m}_{\mathbb{K},\mathbb{L}}$. Vyhodnotíme výraz $\bigoplus_{\mathbf{y}\in\mathbb{Y}} \pi_{\mathbf{v}}(\mathbf{y})$ pro každý vektor $\mathbf{v} \in U_{\mathbb{K}'}$:

$$\begin{aligned}\bigoplus_{\mathbf{y}\in\mathbb{Y}} \pi_{\mathbf{v}}(\mathbf{y}) &= \bigoplus_{\mathbf{x}\in\mathbb{X}} (\pi_{\mathbf{v}} \circ F)(\mathbf{x}) \\ &= \bigoplus_{\mathbf{x}\in\mathbb{X}} ((x_1 \oplus x_2)^{v_1} x_3^{v_2} \ldots x_m^{v_{m-1}}).\end{aligned}$$

Máme dva případy. Buď $v_1 = 0$ nebo $v_1 = 1$:

(A.) $v_1 = 0$, potom

$$\begin{aligned}\bigoplus_{\mathbf{y}\in\mathbb{Y}} \pi_{\mathbf{v}}(\mathbf{y}) &= \bigoplus_{\mathbf{x}\in\mathbb{X}} ((x_1 \oplus x_2)^0 x_3^{v_2} \ldots x_m^{v_{m-1}}) \\ &= \bigoplus_{\mathbf{x}\in\mathbb{X}} (x_1^0, x_2^0, x_3^{v_2} \ldots x_m^{v_{m-1}}) \\ &= \bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(0,0,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}). \end{aligned} \tag{4.5}$$

Podle definice dělící vlastnosti platí, že pro všechna $(0,0,v_3,\ldots,v_{m-1}) \in U_{\mathbb{K}}$:

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(0,0,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}) = \begin{cases} 1, & \text{pokud } (0,0,v_2,v_3,\ldots,v_{m-1}) \in \mathbb{L} \\ 0, & \text{jinak.} \end{cases}$$

Nejdřív dokážeme, že pokud $(0,v_2,v_3,\ldots,v_{m-1}) \in U_{\mathbb{K}'}$, potom platí, že $(0,0,v_2,v_3,\ldots,v_{m-1}) \in U_{\mathbb{K}}$. Dokážeme obměnu implikace, že pokud $(0,0,v_2,v_3,\ldots,v_{m-1}) \notin U_{\mathbb{K}}$, potom platí, že $(0,v_2,v_3,\ldots,v_{m-1}) \notin U_{\mathbb{K}'}$.

Předpokládejme, že $(0,0,v_2,v_3,\ldots,v_{m-1}) \notin U_{\mathbb{K}}$, potom podle definice $U_{\mathbb{K}}$ platí, že

$$\exists \mathbf{k} = (k_1,k_2,\ldots,k_m) \in \mathbb{K} \text{ takové, že } (0,0,v_2,v_3,\ldots,v_{m-1}) \succeq (k_1,k_2,\ldots,k_m).$$

Z toho plyne, že $\forall i \in \{2,3,\ldots,m-1\} : v_i \geq k_{i+1}$ a $0 \geq k_1$ a $0 \geq k_2$. Neboli $k_1 = k_2 = 0$. Z toho plyne

$$v_1 = 0 \geq k_1 \vee k_2.$$

Tímto dostáváme, že

$$(0,v_2,\ldots,v_{m-1}) \succeq (k_1 \vee k_2, k_3 \ldots, k_m).$$

Z definice $\mathbb{K}'$ plyne, že $(k_1 \vee k_2, k_3 \ldots, k_m) \in \mathbb{K}'$. Tudíž existuje $(k_1 \vee k_2, k_3 \ldots, k_m) \in \mathbb{K}'$ takové, že platí $(0,v_2,\ldots,v_{m-1}) \succeq (k_1 \vee k_2, k_3 \ldots, k_m)$. Tedy $(0,v_2,\ldots,v_{m-1}) \notin U_{\mathbb{K}'}$.

Tím jsme dokázali implikaci, že pokud $(0, v_2, \ldots, v_{m-1}) \in U_{\mathbb{K}'}$, potom $(0, 0, v_2, \ldots, v_{m-1}) \in U_{\mathbb{K}}$.

Nyní předpokládáme, že $(0, v_2, v_3, \ldots, v_{m-1}) \in U_{\mathbb{K}'}$. Přímo z definice množiny $\mathbb{L}'$ plyne, že $(0, v_2, v_3, \ldots, v_{m-1}) \in \mathbb{L}'$ právě tehdy, když $(0, 0, v_2, \ldots, v_{m-1}) \in \mathbb{L}$.

Nyní dokážeme, že $\mathbb{Y}$ má $\mathcal{D}^{1^{m-1}}_{\mathbb{K}',\mathbb{L}'}$. Pro všechna $(0, v_2, \ldots, v_{m-1}) \in U_{\mathbb{K}'}$ z rovnosti (4.5) platí, že

$$\bigoplus_{\mathbf{y}\in\mathbb{Y}} \pi_{(0,v_2,v_3,\ldots,v_{m-1})}(\mathbf{y}) = \bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(0,0,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}).$$

Dokázali jsme, že pokud $(0, v_2, v_3, \ldots, v_{m-1}) \in U_{\mathbb{K}'}$, potom platí, že $(0, 0, v_2, v_3, \ldots, v_{m-1}) \in U_{\mathbb{K}}$. Tedy máme 2 případy:

(a) $(0, v_2, v_3, \ldots, v_{m-1}) \in \mathbb{L}'$. Dokázali jsme, že je to ekvivalentní s podmínkou, že $(0, 0, v_2, \ldots, v_{m-1})$ je prvek množiny $\mathbb{L}$. Potom platí:

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(0,0,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}) = 1.$$

(b) $(0, v_2, v_3, \ldots, v_{m-1}) \notin \mathbb{L}'$. Je to ekvivalentní s tím, že $(0, 0, v_2, \ldots, v_{m-1}) \notin \mathbb{L}$. Potom platí:

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(0,0,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}) = 0.$$

Tím jsme dokázali tvrzení pro případ $v_1 = 0$.

(B.) $v_1 = 1$, potom

$$\begin{aligned}\bigoplus_{\mathbf{y}\in\mathbb{Y}} \pi_{\mathbf{v}}(\mathbf{y}) &= \bigoplus_{\mathbf{x}\in\mathbb{X}} ((x_1 \oplus x_2)^1 x_3^{v_2} \ldots x_m^{v_{m-1}}) \\ &= \bigoplus_{\mathbf{x}\in\mathbb{X}} (x_1^1 x_3^{v_2} \ldots x_m^{v_{m-1}}) \oplus (x_2^1 x_3^{v_2} \ldots x_m^{v_{m-1}}) \\ &= \bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(1,0,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}) \oplus \bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(0,1,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}). \qquad (4.6)\end{aligned}$$

Podle definice dělící vlastnosti platí, že pro všechna $(1, 0, v_3, \ldots, v_{m-1}) \in U_{\mathbb{K}}$ platí:

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(1,0,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}) = \begin{cases} 1, & \text{pokud } (1, 0, v_2, v_3, \ldots, v_{m-1}) \in \mathbb{L} \\ 0, & \text{jinak.} \end{cases}$$

Pro všechna $(0, 1, v_3, \ldots, v_{m-1}) \in U_{\mathbb{K}}$:

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(0,1,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}) = \begin{cases} 1, & \text{pokud } (0, 1, v_2, v_3, \ldots, v_{m-1}) \in \mathbb{L} \\ 0, & \text{jinak.} \end{cases}$$

Nejdříve dokážeme, že pokud $(1, v_2, v_3, \ldots, v_{m-1}) \in U_{\mathbb{K}'}$, potom platí, že oba vektory $(1, 0, v_2, v_3, \ldots, v_{m-1})$ a $(0, 1, v_2, v_3, \ldots, v_{m-1})$ jsou prvky množiny $U_{\mathbb{K}}$. Dokážeme obměnu implikace, že pokud alespoň jeden vektor $(1, 0, v_2, v_3, \ldots, v_{m-1}) \notin U_{\mathbb{K}}$ nebo $(0, 1, v_2, v_3, \ldots, v_{m-1}) \notin U_{\mathbb{K}}$, potom platí, že $(1, v_2, v_3, \ldots, v_{m-1}) \notin U_{\mathbb{K}'}$.

Předpokládejme, že $(1, 0, v_2, v_3, \ldots, v_{m-1}) \notin U_{\mathbb{K}}$, potom podle definice $U_{\mathbb{K}}$ platí, že

$$\exists \mathbf{k} = (k_1, k_2, \ldots, k_m) \in \mathbb{K} \text{ takové, že } (1, 0, v_2, v_3, \ldots, v_{m-1}) \succeq (k_1, k_2, \ldots, k_m).$$

Z toho plyne, že $\forall i \in \{2,3, \ldots, m-1\}$ platí: $v_i \geq k_{i+1}, 1 \geq k_1$ a $0 \geq k_2$. Neboli $k_2 = 0$. Tím jsme dostali

$$1 \geq k_1 + 0 = k_1 \vee k_2.$$

Tudíž

$$(1, v_2, \ldots, v_{m-1}) \succeq (k_1 \vee k_2, k_3 \ldots, k_m).$$

Z definice $\mathbb{K}'$ plyne, že $(k_1 \vee k_2, k_3 \ldots, k_m) \in \mathbb{K}'$. Z toho plyne, že existuje $(k_1 \vee k_2, k_3 \ldots, k_m) \in \mathbb{K}'$ takové, že platí $(1, v_2, \ldots, v_{m-1}) \succeq (k_1 \vee k_2, k_3 \ldots, k_m)$. Tedy $(1, v_2, \ldots, v_{m-1}) \notin U_{\mathbb{K}'}$.

Zcela podobně snadno ukážeme, že pokud $(0, 1, v_2, \ldots, v_{m-1}) \notin U_{\mathbb{K}}$, potom $(1, v_2, \ldots, v_{m-1}) \notin U_{\mathbb{K}'}$.
Tím jsme dokázali implikaci, že $(1, v_2, \ldots, v_{m-1}) \in U_{\mathbb{K}'}$, potom oba vektory $(1, 0, v_2, \ldots, v_{m-1})$ a $(0, 1, v_2, \ldots, v_{m-1})$ jsou prvky množiny $U_{\mathbb{K}}$.

Nyní předpokládejme, že $(1, v_2, \ldots, v_{m-1}) \in U_{\mathbb{K}'}$. Dále budeme dokazovat dichotomii, že $(1, v_2, v_3, \ldots, v_{m-1}) \in \mathbb{L}'$ právě tehdy, když buď $(1, 0, v_2, \ldots, v_{m-1}) \in \mathbb{L}$, nebo $(0, 1, v_2, \ldots, v_{m-1}) \in \mathbb{L}$.

Nejdříve dokážeme první implikaci: $(1, v_2, \ldots, v_{m-1}) \in \mathbb{L}'$ implikuje, že jeden ze dvou vektorů $(1, 0, v_2, \ldots, v_{m-1}), (0, 1, v_2, \ldots, v_{m-1})$ je prvkem množiny $\mathbb{L}$.
Předpokládejme, že $\boldsymbol{\ell'} \in \mathbb{L}'$, pro které $(1, v_2, v_3, \ldots, v_{m-1}) = \boldsymbol{\ell'}$. Potom platí, že buď $(1, 0, v_2, \ldots, v_{m-1}) \in \mathbb{L}$, nebo $(0, 1, v_2, \ldots, v_{m-1}) \in \mathbb{L}$. Tím jsme dokázali první implikaci.

Nyní dokážeme druhou implikaci, pokud jeden ze dvou vektorů $(1, 0, v_2, \ldots, v_{m-1}), (0, 1, v_2, \ldots, v_{m-1})$ je prvkem množiny $\mathbb{L}$, potom platí, že $(1, v_2, \ldots, v_{m-1}) \in \mathbb{L}'$.
Předpokládejme, že $(1, 0, v_2, \ldots, v_{m-1}) \in \mathbb{L}$ a současně $(0, 1, v_2, \ldots, v_{m-1}) \notin \mathbb{L}$. Potom platí, že $(1, v_3, \ldots, v_{m-1}) \in \mathbb{L}'$.
Předpokládejme v opačném případě, že $(1, 0, v_2, \ldots, v_{m-1}) \notin \mathbb{L}$ a současně $(0, 1, v_2, \ldots, v_{m-1}) \in \mathbb{L}$. Potom platí, že $(1, v_3, \ldots, v_{m-1}) \in \mathbb{L}'$. Tím jsme dokázali ekvivalenci.

Nyní dokážeme, že $\mathbb{Y}$ má $\mathcal{D}^{1^{m-1}}_{\mathbb{K}',\mathbb{L}'}$. Pro všechna $(1, v_2, \ldots, v_{m-1}) \in U_{\mathbb{K}'}$ z rovnosti (4.6) platí, že

$$\bigoplus_{\mathbf{y} \in \mathbb{Y}} \pi_{(1,v_2,v_3,\ldots,v_{m-1})}(\mathbf{y}) = \bigoplus_{\mathbf{x} \in \mathbb{X}} \pi_{(1,0,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}) \oplus \bigoplus_{\mathbf{x} \in \mathbb{X}} \pi_{(0,1,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}).$$

Dokázali jsme, že pokud prvek $(1, v_2, v_3, \ldots, v_{m-1}) \in U_{\mathbb{K}'}$, potom platí, že oba dva vektory $(1, 0, v_2, v_3, \ldots, v_{m-1})$ a $(0, 1, v_2, v_3, \ldots, v_{m-1})$ jsou prvky množiny $U_{\mathbb{K}}$. Tedy máme 2 případy: $(1, v_2, v_3, \ldots, v_{m-1}) \in \mathbb{L}'$ je ekvivalentní s podmínkou, že pouze jeden ze dvou vektorů $(1, 0, v_2, \ldots, v_{m-1})$, $(0, 1, v_2, \ldots, v_{m-1})$ je prvkem množiny $\mathbb{L}$.

(a) $(1, v_2, v_3, \ldots, v_{m-1}) \in \mathbb{L}'$. Dokázali jsme, že je to ekvivalentní s podmínkou, že pouze jeden ze dvou vektorů $(1, 0, v_2, \ldots, v_{m-1})$, $(0, 1, v_2, \ldots, v_{m-1})$ je prvkem množiny $\mathbb{L}$. Máme tedy dva případy:

i. $(1, 0, v_2, \ldots, v_{m-1}) \in \mathbb{L}$ a $(0, 1, v_2, \ldots, v_{m-1}) \notin \mathbb{L}$, potom platí:

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(1,0,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}) \oplus \bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(0,1,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}) = 1 \oplus 0 = 1.$$

ii. $(1, 0, v_2, \ldots, v_{m-1}) \notin \mathbb{L}$ a $(0, 1, v_2, \ldots, v_{m-1}) \in \mathbb{L}$, potom platí:

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(1,0,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}) \oplus \bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(0,1,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}) = 0 \oplus 1 = 1.$$

(b) $(1, v_2, v_3, \ldots, v_{m-1}) \notin \mathbb{L}'$. Potom platí, že bud' oba vektory $(1, 0, v_2, \ldots, v_{m-1})$,$(0, 1, v_2, \ldots, v_{m-1})$ nepatří do $\mathbb{L}$ nebo oba dva jsou prvky množiny $\mathbb{L}$.

i. pokud oba vektory $(1, 0, v_2, \ldots, v_{m-1}), (0, 1, v_2, \ldots, v_{m-1}) \in \mathbb{L}$, potom platí:

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(1,0,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}) \oplus \bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(0,1,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}) = 1 \oplus 1 = 0.$$

ii. pokud oba $(1, 0, v_2, \ldots, v_{m-1}), (0, 1, v_2, \ldots, v_{m-1})$ nepatří do $\mathbb{L}$, potom platí:

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(1,0,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}) \oplus \bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{(0,1,v_2,v_3,\ldots,v_{m-1})}(\mathbf{x}) = 0 \oplus 0 = 0.$$

Tedy pokud multimnožina $\mathbb{X}$ má $\mathcal{D}^{1^m}_{\mathbb{K},\mathbb{L}}$, potom platí, že výstupní množina $\mathbb{Y}$ má dělící vlastnost $\mathcal{D}^{1^{m-1}}_{\mathbb{K}',\mathbb{L}'}$.

□

Závěr

Hlavními výsledky práce jsou, vedle zpracování několika dílčích aspektů teorie z článků Todo (2015), Todo a Morii (2016) a Wang a kol. (2014), doplnění ilustrativních příkladů a sepsání vlastních důkazů tvrzení klíčových pro další použití dělící vlastnosti.

Popsali jsme obecný koncept integrálního útoku a uvedli konkretní příklad útoku na SIMON32. Vlatními slovy jsme popsali propagaci pro jádro rundové funkce šifry SIMON. Formulovali jsme tvrzení o tom, jak se šíří bitová dělící vlastnost po propagaci a ukázali vlastní důkaz. Zadefinovali jsme množinu $U_{\mathbb{K}}$, která nám pomohla lépe definovat bitovou dělící vlastnost se třemi podmnožinami. Přeformulovali jsme tvrzení pravidla propagace bitové dělící vlastnosti se třemi podmnožinami pro funkce kopírování, AND-komprese, XOR-komprese tak, aby byla matematicky správná. Uvedli jsme vlastní důkazy, které byly v článku Todo a Morii (2016) jen naznačeny. V důkazu tvrzení Pravidlo XOR-komprese bylo nutné rozlišit na dva případy, že buď $v_1 = 0$ nebo $v_1 = 1$.

Motivace pro zkoumání bitové dělící vlastnosti se třemi podmnožinami je způsob, jak dokázat obecnou existenci integrální charakteristiky, která je nalezena v experimentu od Wang a kol. (2014). V této práci se dál praktickému využití nevěnujeme, to by mohlo být námětem dalšího zkoumání.

Aplikace dělící vlastnosti se třemi množinami na šifře SIMON2n, kterým se tato práce již nevěnuje, lze najít v sekcích 4.6, 4.7. článku Todo a Morii (2016).

Seznam použité literatury

Knudsen, L. a Wagner, D. (2002). Integral cryptanalysis (extended abstract.

Todo, Y. (2015). Integral cryptanalysis on full misty1. *JRosario Gennaro and Matthew Robshaw*, **9215 of LNCS**, 298–299.

Todo, Y. a Morii, M. (2016). Bit-based division property and application to simon family. *International Conference on Fast Software Encryption*, pages 357–377.

Wang, Q., Liu, Z., Varici, K., Sasaki, Y., Rijmen, V. a Todo, Y. (2014). Cryptanalysis of reduced-round simon32 and simon48. pages 143–160.

Z'aba, M. R., Raddum, H., Henricksen, M. a Dawson, E. (2008). Bit-pattern based integral attack. pages 363–381.

Seznam obrázků

1.1 Schéma rundové funkce u SIMON2n. 6

3.1 Jádro rundové funkce šifry SIMON2n. 10