Bitová dělící vlastnost a aplikace na Simon family

Kieu Trang Phamová

30. Března 2020

Osnova

Upozorňuji, že jde o celkem odbornou prezentaci. Neuvedla jsem uplně všechny definice pojmů. Přepokládám znalost kryptografie čtenáře nebo je s její problematikou lehce obeznámen. Dále některé fráze ponechám v anglické podobě, protože neznám jejich český překlad, nebo je považuju za základní fráze, které čtenář jistě zná. Děkuji za pochopení!

Značení

- Dvouprvková množina $\mathbb{F}_2$
- $\mathbb{F}_2^n$ je množina n-složkových vektorů nad $\mathbb{F}_2$
- $\forall a \in \mathbb{F}_2^n$ označme a[i] jako i-tý prvek vektoru a
- Hammingova váha vektoru a: $w(a) = \sum_{i=1}^{n} a[i]$
- $\forall \mathbf{a} \in (\mathbb{F}_2^{n_1} x \mathbb{F}_2^{n_2} x ... x \mathbb{F}_2^{n_m})$ definujeme Vektorovou Hammingovou váhu a:

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

- $\forall \mathbf{k}, \mathbf{l} \in \mathbb{Z}^m : \mathbf{k} \succeq \mathbf{l} \Leftrightarrow k_i \geq l_i \forall i.$
- Množinu takových $\mathbf{k}$ označme $\mathbb{K}$

Motivace

- Najít Integrální vlastnost u blokových šifer, abychom mohli provést Integrální útok.
- Známe velmi užitečnou techniku jak najít integrální vlastnost pro S-boxové šifry z článku the Full MISTY1 in CRYPTO 2015. Ale tahle technika dokáže prolomit pouze šifry, které mají S-boxy jako MISTY1.
- Ukážeme, že Dělící vlastnost umožňuje hledat Integrální vlastnost u šifer, které nemají S-boxy.

Bloková šifra

- Bloková šifra je typ symetrické šifry, kde se pracuje s bloky pevně stanovené délky. Pokud je dat více, rozdělí se na více bloků, přičemž do zbylého místa v posledním je umístěna výplň.
- Při šifrování je každý blok zakódován pomocí šifrovacího algoritmu řízeného utajeným šifrovacím klíčem. Dešifrování probíhá stejným postupem pomocí stejného klíče.
- S-box neboli substitution box (volně přeloženo zaměňovací krabička) je část symetrické šifry, se jedná o funkci $S : \{0,1\}^m \to \{0,1\}^n$, tedy jde o nelineární část šifry, která zaručí bezpečnost šifry.
- Bloková šifra může ale nemusí mít S-box

Simon Family jako bloková šifra bez S-boxu

Simon Family je rodina blokových šifer, které jsou založeny na Feistelovy konstrukci

Definice (Simon Family)

SIMON2n je Simon 2n-bitová bloková šifra. Výstup i-té rundové funkce je $(L_i, R_i) = (L_{i-1}^{<<<1} \wedge L_{i-1}^{<<<8}) \otimes L_{i-1}^{<<<2} \otimes R_{i-1} \otimes k_i, L_{i-1})$. Kde (L_0, R_0) je vstupní plaintext, k_i i-tý rundový klíč. Funkce jsou $<<<$ rotace, $\otimes$ XOR, $\wedge$ AND.

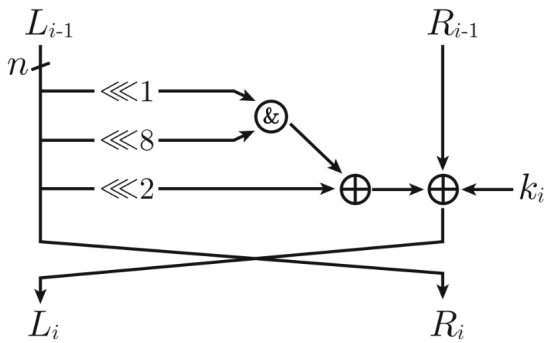

Fig. 1. Round function of SIMON2n

Definice Integrální útok

- Útočník se snaží prolomit blokovou šifru např. SIMON32. Útočník zná algoritmus šifry ale nezná tajný klíč, a snaží se ho dostat.
- Útočník připraví N plaintextů a zašifruje na R rundy (R kola)

Definice (R-rundová integrální vlastnost)

Pokud provede XOR operaci na všechny zašifrované zprávy (něco jako suma XOR) a dostaneme výsledek 0. Říkáme, že šifra má R-rundovou integrální vlastnost s N vybranými plaintexty.

- Potom útočník využije integrální vlastnost pro obnovení tajného klíče

Funkce bitového součinu

Abychom mohli definovat dělící vlastnost, potřebujeme funkci bitového součinu.

Definice

Nechť $\pi_u : \mathbb{F}_2^n \to \mathbb{F}_2$ funkce bitového součinu pro každý $u \in \mathbb{F}_2^n$. Nechť $x \in \mathbb{F}_2^n$ platí, že $\pi_u(x)$ je výsledek operace AND všech těch x[i] splňující u[i] $= 1$.

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

Snadno všímáme, že $x[i]^1 = x[i]$ a $x[i]^0 = 1$

Funkce bitového součinu

Zobecníme definici

Definice

Nechť $\pi_{\mathbf{u}} : (\mathbb{F}_2^{n_1} x \mathbb{F}_2^{n_2} x ... x \mathbb{F}_2^{n_m}) \rightarrow \mathbb{F}_2$ funkce bitového součinu pro každý $\mathbf{u} \in (\mathbb{F}_2^{n_1} x \mathbb{F}_2^{n_2} x ... x \mathbb{F}_2^{n_m})$. Nechť $\mathbf{x} \in (\mathbb{F}_2^{n_1} x \mathbb{F}_2^{n_2} x ... x \mathbb{F}_2^{n_m})$ platí, že:

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

Dělící vlastnost

Definice (Dělící vlastnost)

Nechť $\mathbb{X}$ je multimnožina s prvkami z $(\mathbb{F}_2^{n_1} x \mathbb{F}_2^{n_2} x ... x \mathbb{F}_2^{n_m})$. Řekneme, že $\mathbb{X}$ má Dělící vlastnost $\mathcal{D}_{\mathbb{K}}^{n_1,n_2,...,n_m}$, kde $\mathbb{K}$ označí množinu m-složkových vektorů, jejichž i-tý prvek má hodnotu mezi 0 a n_i, splňuje následující podmínky:

$$\bigoplus_{\mathbf{x} \in \mathbb{X}} \pi_{\mathbf{u}}(\mathbf{x}) = \begin{cases} \textit{neznámé}, & \text{pokud } \exists \mathbf{k} \in \mathbb{K} \text{ takové, že } W(\mathbf{u}) \succeq \mathbf{k} \\ 0, & \text{jinak} \end{cases} \tag{1}$$

- Tedy $\bigoplus_{\mathbf{x} \in \mathbb{X}} \pi_{\mathbf{u}}(\mathbf{x})$ bude nula pro Hammingovou váhu menší než k

Bitová dělící vlastnost

- Jednoduše řečeno bitová dělící vlastnost je aplikace dělící vlastnosti na každý bit vstupu.
- Přeformuluje, mějme $\mathbb{X} \subseteq (\mathbb{F}_2)^m$ a dále $\mathbf{k}$ je m-složkový vektor složený z 0 nebo 1. Řekneme, že $\mathbb{X}$ má bitovou dělící vlastnost $\mathcal{D}^{1^m}_{\mathbb{K},\mathbb{L}}$ pokud:

$$\bigoplus_{\mathbf{x}\in\mathbb{X}} \pi_{\mathbf{u}}(\mathbf{x}) = \begin{cases} \textit{neznámé}, & \text{pokud } \exists \mathbf{k} \in \mathbb{K} \text{ takové, že } W(\mathbf{u}) \succeq \mathbf{k} \\ 1, & \text{pokud } \exists \mathbf{l} \in \mathbb{L} : W(\mathbf{u}) = \mathbf{l} \\ 0, & \text{jinak} \end{cases} \tag{2}$$

Bitová dělící vlastnost - příklad

- priklad

Aplikace na SIMON family

- Jak najdeme integrální vlastnost šifry SIMON32 pomocí bitové dělící vlastnosti?
- Trik je v tom, že se zaměříme pouze na 1 bit, a postup opakujeme pro všechny bity pravé poloviny vstupu, a zašifujeme podle SIMON32.
- Hlavní operace je veřejná funkce a nevyžaduje žádné tajemství informace. Můžeme tedy vyhodnotit propagace z $\mathbb{K}$ a $\mathbb{L}$ nezávisle.
- Dále může být propagace na rundové funkci vyhodnocena opakováním pro všechny bity pravé poloviny. Když jsou rundové klíče XOR-ovány s pravou polovinou, nové vektory jsou generovány z $\mathbb{L}$ a nové vektory jsou vloženy do $\mathbb{K}$. viz Fig.1

Výsledek

- Výsledek = výstup 14. rundové funkce má $\mathcal{D}^{1^3 2}_{\mathbb{K},\phi}$ kde phi prázdá množina. Tato dělící vlastnost znamená, že výstup 14. rundové funkce má následující integrální vlastnost (????, ????, ????, ????,? b ??, ????, b ???, ??? b), kde vyvážený bit = b a neznámé bity = ? . V SIMON32 můžeme snadno získat 15-rundovou integrální vlastnost ze 14-rund, tedy je prokázaná integrální vlastnost.
- Docházíme proto k závěru, že experimentální charakteristika není pravděpodobnostní ale funguje pro všechny klíče.

Děkuji za pozornost!