NORMALIZED INTER-CLASS VARIANCE V PROUDOVÉ ANALÝZE

Vaněk Stanislav
Bachelor Degree Programme (3), FEEC BUT
E-mail: xvanek35@stud.feec.vutbr.cz

Supervised by: Martinásek Zdeněk
E-mail: martinasek@feec.vutbr.cz

Abstract: The internet of things leads to a massive interest in security of embedded devices. Nowadays, power analysis poses extremely effective and successful types of attacks to break confidential cryptographic algorithms such as AES (Advanced Encryption Standard), RSA (Rivest Shamir Adleman) and cryptographic devices such as smart cards. This paper deals with the method of localization of interesting markers in power analysis called NICV (Normalized Inter-Class Variance). The aim of the paper is to describe this method and its implementation.

Keywords: NICV, DPA, CPA, variance

1 ÚVOD

Masivní nasazení vestavěných systémů vede k velkému zájmu o jejich zabezpečení. Proudová analýza měří a zkoumá proudovou spotřebu kryptografického zařízení s cílem odhalit korelaci proudové spotřeby a senzitivní informace, kterou představuje většinou šifrovací klíč. Proudová analýza představuje v dnešní době efektivní a velice účinný způsob útoku na doposud bezpečné kryptografické primitiva jako AES, RSA a kryptografická zařízení jako čipové karty, jednočipové počítače atd.

Při proudové analýze představuje nejkritičtější část detekce zajímavých bodů, kterými je vyzařována požadovaná senzitivní informace. Je zřejmé, že detekce zajímavých bodů je důležitá také pro ochranu proti proudové analýze, protože dokážeme detekovat únik informace a následně jej eliminovat.

2 METODY DETEKCE ZAJÍMAVÝCH BODŮ

Pro detekci zajímavých bodů v proudové analýze se používají různé metody, nejznámější je DPA (Differnetial Power Analysis) založená na korelačním koeficientu. Dalšími metodami, které lze použít jsou např. metoda založená na rozdílu sumy čtverců (SOSD), nebo metoda založená rozdílu sumy čtverců s T-testem (SOST). Metoda NICV (Normalized Inter-Class Variance) není běžně implementována v prostředích zabývající se proudovou analýzou. Mým cílem bylo tuto metodu implementovat v prostředí Matlab a následně ověřit funkčnost na veřejně dostupných proudových průbězích ze soutěže DPA Contest.

3 NICV

NICV se dá volně přeložit jako analýza rozptylu. Oproti jiným metodám má útočník výhodu v tom, že nepotřebuje profilující zařízení, tedy pracuje přímo s průběhy, na které je aplikována proudová analýza (útok). Další výhodou je, že veškeré parametry potřebné k útoku jsou veřejné, a tudíž útočníkovi známé. Naopak nevýhodou této metody je, že je oproti jiným metodám méně přesná.

3.1 MATEMATICKÉ VYJÁDŘENÍ

Označme si jeden byte otevřeného nebo zašifrovaného textu X a proudovou spotřebu měřenou útočníkem Y. Pak vztah pro výpočet analýzy rozptylu mezi těmito veličinami bude následující:

$$NICV = \frac{(Var[E[Y|X|]])}{(Var[Y])}, \tag{1}$$

kde Var značí rozptyl a E průměr.

3.2 IMPLEMENTACE

Praktická realizace této metody byla provedena ve vývojovém prostředí MATLAB. Naměřené proudové průběhy a nástroje byly získány ze soutěže DPA Contest. Cílem této soutěže je poskytnout objektivní způsob porovnání metod proudové analýzy, především DPA útoku veřejnosti. Použité kryptografické zařízení je programovatelná čipová karta ATmega, která má v sobě naimplementována algoritmus AES-256 a k maskování tohoto algoritmu slouží metoda RSM (Rotating Sbox Masking). Implementovaný algoritmus je zobrazen na obr.1. Algoritmus funguje následovně, na začátku je vygenerován offset, který musí být udržen v tajnosti (hodnota 0 až 15). Podle této hodnoty je rotována sada šestnácti konstantních masek, která je veřejně známá. Následuje rotace řádků a poté mixování sloupců bytu otevřeného textu. Jako poslední je provedena korekce masky.

Implementace AES použitá pro DPAContestv4

Input : 16-bytes Plaintext X $[\![X_0, X_1 \cdots X_{15}]\!]$, // 16 bajtů otevřeného textu
Key, 15 16-bytes constants RoundKey$[r]$, $r \in [\![0, 14]\!]$ // Rozšiřování klíče
Output: 16-bytes Ciphertext X $[\![X_0, X_1 \cdots X_{15}]\!]$ // Šifrovaný text - 16 bajtů

Draw a random offset, uniformly in $[\![0, 15]\!]$ // Náhodně generovaný offset s náhodným rozdělením
$X = X \oplus \text{Mask}_{\text{offset}}$ // Maskování otevřeného textu

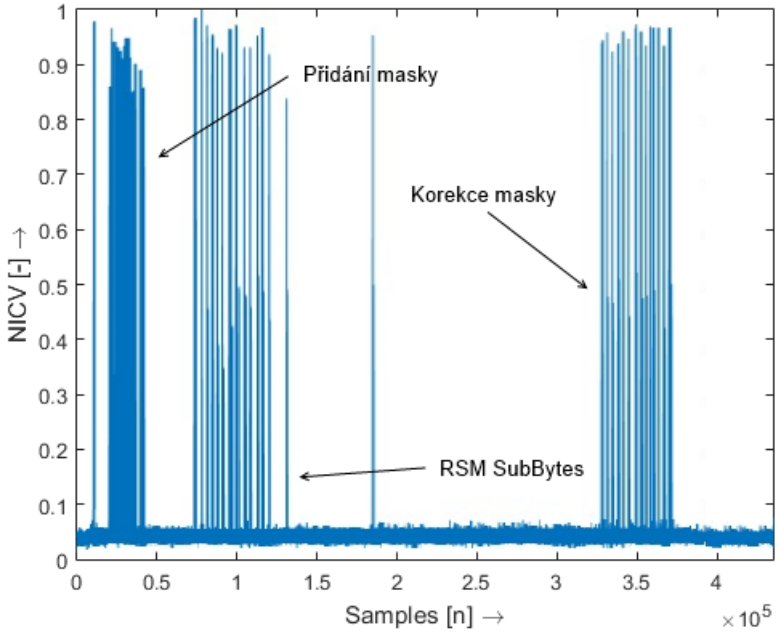
// Všechny rundy kromě poslední
for $r \in [\![0, 12]\!]$ **do**
  $X = X \oplus \text{RoundKey}[r]$
  for $i \in [\![0, 15]\!]$ **do** // Add round key
    $X_i = \text{MaskedSubBytes}_{\text{offset}+i+r}(X_i)$
  end
  $X = \text{ShiftRows}(X)$ // Rotace řádků
  $X = \text{MixColumns}(X)$ // Mixování sloupců
  $X = X \oplus \text{MaskCompensation}_{\text{offset}+1+r}$ // Korekce masky
end

// Poslední runda
$X = X \oplus \text{RoundKey}[13]$
for $i \in [\![0, 15]\!]$ **do**
  $X_i = \text{MaskedSubBytes}_{\text{offset}+13+r}(X_i)$
end
$X = \text{ShiftRows}(X)$
$X = X \oplus \text{RoundKey}[14]$

// Unmasking zašifrovaného textu
$X = X \oplus \text{MaskCompensationLastRound}_{\text{offset}+14}$

Obrázek 1: Algoritmus AES-256

Nejprve je třeba se rozhodnout, na co přesně chce útočník útočit. V tomto případě je to byte otevřeného textu po vykonání první rundy algoritmu AES, ze kterého by útočník mohl zachytit citlivé informace. Nejprve je pomocí NICV vypočítán rozptyl hypotézy proudové spotřeby. Následně je spočítán rozptyl pro měřenou proudovou spotřebu. Poté je provedena korelační proudová analýza (CPA). Výsledkem je matice koeficientů NICV, což je matice obálek korelačních koeficientů. Čím více se hodnota v matici koeficientů NICV blíží 1, tím větší je závislost mezi hypotetickou proudovou spotřebou a změřenou proudovou spotřebou. Naopak hodnoty blížící se k 0 značí velmi nízkou, téměř nulovou závislost.



Obrázek 2: NICV spočítané pro byte otevřeného textu

Na obr. 2 je vidět 48 bodů. Tyto body odpovídají bělení textu, přidání klíče, funkci SubBytes a korekci masky. Při úniku těchto dat ze zařízení může být jeden složený útok, na tento únik, dostačující pro obnovu klíče. Jestliže je známá sekvence masky, útočníkovi pak stačí na základě masky odhalit klíč a ten nahrát do svého zařízení (přístupové karty) a pomocí této karty se může vydávat za pravého majitele.

4 ZÁVĚR

Metoda analýzy rozptylu NICV je jedna z metod lokalizace zajímavých bodů u proudové analýzy. Nicméně jen samotné NICV k nalezení citlivých informací nestačí. Je nutné ještě provést korelační proudovou analýzu (CPA), díky které už lze vyčíst z průběhů citlivé informace. NICV funguje tedy jako tzv. předpříprava průběhů či zrychlení analýzy pro další zpracování útočníkem. Velmi často je analýza rozptylu používána právě spolu s CPA pro zrychlení analýzy.

REFERENCE

[1] MORADI, Amir, Sylvain GUILLEY a Annelie HEUSER. *Detecting Hidden Leakages* [online]. [cit. 2016-03-7]. Dostupné z: https://eprint.iacr.org/2013/842.pdf

[2] BHASIN, Shivam, Nicolas BRUNEAU, Jean-Luc DANGER a Zakaria NAJM. *Analysis and Improvements of the DPA Contest v4 Implementation*.

[3] BHASIN, Shivam, Jean-Luc DANGER a Zakaria NAJM. *NICV: Normalized Inter-Class Variance for Detection of Side-Channel Leakage** [online]. , 17 [cit. 2016-03-7]. Dostupné z: https://eprint.iacr.org/2013/717.pdf