VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

**Ing. Zdeněk Martinásek**

# KRYPTOANALÝZA POSTRANNÍMI KANÁLY

## SIDE CHANNEL CRYPTANALYSIS

ZKRÁCENÁ VERZE PH.D. THESIS

Obor: Teleinformatika
Školitel: doc. Ing. Václav Zeman, Ph.D.
Oponenti: Ing. Tomáš Vaněk, Ph.D.
doc. Ing. Jaromír Dočkal, CSc.
Datum obhajoby: 11.7.2013

**KLICOVA SLOVA**
Postranní kanály, proudový postranní kanál, jednoduchá proudová analýza, diferenciální proudová analýza, neuronové sítě, proudová analýza pomocí neuronových sítí

**KEYWORDS**
Side channels, power side channel, simple power analysis, differential analysis, neural networks, power analysis using neural networks

**Místo uložení práce**

Práce je k dispozici na Vědeckém oddělení děkanátu Fakulty Elektrotechniky a komunikačních technologií VUT v Brně, Technická 10, Brno, 616 00.

© Zdeněk Martinásek, 2013
ISBN 978-80-214-4786-8
ISSN 1213-4198

# OBSAH

**Úvod** **5**

**1 Cíle disertace** **6**

**2 Současný stav problematiky** **7**
2.1 Jednoduchá proudová analýza SPA . . . . . 7
2.2 Diferenciální proudová analýza DPA . . . . . 7
2.2.1 Útok založený na korelačním koeficientu . . . . . 9
2.2.2 Útok založený na rozdílu středních hodnot . . . . . 9
2.2.3 Diferenciální proudová analýza - shrnutí . . . . . 10
2.3 Protiopatření proti proudové analýze . . . . . 10
2.4 Neuronové sítě v kryptografii . . . . . 11

**3 Vlastní řešení - proudová analýza** **12**
3.1 Proudová analýza využívající neuronové sítě . . . . . 12

**4 Závěr** **25**

**Literatura** **26**

**Literatura** **28**

# ÚVOD

Se stále zrychlujícím se vývojem moderních komunikačních a počítačových systémů se objevila řada nových typů útoků na kryptografické systémy. Útočníci neodposlouchávají pasivně přenosový kanál, ale využívají stále sofistikovanějších metod kryptoanalýzy. Všechny kryptografické služby zajišťuje v systému kryptografický modul, který bývá součástí bezpečnostního subsystému. Tento modul je v podstatě fyzickou implementací konkrétního kryptografického algoritmu popř. protokolu. Realizace kryptografického modulu může být hardwarová, softwarová nebo kombinovaná. Během činnosti kryptografického modulu probíhají uvnitř procesy, které jsou spojeny s šifrováním, dešifrováním, ověřením, autentizací atd. Během těchto činností pracuje modul se senzitivními daty (např. šifrovací klíč), které bývají uloženy v paměti modulu. Z toho plyne, že praktická realizace kryptografického modulu, která v sobě obsahuje všechny pravidla, klíče a další senzitivní materiál, do značné míry ovlivňuje bezpečnost celého systému.

Dosavadní konvenční způsoby kryptoanalýzy se soustředily na objevení slabiny v matematické podstatě kryptografických algoritmů. Proti v současnosti používaným šifrovacím algoritmům je tento způsob neefektivní a časově prakticky nerealizovatelný. Nový způsob kryptoanalýzy, využívající postranní kanály (Side Channels), se soustředí na konkrétní implementace algoritmů a protokolů. Při konstrukci modulu se předpokládá jediná možná komunikace modulu s okolím a to jen prostřednictvím přesně definované vstupů a výstupů. V reálném prostředí modul během své činnosti komunikuje se svým okolím i jiným, nežádoucím způsobem. Modul může vyzařovat do svého okolí např. tepelné nebo elektromagnetické záření, každý reálný modul při své činnosti odebírá určitý proud ze zdroje, každá jeho operace způsobuje různé časové zpoždění, na konkrétní situaci reaguje modul stavovým nebo chybovým hlášením, klávesnice modulu může být mechanicky opotřebená atd. Všechny tyto projevy modulu jsou neodmyslitelně spojeny s jeho činností, při které mohou být vyneseny některé ze senzitivních informací. Každý nežádoucí způsob výměny informace mezi kryptografickým modulem a jeho okolím se nazývá postranním kanálem. Analýzou postranního kanálu (Side Channels analysis) je označován postup, při kterém je možné získat užitečné informace, které lze odvodit ze signálu přicházejícím po tomto kanálu. Útok vedený pomocí postranního kanálu je založen na využití takto získané informace k napadení daného kryptografického modulu a získání tak senzitivních informací.

Koncept útoku postranními kanály, tak jak je chápán v dnešní době, zadefinoval a popsal Kocher v práci [17] v roce 1999. Princip útoku byl proveden na algoritmus Data Encryption Standard metodou založenou na rozdílu středních hodnot. Postranní kanály se prakticky využívaly dříve, kdy se definice postranních kanálů nepoužívala. Akustický postranní kanál patří k nejstarším používaným postranním kanálům, např. v roce 1956 Britové získávají informace z egyptského šifrátoru odposlechem zvuků klávesnice a v roce 1961 Američané provádějí akustický odposlech prostřednictvím ústředního topení. Elektromagnetický postranní kanál byl ve své historii také nejdříve využíván v armádě a tajných službách. Tyto organizace se odborně zabývaly studiem problematiky parazitních emisí, která označovaly termínem TEMPEST. Hlavním zájmem vojenských organizací bylo zamezení nežádoucích emisí a naopak využití tohoto vyzařování k špionážní činnosti. Pojem TEMPEST vznikl na přelomu 60. a 70.let dvacátého století a označuje i skupinu vojenských standardů, ve kterých jsou stanoveny maximální povolené limity elektromagnetického záření v různých elektronických systémech. Ve veřejném sektoru se o významný posuv na poli elektromagnetických útoků zasloužil nizozemský vědec van Eck [9], který jako první dokázal, že je možné zachytit a změřit velikost elektromagnetického pole počítačových monitorů a z naměřených průběhů extrahovat snímaný obraz. První veřejně publikovanou prací na téma EM analýzy integrovaných obvodů a výpočetních jednotek provádějících kryptografické operace, byla v roce 2001 práce [12].

Postranní kanály zcela mění celkový pohled na bezpečnost systému. Již nestačí zvolit kvalitní šifru ale je nezbytné velkou pozornost věnovat i její implementaci. Návrháři a konstruktéři kryptografického modulu často neví a ani nemohou vědět o existenci všech nežádoucích postranních kanálů. Existují ovšem některé postranní kanály, které jsou schopni minimalizovat. V současné době neexistuje žádný konkrétní návod pro návrh zcela imunního kryptografického modulu vůči postranním kanálům, ale existují testy které otestují navrhovaný modul na některé konkrétní typy postranních kanálů a na množství unikající informace.

# 1 CÍLE DISERTACE

Disertační práce bude zaměřena na jednoduchou a diferenciální analýzu proudovým postranním kanálem. Hlavním cílem disertační práce bude návrh nové metody proudové analýzy, která umožní určit hodnotu šifrovacího klíče jen z jednoho proudového průběhu a to u algoritmů, které jsou odolné vůči jednoduché proudové analýze. Do jisté míry bude navržená metoda spojovat vlastnosti jednoduché a diferenciální proudové analýzy. Většina proudových analýz využívá různé statistické metody (rozdíl středních hodnot, korelační koeficient atd. viz kapitola 2) k určení závislosti proudové spotřeby a hledané senzitivní informace. Navrhovaná metoda bude založena na odlišném způsobu a plánuje využít neuronové sítě ke klasifikaci senzitivní informace z naměřených průběhů proudové spotřeby. Tento typ útoku proudovým postranním kanálem, který bude zaměřen na klasifikaci konkrétní hodnoty šifrovacího klíče, nebyl dosud publikován. Navržená metoda bude pracovat odlišným způsobem než klasické metody, a proto se předpokládají odlišné vlastnosti např. potřebný počet naměřených proudových průběhů, úspěšnost určení šifrovacího klíče atd. Analýza těchto parametrů je dalším cílem disertační práce. K ověření funkce nové metody je nutné navrhnout a ověřit metodu pro snímání a záznam proudového odběru kryptografického modulu. Způsob a přesnost měření proudového odběru má zásadní vliv na správnou funkci navrhované metody kryptoanalýzy. Z tohoto důvodu je nutné sestavit experimentální pracoviště včetně kryptografického modulu s implementovaným kryptografickým algoritmem, a navrhovanou metodu analýzy implementovat a prakticky ověřit její funkčnost. Proudové analýzy jsou testovány většinou na implementaci algoritmu AES, proto bude navržená metoda proudové analýzy využívající neuronové sítě také testována pomocí implementace kryptografického algoritmu AES. Posledním důležitým dílčím cílem práce je analýza možných ochran proti proudové analýze a útoku postranním kanálem. Z analyzovaných ochran vybrat vhodné řešení zabraňující použití navržené metody.

Cíle disertační práce mohou být shrnuty do následujících bodů:

- analýza současného stavu problematiky (proudová analýza, protiopatření proti proudové analýze, neuronové sítě),
- návrh a realizace metody pro měření proudového odběru, způsob snímání proudu má zásadní vliv na úspěšnost navrhované metody proudové analýzy,
- návrh a implementace nové metody proudové analýzy využívající neuronové sítě,
- analýza a zhodnocení dosažených výsledků klasifikace.

# 2 SOUČASNÝ STAV PROBLEMATIKY

Cílem kapitoly je detailně popsat jednoduchou a diferenciální proudovou analýzu používanou při útoku na kryptografické zařízení. Na podobných principech jsou založeny všechny jednoduché a diferenciální analýzy postranním kanálem. Další část kapitoly popisuje techniky protiopatření vedoucí k znesnadnění a nebo plnému znemožnění útoku proudovým postranním kanálem. Závěrečná část kapitoly rozebírá použití neuronových sítí v kryptografii a v oblasti postranních kanálů.

## 2.1 Jednoduchá proudová analýza SPA

Jednoduchá proudová analýza byla definována Kocherem [17] následovně: jednoduchá proudová analýza je technika, která představuje přímé interpretování proudové spotřeby měřené během provozu kryptografického zařízení. Jinými slovy se útočník snaží určit šifrovací klíč přímo ze změřených průběhů proudové spotřeby. To činí SPA pro potencionální útočníky atraktivní technikou, ale ti většinou potřebují detailní znalost implementovaného algoritmu a kryptografického zařízení. SPA můžeme rozdělit do dvou základních skupin a to na analýzu jen jednoho proudového průběhu (single-shot SPA) a analýzu několika proudových průběhů (multiple-shot). Analýza jednoho proudového průběhu představuje extrémní případ, kdy útočník zaznamenal a zkoumá jen jeden průběh proudové spotřeby odpovídající jednomu vstupnímu textu. Ve většině případů je nutné použít statistických metod k extrakci užitečného signálu. Při jednoduché analýze několika proudových průběhů má útočník k dispozici více naměřených proudových průběhů, a to pro stejný nebo různý vstupní text, které použije k redukci šumu v naměřených datech. Pro oba typy útoku SPA je nutné, aby v kryptografickém zařízení, na které je prováděn útok, existovala výrazná (přímá nebo nepřímá) závislost proudové spotřeby na hodnotě šifrovacího klíče.

## 2.2 Diferenciální proudová analýza DPA

Cílem útoků DPA je získat šifrovací klíč kryptografického zařízení na základě znalosti velkého počtu proudových spotřeb, které byly zaznamenány útočníkem během provádění operace šifrování nebo dešifrování pro různá vstupní data. Hlavní výhodou diferenciální proudové analýzy ve srovnání s SPA je, že útočník nepotřebuje detailní znalost kryptografického zařízení a šifrovacího algoritmu. Dalším důležitým rozdílem mezi těmito analýzami způsob zpracování naměřených dat. V SPA jsou proudové průběhy zpracovávány většinou v časové ose. Útočník se zde pokouší v jednom proudovém průběhu najít vzor, známý otisk instrukce nebo šablonu. Naproti tomu, tvar proudového průběhu v časové oblasti není v DPA důležitý. DPA analyzuje závislost proudové spotřeby v určitý konstantní časový okamžik na právě zpracovávaných datech. V následujícím textu bude popsán detailněji postup získání šifrovacího klíče metodou DPA. Všechny DPA útoky využívají prakticky stejného postupu, který se skládá z pěti kroků.

#### První krok: Volba mezivýsledku algoritmu

Prvním krokem DPA je volba mezivýsledku kryptografického algoritmu, který je vykonáván zařízením. Mezivýsledek musí být funkcí $f(d, k)$, kde $d$ jsou známá nekonstantní data a $k$ je malá část šifrovacího klíče (např. první bajt). Ve většině případů DPA útoku $d$ představuje otevřený text nebo šifrovaný text. Takto definovaný mezivýsledek může být použit k určení části šifrovacího klíče $k$.

#### Druhý krok: Měření proudové spotřeby

Druhým krokem DPA útoku je měření proudové spotřeby kryptografického zařízení při šifrování nebo dešifrování různých bloků dat $D$. Pro všechny operace šifrování či dešifrovaní potřebuje útočník znát hodnoty zpracovávaných dat $d$, které se podílí na výpočtu mezivýsledku zvoleného v prvním kroku. Hodnoty známých dat tvoří vektor $\mathbf{d} = (d_1, \ldots, d_D)'$, kde $d_i$ označuje hodnotu $i$-tého kroku šifrování nebo dešifrování. V průběhu

každého tohoto kroku si útočník zaznamenává proudovou spotřebu. Průběhy proudové spotřeby, korespondující s bloky dat $d_i$, označíme $t_i^{'} = (t_{i,1}, \ldots, T_{i,T})$, kde $T$ označuje délku naměřené proudové spotřeby. Útočník měří proudovou spotřebu pro každý blok dat $D$, a proto naměřené průběhy mohou být zapsány do matice $\mathbf{T}$ o velikosti $D \times T$. Pro DPA útok je klíčové, aby naměřené proudové průběhy byly přesně zarovnané. To znamená, že hodnoty pro jednotlivé sloupce $t_j$ matice $\mathbf{T}$ musí odpovídat stejné operaci. K získání takto zarovnaných dat je nutná správná synchronizace s měřicím zařízením, nebo je zapotřebí zarovnat data softwarově pomocí nalezení několika markantů (otisků v proudovém průběhu).

#### Třetí krok: Výpočet hypotetických mezivýsledků

Dalším krokem útoku je výpočet hypotetických mezivýsledků pro všechny možné hodnoty šifrovacího klíče $k$. Všechny možnosti klíče lze zapsat jako vektor $\mathbf{k} = (k_1, \ldots, k_K)$, kde $K$ označuje celkový počet možných klíčů. V DPA jsou jednotlivé prvky vektoru $\mathbf{k}$ označovány za hypotézy klíče nebo odhady klíče. Z vektoru známých dat $\mathbf{d}$ a vektoru hypotéz všech klíčů může útočník jednoduše vypočítat hodnotu mezivýsledku $f(d, k)$ pro všechny šifrovací operace $D$ a pro všechny hypotézy klíče $K$. Výsledkem výpočtu je matice $\mathbf{V}$ o rozměrech $D \times K$ vypočtená dle následujícího vztahu:

$$v_{i,j} = f(d_i, k_j)\ i = 1, \ldots, D\ j = 1, \ldots, K \tag{2.1}$$

Sloupec $j$ matice $\mathbf{V}$ obsahuje mezivýsledky, které byly vypočítány dle hypotéz klíče $k_j$. Je zřejmé, že jeden sloupec matice $\mathbf{V}$ obsahuje takové mezivýsledky, které byly vypočítány v zařízení během šifrování a dešifrování. Jinými slovy, jednotlivé sloupce matice $\mathbf{V}$ obsahují mezivýsledky pro všechny klíče, tedy i pro klíč který byl použit v zařízení. Tento index bude označen $ck$, tedy $k_{ck}$ označuje hledaný tajný klíč. Cílem DPA je nalezení odpovídajícího sloupce, který byl zpracováván při operacích šifrování a dešifrování v zařízení a tedy nalezení $k_{ck}$.

#### Čtvrtý krok: Mapování hypotetických mezivýsledků na hodnoty proudové spotřeby

Čtvrtým krokem DPA útoku je namapování matice hypotetických mezivýsledků $\mathbf{V}$ na matici $\mathbf{H}$ reprezentující předpokládané hodnoty proudové spotřeby. V tomto bodě se využívá simulace proudové spotřeby kryptografického zařízení. Použitý model spotřeby přiřadí každému hypotetickému mezivýsledku $v_{i,j}$ předpokládanou hodnotu proudové spotřeby $h_{i,j}$. Správnost výsledků simulace silně závisí na útočníkových znalostech o zařízení a činní DPA efektivnější. Mezi často používané modely přiřazení hodnot $\mathbf{V}$ na $\mathbf{H}$ patří model Hammingovy vzdálenosti a Hammingovy váhy.

#### Pátý krok: Porovnání hypotetických hodnot s naměřenými průběhy proudové spotřeby

V posledním kroku útočník porovná předpokládané hodnoty proudové spotřeby závislé na odhadu klíče (hodnoty ve sloupci $h_i$ matice $\mathbf{H}$) se změřenými průběhy proudové spotřeby (hodnoty ve sloupci $t_j$ matice $\mathbf{T}$). Výsledkem je matice $\mathbf{R}$ velikosti $K \times T$, kde každý element $r_{i,j}$ představuje výsledek porovnání sloupců $h_i$ a $t_j$. Samotné porovnání je realizováno různými metodami, které jsou detailněji popsány v následujícím textu (jsou uvedeny dvě nejznámější metody kapitoly 2.2.1 a 2.2.2). Společná vlastnost všech postupů je, že hodnota $r_{i,j}$ je větší pro lepší shodu sloupců $h_i$ a $t_j$. Určení tajného klíče využívá následujících skutečností.

- Proudové průběhy odpovídají proudové spotřebě zařízení během provádění algoritmu šifrování nebo dešifrování pro různá vstupní data.
- Mezivýsledek, který byl vybrán v prvním kroku, je částí tohoto algoritmu.

Z těchto důvodu počítá zařízení hodnotu mezivýsledku $v_{ck}$ v průběhu šifrování nebo dešifrování pro různá vstupní data. V důsledku toho jsou naměřené průběhy v určitých časových okamžicích závislé na hodnotě mezivýsledku. Označíme toto místo naměřených průběhů jako $ct$ (to znamená, že sloupec $t_{ct}$ obsahuje hodnoty proudové spotřeby, které závisí na hodnotě mezivýsledku $v_{ck}$). Hypotetické hodnoty proudové spotřeby $h_{ck}$ byly simulovány útočníkem na základě hodnot $v_{ck}$. Proto jsou sloupce $h_{ck}$ a $t_{ct}$ na sobě silně závislé. Ve

skutečnosti tyto dva sloupce vedou k největší hodnotě v **R**, to znamená, že největší hodnota matice **R** je hodnota $r_{ck,ct}$. Další prvky matice **R** mají malou hodnotu, protože ostatní sloupce **H** a **T** nejsou na sobě silně závislé. Útočník tak může určit index pro správný klíč *ck* a časový okamžik *ct* jednoduše a to nalezením největší hodnoty v matici **R**. Příslušné indexy této hodnoty jsou pak výsledkem DPA útoku.

V praxi se může stát, že všechny hodnoty z **R** si budou prakticky rovny. V tomto případě útočník nezměřil dostatečné množství proudových průběhů k ustanovení vztahu mezi řádky **H** a **T**. Čím více průběhů útočník změří, tím více elementů budou mít sloupce **H** a **T** a tím lépe může útočník určit vztah mezi sloupci.

### 2.2.1 Útok založený na korelačním koeficientu

Korelační koeficient (Correlation coefficient) patří k nejznámější metodě k určení lineární závislosti mezi dvěma náhodnými proměnnými. Proto je to také vhodná metoda pro provedení DPA útoku. Existuje velmi dobře definovaná teorie pro korelační koeficient, který může být použit k modelování statických vlastností DPA útoků. Korelační koeficient je definován pro veličiny $X$ a $Y$ pomocí kovariance vztahem:

$$\rho(X,Y) = \frac{Cov(X,Y)}{\sqrt{\sigma^2(X) \cdot \sigma^2(Y)}}, \tag{2.2}$$

kde $Cov(X,Y)$ označuje kovarianci tedy střední hodnotu součinu odchylek obou náhodných veličin $X$, $Y$ od jejich středních hodnot a $\sigma^2(X)$ a $\sigma^2(Y)$ označují rozptyl těchto veličin. Veličina $\rho$ je bezrozměrná a může nabývat hodnot $-1 \leq \rho \leq 1$. Hodnota $-1$ korelačního koeficientu značí nepřímou závislost (změna v jedné skupině je provázena opačnou změnou ve skupině druhé). Hodnota 0 korelačního koeficientu značí, že mezi hodnotami obou skupin neexistuje žádná statisticky zjistitelná lineární závislost. Při nulovém korelačním koeficientu na sobě veličiny mohou záviset, ale tento vztah nelze vyjádřit lineární funkcí. Jestliže korelační koeficient je roven 1, značí to přímou závislost, dokonalou korelaci mezi hodnotami obou skupin. Výpočet $\rho$ se liší podle typu zkoumaných statistických proměnných. V případě, že náhodné veličiny $X$ a $Y$ jsou kvantitativní náhodné veličiny se společným dvourozměrným normálním rozdělením, je pro konkrétní hodnoty $(x_1, y_1)$, $(x_2, y_2)$, …, $(x_n, y_n)$ výběrový korelační koeficient dán vztahem:

$$r = \frac{\sum_{i=1}^{n}(x_i - \overline{x}) \cdot (y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \overline{x})^2 \cdot \sum_{i=1}^{n}(y_i - \overline{y})^2}}. \tag{2.3}$$

V DPA je korelační koeficient použit k určení lineární závislosti mezi sloupci $h_i$ a $t_j$ pro $i = 1, \ldots, K$ a $j = 1, \ldots, T$. Výsledkem je matice **R** obsahující korelační koeficienty. Označíme každou hodnotu jako $r_{i,j}$ na základě elementů $D$ ze sloupců $h_i$ a $t_j$. Použijeme-li předchozí definici korelačního koeficientu, můžeme vztah 2.3 vyjádřit:

$$r_{i,j} = \frac{\sum_{d=1}^{D}(h_{d,i} - \overline{h_i}) \cdot (t_{d,j} - \overline{t_j})}{\sqrt{\sum_{d=1}^{D}(h_{d,i} - \overline{h_i})^2 \cdot \sum_{d=1}^{D}(t_{d,j} - \overline{t_j})^2}}, \tag{2.4}$$

kde $\overline{h_i}$ a $\overline{t_j}$ označují průměrné hodnoty sloupců $h_i$ a $t_j$.

### 2.2.2 Útok založený na rozdílu středních hodnot

Základem statistické metody založené na rozdílu středních hodnot (Difference of mean) je srovnání dvou skupin naměřených hodnot (distribucí) výpočtem rozdílu středních hodnot těchto skupin. Systematický popis metody je uveden v práci [32]. Tato metoda používá jiný způsob k určení závislosti mezi sloupci matice **H** a **T**. Útočník vytvoří binární matici **H**, která rozdělí naměřené proudové průběhy do dvou skupin. Posloupnost nul a jedniček v každém sloupci **H** je funkcí vstupních dat $d$ a odhadů klíče $k_i$. Za účelem ověření zda odhad klíče $k_i$ je správný útočník může rozdělit matici **T** na dva soubory řádků (tzn. dvě sady proudových spotřeb podle $h_i$). První soubor obsahuje ty řádky matice **T**, kde index odpovídá pozici nul ve vektoru $h_i$. Druhý soubor obsahuje zbylé řádky **T**. Následně útočník vypočítá průměr řádků. Vektor $m'_{0i}$ značí průměr řádků prvního souboru a $m'_{1i}$ označuje průměr druhého souboru. Odhad klíče $k_i$ je správný pokud existuje výrazný

rozdíl mezi $m'_{0i}$ a $m'_{1i}$. Rozdíl mezi $m'_{0i}$ a $m'_{1i}$ indikuje vztah mezi $h_{ck}$ a některým ze sloupců $\mathbf{T}$. Stejně tak jako v předchozím případě tato diference označuje časový okamžik kdy jsou mezivýsledky odpovídající $h_{ck}$ zpracovávány. V jiných okamžicích je diference mezi vektory rovna nule. Výsledkem útoku je tedy matice $\mathbf{R}$, kde každý řádek odpovídá rozdílu mezi vektory $m'_{0i}$ a $m'_{1i}$ pro jeden odhad klíče. Rovnice výpočtu $\mathbf{R}$ je dána vztahem:

$$m'_{1i,j} = \frac{1}{n_{1i}} \cdot \sum_{l=1}^{n} h_{l,i} \cdot t_{l,j}, \tag{2.5}$$

$$m'_{0i,j} = \frac{1}{n_{0i}} \cdot \sum_{l=1}^{n} (1 - h_{l,i}) \cdot t_{l,j}, \tag{2.6}$$

$$n_{1,i} = \sum_{l=1}^{n} h_{l,i}, \tag{2.7}$$

$$n_{0i} = \sum_{l=1}^{n} (1 - h_{l,i}), \tag{2.8}$$

$$\mathbf{R} = \mathbf{M_1} - \mathbf{M_0}, \tag{2.9}$$

kde $n$ značí počet řádků matice $\mathbf{H}$ (tzn. počet naměřených proudových spotřeb).

### 2.2.3 Diferenciální proudová analýza - shrnutí

Koncept útoku DPA byl poprvé popsán v práci [17]. Útok byl proveden na algoritmus DES metodou založenou na rozdílu středních hodnot. Následně pak byly diskutovány možné aplikovatelné statistické testy v [8]. Proudové modely byly poprvé definovány v práci [6] a v [1] byly základní proudové modely analyzovány v kontextu čipových karet. Simulační modely jsou stále modifikovány k zvýšení efektivity PA [29, 27, 10]. V [5] je popsáno použití korelačního koeficientu jako statistické metody. Ve vědecké literatuře se stalo populárním zavádět nové názvy pro DPA útoky, které jsou drobnou variací obecného schématu, např. používají jen jiný statistický test (Korelační analýza [5, 7]). V kontextu DPA je důležité si uvědomit, že pojem DPA útok je nezávislý na použitém statistickém testu nebo použitém mezivýsledku. Pokročilé metody DPA jsou uvedeny v práci [34]. V práci [31] byla představena koncepce stochastických modelů. Útoky vyššího řádu (Higher-order DPA) kombinují DPA útoky pro několik zvolených mezivýsledků algoritmu. Tato myšlenka byla zmíněna již v prvním článku o DPA [17], ale až práce [25] popisuje konkrétní implementaci. Navazující práce [2, 33] popisují metody maskování a útoky vyššího řádu umožňující získat senzitivní data. Důležitá otázka vlivu předzpracování naměřených dat na efektivitu DPA byla prezentována v pracích [13].

## 2.3 Protiopatření proti proudové analýze

Hlavním cílem protiopatření je zajistit, aby proudová spotřeba byla nezávislá na hodnotě mezivýsledku a operacích právě zpracovávaných kryptografickým modulem. Metody a techniky, kterými lze tuto nezávislost více či méně docílit jsou detailněji popsány v následující kapitole. Obecně lze techniky protiopatření kryptografického modulu proti útoku postranním kanálem rozdělit do dvou velkých skupin a to techniky skrývání (hiding) a maskování (masking). Tyto dvě skupiny se následně dělí do dvou podskupin dle implementace na hardwarová a softwarová protiopatření. Cílem skrývání je zajistit, aby proudová spotřeba byla nezávislá na hodnotě mezivýsledků, operacích právě zpracovávaných kryptografickým modulem a hodnotě dat. V podstatě existují dva způsoby jak docílit této požadované nezávislosti. První způsob je vyrobit zařízení takovým způsobem, aby proudová spotřeba byla náhodná. To znamená, že v každém hodinovém taktu bude proudová spotřeba různá i pro stejné instrukce. Druhý způsob je vyrobit zařízení takovým způsobem, že proudová spotřeba bude konstantní pro všechny operace a všechny datové hodnoty, tzn. proudová spotřeba bude v každém hodinovém cyklu stejná. Ideálním cílem skrývání, kterého však v praxi nelze dosáhnout, je realizace takového zařízení. Existuje několik návrhů a řešení jak se k tomuto ideálnímu stavu proudové spotřeby alespoň přiblížit. Tyto

řešení můžeme rozdělit do dvou skupin. První skupina návrhů znáhodní proudovou spotřebu provedením operací kryptografického algoritmu v různých časových okamžicích při každém spuštění algoritmu. Tyto návrhy mají vliv na **časovou oblast proudové spotřeby**. Druhá skupina návrhů si klade za cíl učinit proudovou spotřebu náhodnou nebo konstantní a to přímo změnou charakteristické proudové spotřeby prováděných operací. Z tohoto důvodu mají tyto návrhy vliv na **okamžitou velikost proudové spotřeby**.

Při maskování je každý mezivýsledek $v$ zamaskován náhodnou hodnotou $m$, kterou nazýváme maska $v_m = v * m$. Maska $m$ je generována interně v kryptografickém modulu a pro každé spuštění má jinou hodnotu, proto její hodnotu útočník nezná. Operace $*$ je typicky definovaná dle operací, které jsou použity algoritmem. Tato operace je většinou v kryptografickém modulu realizována exklusivním součtem XOR značeným symbolem $\oplus$ (aditivní maskování) nebo násobením značeným symbolem $\otimes$ (multiplikativní maskování). Ve většině případů jsou masky používány přímo na otevřený text nebo tajný klíč. Při použití maskování musí být implementace algoritmu mírně modifikována s ohledem na maskované mezivýsledky. Výsledkem kryptografického algoritmu je také maska, kterou je nutno odstranit k získání kryptogramu. Typické maskovací schéma popisuje jak jsou všechny mezivýsledky maskovány a jak se masky mění v algoritmu a následně konečné odstranění masek.

## 2.4 Neuronové sítě v kryptografii

Neuronové sítě v kryptografii (Neuro-Cryptography nebo Neural Cryptography) je obor kryptologie věnovaný analýze využití statistických algoritmů, zejména neuronových sítí v kryptografii a kryptoanalýze. Neuronové sítě jsou dobře známé pro svou schopnost selektivně prozkoumat prostor řešení daného problému. Tato funkce jde přirozeně využít v oblasti kryptoanalýzy. Neuronové sítě také nabízí nový přístup k šifrování a dešifrování založený na zásadě, že každá funkce může být reprezentována pomocí neuronové sítě. Neuronové sítě jsou také výkonný výpočetní nástroj, který může být použit k nalezení inverzní funkce šifrovacího algoritmu. Neuronové sítě se nejčastěji využívají v kryptografii v následujících oblastech:

- obdoba asymetrických šifrovacích algoritmů [22],
- problematika distribuce klíčů [16],
- hašovací funkce [21],
- generátory náhodných čísel [35],
- protokol na výměnu klíčů [26] (obdoba Diffie-Hellman protokolu).

Neuronové sítě byly poprvé použity při klasifikaci informací unikajících prostřednictvím akustického postranního kanálu viz [11, 23, 36]. Při analýze proudovým postranním kanálem byla možnost využití neuronových sítí poprvé publikována v práci [30]. Následně na tuto práci navazovali další autoři např. [19, 18], kteří se zabývali klasifikací proudových otisků, tedy přiřazením specifických proudových otisků jednotlivým prováděným instrukcím kryptografického modulu. Jednalo se v podstatě o metody zpětného inženýrství využívající proudovou spotřebu k určení vykonávaného kryptografického algoritmu. Použití neuronových sítí při analýze proudovým postranním kanálem a při klasifikaci konkrétní hodnoty bajtu tajného klíče bylo doposud velice málo publikováno a testováno. Práce zabývající se touto problematikou jsou založeny na algoritmech podpůrných vektorů (Support vector machines (SVM) [14, 4, 15, 20] a nevyužívají klasické vícevrstvé neuronové sítě s algoritmy učení.

# 3 VLASTNÍ ŘEŠENÍ - PROUDOVÁ ANALÝZA

Cílem kapitoly je přehledně shrnout dosažné výsledky. Dle definovaných cílů práce byla nejprve pro ověření teoretických znalostí testována metoda měření proudovým postranním kanálem. Na metodě měření byly testovány různé konfigurace a nastavení, tak aby výsledky měření byly co nejmarkantnější. Nejprve byly porovnávány různé metody měření proudového odběru kryptografického modulu: proudový bočník, proudová sonda, diferenciální sonda, pasivní sondy a pasivní sonda s oddělovacím transformátorem [4]. Následně byl zkoumán vliv parametrů vybrané metody měření využívající odporový bočník na výslednou proudovou analýzu [9, 8]. Zkoumané parametry vycházely z nastudované teorie proudového postranního kanálu: vliv velikosti napájecího napětí, vliv odporu bočníku (při měřicí metodě proudové spotřeby využívající vložený odporový bočník [4]), frekvence hodinového signálu a velikost kapacity blokovacích kondenzátorů. Získané znalosti a zkušenosti byly nezbytné ke správné analýze proudové spotřeby kryptografického modulu a návrhu nové proudové analýzy využívající neuronové sítě.

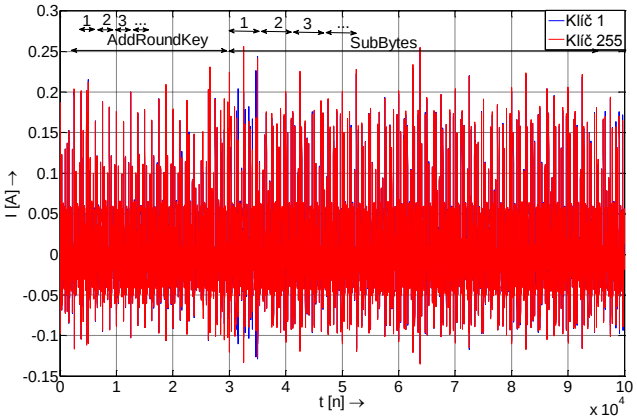
Metoda měření proudovým postranním kanálem byla přizpůsobena pomocí sondy na měření blízkého elektromagnetického pole [7]. Byl porovnán proudový a elektromagnetický průběh šifrovacího algoritmu AES [11] a průběhy byly podrobeny detailní analýze v závislosti na implementovaném algoritmu. Získané elektromagnetické a proudové průběhy byly využity na realizaci útoků elektromagnetickým a proudovým postranním kanálem využívající jednoduchou i diferenciální analýzu [7, 12, 11, 1, 2]. Teoretický návrh optimalizace základní metody diferenciální proudové analýzy využívající rozdíl středních hodnot byl popsán v [3]. Následné experimenty se zaměřily na způsoby klasifikace pomocí neuronových sítí [5, 6]. Kompletní výsledky těchto analýz jsou detailně popsány ve výše uvedených pracích a tato kapitola shrnuje jen nejdůležitější výsledky.

Stěžejní částí této kapitoly je popis navržené analýzy proudovým postranním kanálem využívající neuronovou síť, který odpovídá hlavnímu cíli disertační práce [10]. Konkrétní návrh metody byl rozdělen do tří fází, které jsou postupně detailně popsány včetně naměřených proudových průběhů, implementace a získaných výsledků klasifikace. Závěrečná část kapitoly je popis optimalizace navržené metody, která umožnila zvýšení pravděpodobnosti správné klasifikace šifrovacího klíče, testování opakovatelnosti (realizovatelnosti metody) na větším počtu naměřených proudových průběhů a zhodnocení metody.

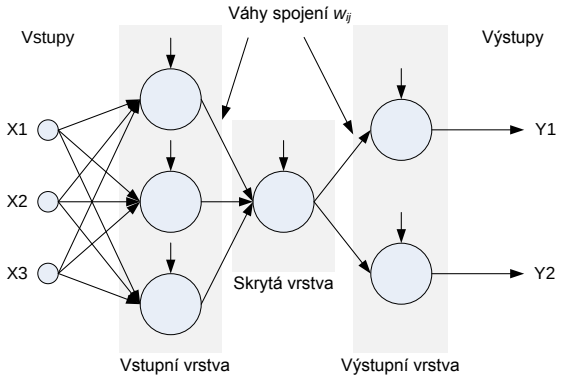
## 3.1 Proudová analýza využívající neuronové sítě

Hlavním cílem disertační práce je návrh a implementace analýzy postranním kanálem, která bude využívat neuronové sítě [10]. Analýza bude zaměřena jen na důležité operace algoritmu AES (operaci `AddRoudnKey` a operaci `SubBytes`), z kterých lze přímo určit tajný klíč algoritmu. Tento typ útoku proudovým postranním kanálem nebyl dosud publikován, jedná se tedy o zcela novou myšlenku. Předpokládá se, že k provedení útoku nebude zapotřebí velké množství měření proudové spotřeby jako například u DPA viz kapitola 2.2. Tato výhoda je stěžejní v porovnání s SPA a DPA a umožní v extrémním případě určení tajného klíče z jednoho proudového průběhu u algoritmů, které jsou odolné vůči SPA. Útočník tak může provést útok na modul, který se mu podařilo získat na krátký čas.

Navrhovaná metoda bude pracovat „per partes“, stejně jako většina analýz postranním kanálem, tedy cílem je určení tajného klíče po jednotlivých bajtech, kde tajný klíč je $K = \{k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8\}$ pro $0 \leq k_i \leq 255$ a pro kroky metody označné $i = 0$ až 8. Navrhovaná metoda tedy v prvním cyklu určí hodnotu prvního bajtu $k_1$ v dalším cyklu druhého $k_2$ a v posledním kroku hodnotu posledního bajtu tajného klíče $k_8$. Rozdíl mezi jednotlivými kroky bude v rozdělení naměřené proudové spotřeby na části odpovídající jednotlivým bajtům tajného klíče.




Obr. 3.1: Průběh proudové spotřeby operací `AddRoundKey` a `SubBytes`.




Obr. 3.2: Obecná struktura třívrstvé neuronové síě.

Na obr. 3.1 je zobrazen naměřený proudový průběh odpovídající operacím `AddRoudnKey` a `SubBytes`, kdy došlo ke změně pouze v prvním bajtu tajného klíče $k_1$ a to z hodnoty 1 na hodnotu 255. Na průběhu jsou jasně patrny úseky, na které má vliv první bajt. Čísla označují jednotlivé části, které odpovídají jednotlivým krokům metody. V následujícím textu bude pojmem tajný klíč ($K_{taj}$) označen klíč uložený v kryptografickém modulu, na který je prováděn útok. Pojmem odhad klíče ($K_{odh}$) bude myšlena hodnota odhadu tajného klíče, kterou klasifikuje navrhovaná metoda. Cílem metody je, aby si na konci analýzy hodnota tajného klíče a odhadu klíče byla rovna. Měření proudových průběhů bylo prováděno pomocí metody měření, která byla důkladně otestováno a byla založena na proudové sondě CT-6. Kompletní implementace navržené a testování byly provedeny v prostředí MATLAB. Toto prostředí poskytuje široké možnosti pro implementaci matematických metod, zpracování signálů, simulace a testování. Velkou výhodou je také dostupnost tzv. toolboxů, souborů funkcí a skriptů, které řeší konkrétní problém. Pro implementaci neuronových sítí byla použita neuronová síť vytvořená pomocí Netlab Neural Network toolbox. Autory tohoto toolboxu jsou Ian Nabney a Christopher Bishop z Aston University v Birminghamu. Toolbox je volně ke stažení [28].

### Navržené obecné schéma metody

Dle výše popsaných skutečností byla navržena a realizována metoda využívající neuronové sítě sestávající se z několika fází:

- fáze přípravy vzorů pro tajné klíče $k_i$,
- fáze vytvoření a trénování neuronové sítě vytvořenými vzory,
- fáze útoku, určení odhadu klíče.

Provedení těchto fází umožní útočníkovi realizovat jeden krok analýzy, tedy určení jednoho bajtu tajného klíče $k_i$. V první fázi si útočník připraví trénovací množinu dat, kterými bude následně učit neuronovou síť. Útočník musí znát typ kryptografického modulu, na který hodlá útočit a musí stejný typ modulu mít zcela pod kontrolou (například plánuje-li útoky na čipovou kartu obsahující mikrokontrolér PIC16F84 musí tuto kartu vlastnit). Na kryptografický modul implementuje požadovaný kryptografický algoritmus a zaznamená proudové průběhy pro operace `AddRoundKey` a `SubBytes` pro všechny varianty tajného klíče $k_i$ (256 možných variant). Naměřené průběhy proudové spotřeby odpovídající práci s bajtem $k_i$ použije útočník k natrénování neuronové sítě, která bude dané průběhy přiřazovat k hodnotám tajného klíče. Po úspěšném natrénování neuronové sítě může útočník pokračovat poslední fází a to fází útoku, kdy využije natrénovanou neuronovou síť k napadení kryptografického modulu. V poslední fázi útoku útočník naměří proudovou spotřebu kryptografického modulu, na který útočí a přivede ji na vstup naučené neuronové sítě. Neuronová síť následně přiřadí proudovou spotřebu k odhadům tajného klíče a odhad klíče s největší pravděpodobností bude odpovídat hodnotě tajného klíče a tím dojde k určení hodnoty $k_i$. V následujícím textu budou popsány jednotlivé fáze navržené analýzy včetně implementace a dosažených výsledků.

**Příprava vzorů**

Cílem této fáze je získat trénovací vzory proudové spotřeby pro operaci `AddRoundKey` a `SubBytes` pro všechny varianty tajného klíče $k_1$ (256 možných variant). Do kryptografického modulu byl implementovány operace `AddRoundKey` a `SubBytes` dle předem ověřených znalostí o algoritmu AES a kryptografickém modulu. Program pracoval ve smyčce a před započetím každé smyčky byla načtena data klíče $k_i$ do paměti tak, aby smyčka vždy pracovala se stejnými vstupními proměnnými. Program umožňoval inkrementovat nebo dekrementovat hodnotu klíče a indikovat tuto operaci odesláním aktuální hodnoty klíče pomocí sériové linky do počítače. Synchronizační signál a komunikace s PC neměla na zkoumanou proudovou spotřebu vliv. Stejně tak jak v předchozí kapitole vyjádříme operaci `AddRoundKey` pro přehlednost a jednoduchost v maticové podobě:

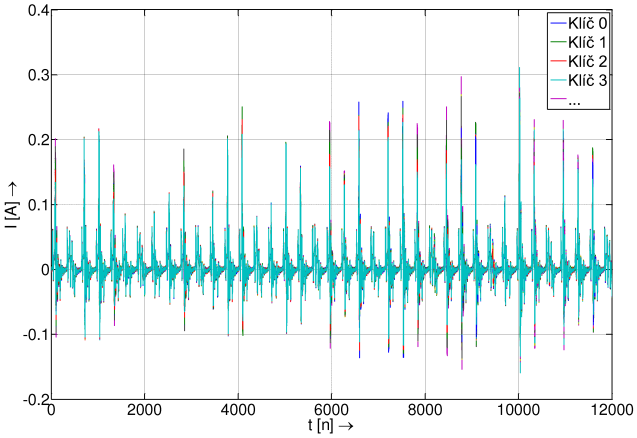
$$\mathbf{S}^{'} = \mathbf{S} \otimes \mathbf{K}. \tag{3.1}$$

V průběhu měření byly hodnoty otevřeného textu $\mathbf{S}$ nastaveny na konstantní hodnoty. Hodnoty prvního bajtu tajného klíče $\mathbf{K}$ nabývaly postupně hodnotu 0 až 255 a zbylé hodnoty byly nulové. Matice tajného klíče a otevřeného textu vypadaly následovně (hexadecimální zápis):

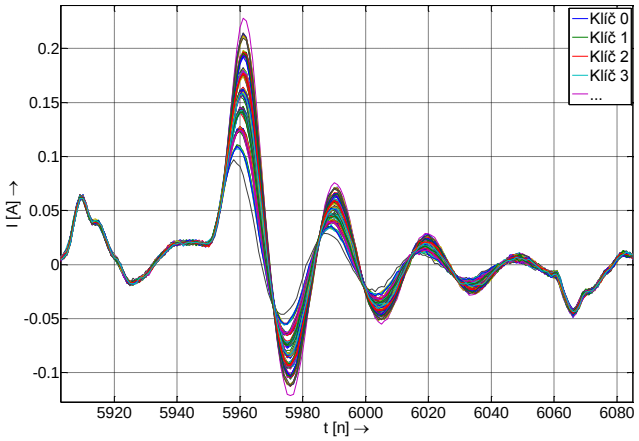
$$\mathbf{S} = \begin{pmatrix} 01 & 03 & 07 & 0F \\ 1F & 3F & 7F & FF \\ 01 & 03 & 07 & 0F \\ 1F & 3F & 7F & FF \end{pmatrix}, \mathbf{K} = \begin{pmatrix} 00 \ldots FF & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{pmatrix}. \tag{3.2}$$

Obr. 3.1 zobrazuje proudové průběhy pro operace `AddRoundKey` a `SubBytes` pro hodnoty klíče 1 a 255. Proudové průběhy jsou si takřka identické s vyjímkou začátku průběhu, který odpovídá načtení registru a operaci `XOR` otevřeného textu s hodnotou tajného klíče a části pro čas $t = 35000$, která odpovídá operacím prováděných během substituce). Je zřejmé, že je zbytečné a značně neefektivní učit neuronovou síť na celé průběhy, a proto byly všechny průběhy redukovány na místa práce s prvním bajtem tajného klíče. Takto redukované a připravené proudové průběhy pro všechny hodnoty tajného klíče určených pro neuronovou síť zobrazuje obr. 3.3. Detail první proudové špičky je zobrazen na obr. 3.4 a je patrné, že proudové průběhy jsou rozděleny do několika skupin, které dle podrobnějšího zkoumání odpovídají HW tajného klíče. Neuronové sítě, které byly použity při klasifikaci akustického signálu [36], byly naučeny (natrénovány) na konkrétní průběhy akustických signálů. Tato metoda předpokládá dostatečné rozdíly mezi jednotlivými průběhy. U proudové analýzy je pravděpodobné, že tento postup povede k neúspěšné klasifikaci instrukcí a to ze dvou základních vlastností PA. První vlastností je, že proudové průběhy jednotlivých instrukcí jsou si velice podobné [3]. Druhou typickou vlastností je, že měříme-li výkonový průběh konkrétní instrukce opakovaně, průběhy nejsou zcela identické a to v důsledku změn pomocných registrů kryptografického modulu (čítač instrukcí atd.). Tato vlastnost bývá nazývána jako elektronický šum (Electronic Noise), který závažným způsobem ovlivňuje výsledky PA. Při přípravě vzorů i během fáze útoku je nutné snížit elektronický šum na minimální hodnotu, jinak bude docházet ke špatné klasifikaci tajného klíče. Výsledkem měření by byl proudový průběh zařazen v chybné skupině, porovnání obrázku obr. 3.4 a obr. 3.5.

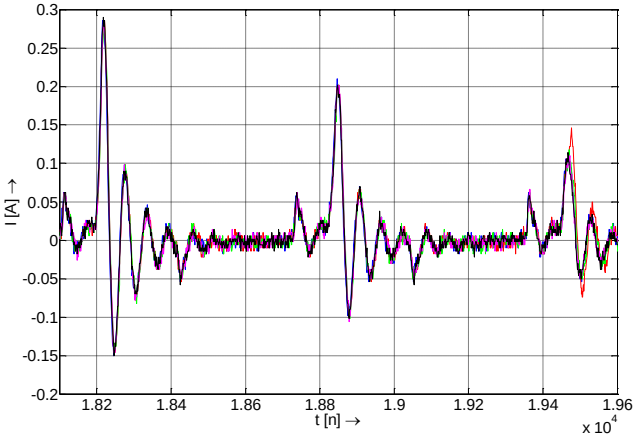
K určení elektronického šumu byla naměřena opakovaně proudová spotřeba kryptografického modulu zpracovávajícího stále stejná data. Kryptografický modul na experimentálním pracovišti zpracovával 200 krát datovou hodnotu 170, kterou ukládal do registru. Obr. 3.5 zobrazuje prvních 5 proudových průběhů operace. Průběhy jsou si velice podobné, protože jsou stále zpracovávány stejné instrukce a data. Rozdíly mezi průběhy způsobuje elektronický šum. S cílem získat lepší představu o rozložení bodů proudové spotřeby bude následující analýza zaměřena pouze na jeden bod z proudové spotřeby.



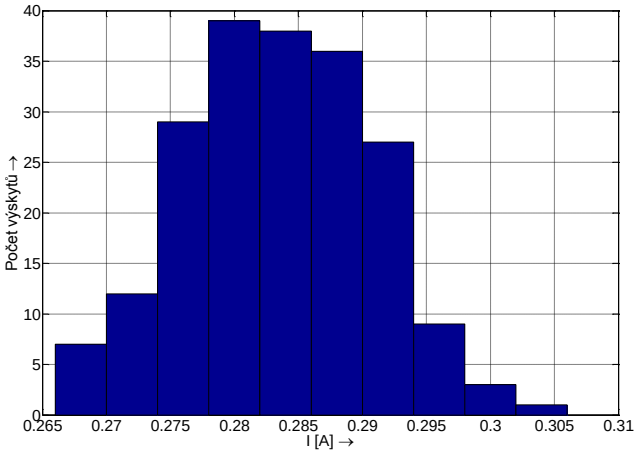

Obr. 3.3: Proudové vzory spotřeby pro všechny hodnoty klíče.




Obr. 3.4: Detail proudové spotřeby pro všechny hodnoty klíče.




Obr. 3.5: Prvních 5 proudových průběhů operace ukládání dat do registru.




Obr. 3.6: Histogram pro zvolený bod proudové spotřeby.

Vezmeme v potaz například bod $n = 18219$ odpovídající proudové špičce. Obr. 3.6 zobrazuje vypočítaný histogram pro daný bod, který zobrazuje jak často byly jednotlivé hodnoty proudu naměřeny. Pokud bude zobrazen histogram pro jakýkoli jiný bod proudové spotřeby, tvar histogramu bude vždy obdobný. Tvary histogramů indikují, že body naměřených průběhů se řídí normálním rozdělením. Normální rozdělení pravděpodobnosti s parametry $\mu$ a $\sigma$, pro $-\infty < \mu < \infty$ a $\sigma > 0$, je pro $-\infty < x < \infty$ definováno hustotou pravděpodobnosti ve tvaru Gaussovy funkce:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} \mathrm{e}^{-\frac{(x-\mu)^2}{2\sigma^2}}, \tag{3.3}$$

parametry $\mu$ a $\sigma$ jsou nazývány střední hodnota a směrodatná odchylka. Mocninou směrodatné odchylky je rozptyl:

$$\begin{aligned} \mathrm{E}(X) &= \mu, \\ \mathrm{D}(X) &= \sigma^2. \end{aligned} \tag{3.4}$$

Normální rozdělení se většinou značí $\mathrm{N}(\mu, \sigma)$. V našem experimentu, proměnná $X$ definuje proudovou spotřebu definovanou zvoleným bodem. V normálním rozdělení je střední hodnota nejpravděpodobnější výsledek měření, tzn. je to výsledek vyskytující se nejčastěji. Navíc z definice normálního rozdělení plyne, že většina výsledků experimentu se pohybuje blízko střední hodnoty, a proto můžeme určit $\mu = \mathrm{E}(X)$ jako průměr hodnoty $\bar{x}$. V uvedeném příkladu vychází průměrná hodnota $\bar{x} = 55,3\mathrm{mA}$, což odpovídá středu histogramu. Lze také vypočítat směrodatnou odchylku $\sigma = 7,5\mathrm{mA}$. Důležitou vlastností je, že $68,3\%$ hodnot se pohybuje v mezích směrodatné odchylky ($\pm\sigma$) a $95,5\%$ všech hodnot se pohybuje v rozmezí dvou směrodatných odchylek ($\pm 2\sigma$).

V provedeném experimentu byly zpracovávána vždy stejná data a stejné instrukce, proto se dá předpokládat, že rozptyl výkonové spotřeby závislé na datech je nulový. Za tohoto předpokladu platí, že elektronický šum je rozložen dle normálního rozdělení s parametry $\mu = 0\text{mA}$ a $\sigma = 7,5\text{mA}$. V praxi se elektronický šum řídí u většiny kryptografických zařízení dle normálního rozdělení se specifickou směrodatnou odchylkou pro každé zařízení. Dle výše popsaných poznatků chování elektronického šumu a také odborné literatury např. [24] je nejlepším způsobem snížení elektronického šumu opakované měření proudových spotřeb a následné vypočtení průměrné hodnoty. Proto byly proudové spotřeby pro různé hodnoty dat měřeny vícekrát a následně byl vypočítán průměrný průběh proudové spotřeby, s kterým se bude následně pracovat. Experimentálně bylo ověřeno, že optimální hodnota průměrování proudových průběhů je 16. Průběhy proudové spotřeby jsou funkcí s diskrétním časem, označme proudové průběhy odpovídající jednotlivým bajtům klíče $k_i[n] = f[n]$ pro $[n] = \{0, \ldots, t\}$ a každé měření je opakováno $s$-krát, kde $s = 16$. Potom průměrná spotřeba, která je použita jako vzorová data je definována:

$$\bar{k_i}[n] = \frac{1}{s} \sum_{j=0}^{s} k_i^j[n]. \tag{3.5}$$

U průběhů proudové spotřeby zobrazených na obr.3.3 a obr.3.4 je použito průměrování dle vztahu 3.5.

**Fáze vytvoření a trénování neuronové sítě**

Naměřené průběhy byly importovány a uloženy do matice $\mathbf{K_{vzor}}$ v programu MATLAB pro následné zpracování. Pro vytvoření neuronové sítě, jak již bylo řečeno, byl zvolen NETLAB Toolbox. Tato kapitola popisuje základní vlastnosti a implementaci neuronové sítě. Vytvořená neuronová síť v prostředí MATLAB je typická třívrstvá, jak popisuje kapitola 2.4. Struktura sítě je zobrazena na obr. 3.2. Metoda učení byla zvolen algoritmus využívající zpětné šíření chyby (Backpropagation), která patří k nejpoužívanějším principům učení neuronových sítí. Tato metoda je popsána následujícími kroky.

- **Krok 1:** Počáteční inicializace vah $w_{ij}$ a prahů $\theta_i$ jednotlivých neuronů.
- **Krok 2:** Přivedení vstupního vektoru $\mathbf{X} = [x_1, \ldots, x_N]^T$ a definice požadované výstupní odezvy $\mathbf{D} = [d_1, \ldots, d_M]^T$.
- **Krok 3:** Výpočet aktuálního výstupu podle následujících vztahů:

$$y_l(t) = f_s(\sum_{k=1}^{N_2} w_{kl}^{''}(t) x_k^{''}(t) - \theta_l^{''}),\ 1 \le l \le M,\ \text{výstupní vrstva}, \tag{3.6}$$

$$x_k^{''}(t) = f_s(\sum_{j=1}^{N_1} w_{jk}^{'}(t) x_j^{'}(t) - \theta_k^{'}),\ 1 \le k \le N_2,\ \text{skrytá vrstva}, \tag{3.7}$$

$$x_j^{'}(t) = f_s(\sum_{i=1}^{N} w_{ij}(t) x_i(t) - \theta_j),\ 1 \le j \le N_1,\ \text{vstupní vrstva}. \tag{3.8}$$

  Výpočet platí pro třívrstvou neuronovou síť uvedenou na obr. 3.2.
- **Krok 4:** Adaptace vah a prahů dle následujících vtahů:

$$w_{ij}(t+1) = w_{ij}(t) + \eta \delta_j x_i,\ \text{popř.} \tag{3.9}$$

$$w_{ij}(t+1) = w_{ij}(t) + \eta \delta_j x_i + \alpha(w_{ij}(t) - w_{ij}(t-1)). \tag{3.10}$$

  Nastavení vah začíná u výstupních neuronů a postupuje rekurzivně směrem ke vstupním neuronům. V uvedených vztazích jsou $w_{ij}$ váhy mezi $i$-tým skrytým neuronem popřípadě vstupním a uzlem $j$-tým v čase $t$. Výstup $i$-tého neuronu je označen $x_i^{'}$, $\eta$ je koeficient učení, $\alpha$ je tzv. momentový koeficient a $\delta_j$ je chyba, pro kterou platí následující vztahy:

$$\delta_j = y_j(1 - y_j)(d_j - y_j),\ \text{pro výstupní neurony}, \tag{3.11}$$

$$\delta_j = x_j^{'}(1 - x_j^{'})(\sum \delta_k w_{jk}),\ \text{pro skryté neurony}, \tag{3.12}$$

  kde $k$ se mění přes všechny neurony vrstvy, které následují za uzlem $j$.

- **Krok 5:** Opakování kroků 3 až 5, dokud chyba není menší než předem stanovená hodnota.

V následujících kapitolách při použití neuronové sítě bude brána v úvahu právě popsaná třívrstvá neuronová síť s metodou učení založeném na zpětném šíření chyby.

Vytvořená neuronová síť v prostředí MATLAB má tyto parametry: vstupní vrstva obsahuje stejný počet neuronů jako je počet vzorků v průběhu, tedy 3000. Výstupní vrstva klasifikuje vstup na jednotlivé klíče, tedy musí obsahovat 256 neuronů pro všechny kombinace klíče 0 až 255. Skrytá vrstva může mít libovolný počet neuronů v závislosti na složitosti řešeného problému. V implementaci je počet možno konfigurovat od 128 do 256 neuronů. S těmito počty bylo provedeno testování a dosahovalo se nejlepších výsledků. Typ aktivační funkce byl zvolen `logistic`, což odpovídá standardní sigmoidě. Následující text obsahuje nejdůležitější část programu implementace neuronové sítě. Uvedené řádky odpovídají postupně vytvoření, konfiguraci a následné trénování neuronové sítě.

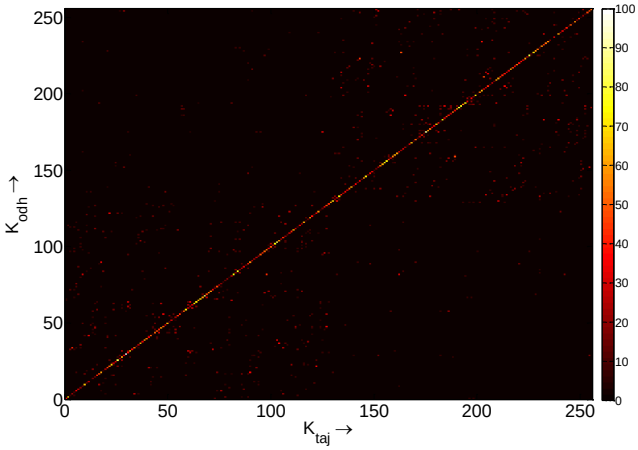
```
%Vytváření neuronové sítě
nn = mlp(pocet_vzorku, pocet_neuronu, pocet_mereni,'logistic');
%Nastavení parametrů neuronové sítě
options = zeros(1,18);              % Reset konfiguračního pole
options(1) = vypis;                 % Výpis chyby během učení
options(14) = pocet_iteraci;        % Počet trénovacích cyklů
%Trénování neuronové sítě
[nn, options] = netopt(nn, options, K_vzor, clas, 'scg');
```

Vzorová data uložená v $\mathbf{K_{vzor}}$ obsahují 256 průběhů a každý z nich má 3000 vzorků. Pro tyto průběhy je nutné vytvořit klasifikační matici, která určí správnou klasifikaci daného vstupu na příslušný klíč. Tato matice má rozměry $256 \times 256$ a jednotlivé řádky odpovídají naměřeným průběhům a příslušné sloupce přiřazují výsledný klíč hodnotou 1. Výsledkem je jednotková klasifikační matice, která jednotlivým průběhům pro klíče 0 až 255 přiřadí klíče 0 až 255. Po úspěšném natrénování neuronové sítě následuje fáze útoku.

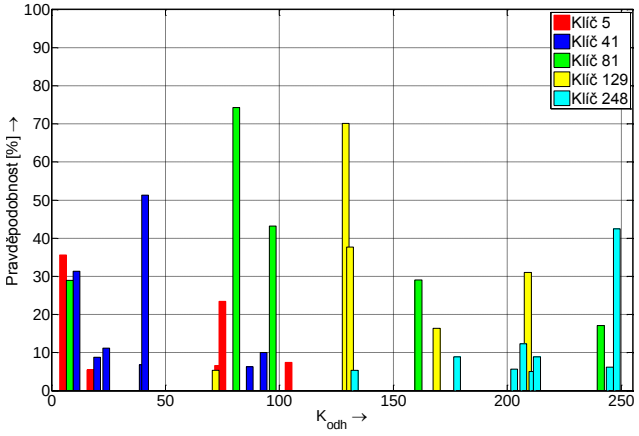
### Fáze útoku

Po úspěšném naučení je neuronová síť připravena k rozpoznávání dat. V reálném útoku by útočník naměřil proudové spotřeby kryptografického modulu odpovídající tajnému klíči a pokusil se izolovat operaci `AddRoundKey`. Tato část je považována za kritickou a je důležité, aby data sloužící k útoku byla stejně synchronizována jako data vzorová. Ideální metodou je vložení identického synchronizačního signálu jako při měření vzorových dat. Pokud tuto možnost útočník nemá nezbývá, než naměřit celý průběh proudové spotřeby kryptografického algoritmu, na který je prováděn útok a následnou postupnou analýzu průběhu určit jednotlivé fáze algoritmu a synchronizovat operaci `AddRoundKey` na například pomocí první proudovou špičky. (práce s prvním bajtem tajného klíče). Důležitým faktorem je také stejná implementace kryptografického algoritmu, pokud by byl algoritmus implementován odlišným způsobem (jiné instrukce, jiná posloupnost instrukcí), výsledky klasifikace by byly chybné. Důležitým faktorem je také dodržení stejného postupu snížení elektronického šumu, tedy průměrování naměřených průběhů dle vztahu 3.5. Po korektním naměření proudové spotřeby kryptografického modulu je provedena klasifikace neuronovou sítí a je určen první bajt tajného klíče jako odhad klíče s největší pravděpodobností.

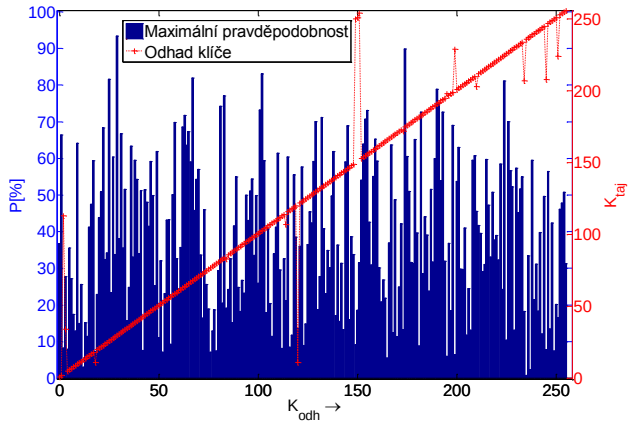
Pro ověření metody byly naměřeny a uloženy do matice **test** proudové průběhy odpovídající všem hodnotám tajného klíče $k_1$. Tato matice byla postupně klasifikována řádek po řádku neuronovou sítí. Tímto způsobem se získaly výsledky pro všechny hodnoty tajného klíče $k_1$ a představa do jaké míry je metoda úspěšná. Následující část zdrojového kódu zobrazuje klasifikaci proudových průběhů neuronovou sítí.



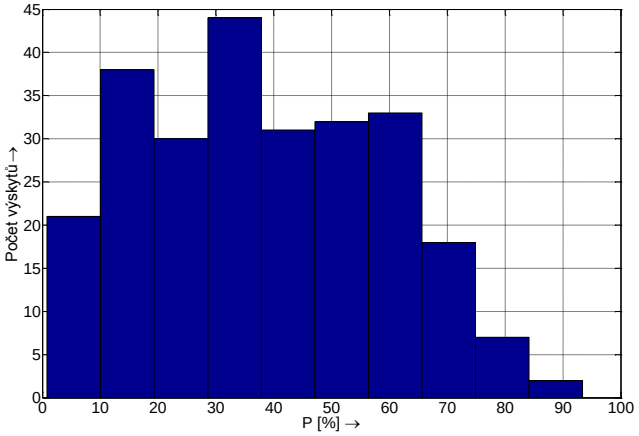

Obr. 3.7: Grafické znázornění kompletních výsledků klasifikace $\mathbf{V_{cel}}$.




Obr. 3.8: Výsledky klasifikace pro 5 náhodně vybraných klíčů.




Obr. 3.9: Maximální hodnoty pravděpodobnosti a určené odhady klíče.




Obr. 3.10: Histogram maximálních hodnot pravděpodobností.

```
load neuronova_sit;          %nacteni neuronove site
test = test(:,3000:6000-1); %matice proudových prubehu
V_cel = [];
for i=1:256                  %cyklus klasifikujici jednotlive prubehy
V_cel = [V_cel; mlpfwd(nn,test(i,:))];
end
```

Výsledkem analýzy pro všechny proudové průběhy korespondující se všemi hodnotami tajného klíče byla matice $\mathbf{V_{cel}}$ o rozměrech $255 \times 255$. Hodnota indexu řádku odpovídala hodnotě tajného klíče, pro který byla měřena proudová spotřeba a index sloupce představoval odhad klíče přiřazeného neuronovou sítí. Neuronová síť přiřadila každému průběhu proudové spotřeby vektor obsahují pravděpodobnosti pro jednotlivé odhady klíče (řádek matice $\mathbf{V_{cel}}$). Celkové výsledky klasifikace jsou graficky znázorněny na obr. 3.7 a pro lepší představu je část výsledné matice číselně zapsána do tab. 3.1. Z tabulky je patrno, že neuronová síť klasifikovala například proudovou spotřebu pro tajný klíč s hodnotou 0 s pravděpodobností $36,77\%$ pro odhad klíče 0 a pro proudový průběh odpovídající hodnotě tajného klíče 1 klasifikovala odhad klíče 1 s pravděpodobností $66,42\%$.

Pro získaní lepší představy o výsledcích klasifikace neuronové sítě a rozložení pravděpodobnosti odhadů klíčů jsou na obr. 3.8 zobrazeny výsledky klasifikace pro 5 náhodně vybraných proudových průběhů korespondující s pěti hodnotami tajných klíčů. Na ose `x` jsou zobrazeny odhady klíče, tzn. výstup neuronové sítě a osa `y` udává s jakou pravděpodobností se odhad klíče rovná tajnému. Barevně jsou vyznačeny jednotlivé průběhy odpovídající tajnému klíči, tedy byly vybrány proudové průběhy pro hodnoty tajného klíče 5, 41, 81, 129 a 248 (dekadický zápis). Z obr.3.8 je patrno, že pravděpodobnost odhadu klíče 5 pro proudový průběh

Tab. 3.1: Výsledky analýzy - část matice $\mathbf{V_{cel}}$.

| | | Pravděpodobnost odhadu klíče $K_{odh}$ | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| Hodnota tajného klíče $K_{taj}$ | ⋮ | ... | ... | ... | ... | ... | ... | ... |
| | 6 | 0,00% | 0,00% | 0,00% | 0,00% | 0,03% | 0,00% | 27,21% |
| | 5 | 0,00% | 0,00% | 0,08% | 0,00% | 0,00% | 35,61% | 0,00% |
| | 4 | 0,00% | 0,00% | 0,00% | 0,00% | 7,91% | 0,00% | 0,00% |
| | 3 | 0,00% | 0,00% | 0,00% | 23,79% | 0,00% | 0,00% | 0,00% |
| | 2 | 0,00% | 0,00% | 6,44% | 0,00% | 6,98% | 0,00% | 0,00% |
| | 1 | 0,00% | 66,42% | 0,00% | 0,00% | 0,00% | 0,00% | 0,00% |
| | 0 | 36,77% | 0,00% | 0,00% | 0,00% | 0,00% | 0,00% | 1,37% |

s hodnotu tajného klíče 5 byla 35% a ostatní pravděpodobnosti určené neuronovou sítí byly: 5% pro odhad klíče 18, 6% pro odhad klíče 74, 23% pro odhad klíče 76 a 7% pro odhad klíče 105. Analogicky lze vyčíst rozložení pravděpodobností pro ostatní vybrané hodnoty tajného klíče. Zobrazené hodnoty korespondují s maticí výsledků $\mathbf{V_{cel}}$ a tab. 3.1. Pro náhodně vybrané hodnoty tajného klíče největší pravděpodobnost odhadu klíče odpovídala vždy hodnotě tajného klíče. Z těchto dílčích výsledků plyne dobrá funkčnost metody.

Pro podrobnější analýzu funkčnosti metody zobrazuje obr. 3.9 **maximální hodnoty pravděpodobností** odhadu klíče pro jednotlivé hodnoty tajného klíče. Graf ukazuje jaký odhad klíče byl klasifikován neuronovou sítí s největší pravděpodobností pro konkrétní proudový průběh korespondující s hodnotou tajného klíče. Graf je zobrazen se dvěma osami `y` a to pro lepší přehlednost a názornost. Osa `x` představuje odhady klíčů a modrá osa `y` příslušné maximální pravděpodobnosti. Červená osa `y` koresponduje s hodnotou tajného klíče.

Z požadavků metody je zřejmé, aby odhad klíče byl roven tajnému klíči, tedy v ideálním případě platí funkce $K_{odh} = K_{taj}$. Průběh funkce $K_{odh} = K_{taj}$ je markantní na první pohled. Hladký průběh funkce ruší body, které indikují chyby klasifikace. Jedná se o odhady klíče, které byly chybně klasifikovány, tedy kdy vybraný odhad klíče s největší pravděpodobností nekorespondoval s hodnotou tajného klíče v kryptografickém modulu ($K_{odh} \neq K_{taj}$). Seznam všech chybně klasifikovaných tajných klíčů je zapsán do tab. 3.2. Z naměřeného souboru, který byl určen pro ověření metody, neuronová síť přiřadila šestnáctkrát špatný odhad klíče. Ze všech možných testovaných variant tajného klíče 256 to odpovídá $6,27\%$ chybných klasifikací. Navržená metoda určila správnou hodnotu tajného klíče v **93,72%** případů.

Tab. 3.2: Chybně určené odhady klíčů.

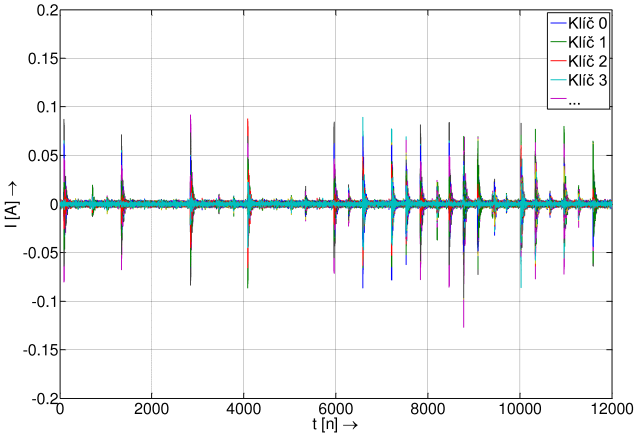
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $K_{taj}$ | 2 | 3 | 18 | 84 | 114 | 120 | 149 | 150 |
| $K_{odh}$ | 112 | 33 | 10 | 82 | 106 | 10 | 249 | 250 |
| P[%] | 8,32 | 27,77 | 7,31 | 19,15 | 21,23 | 13,60 | 9,20 | 18,59 |
| $K_{taj}$ | 151 | 173 | 195 | 199 | 210 | 234 | 245 | 251 |
| $K_{odh}$ | 253 | 171 | 197 | 228 | 202 | 206 | 207 | 223 |
| P[%] | 31,57 | 13,23 | 6,02 | 6,44 | 45,59 | 18,27 | 7,82 | 16,60 |

Při opětovném experimentálním testování metody se dosahovalo obdobných výsledků, kdy metoda dosahoval okolo 85 až 90% úspěšnosti správné klasifikace s chybami, které se vyskytovaly u odhadů klíčů u nichž je maximální hodnota pravděpodobnosti nízká. Tento poznatek potvrzují data v tab. 3.2, medián pravděpodobností, které vedly ke špatné klasifikaci je zde 15% a průměrná hodnota 17%. Při klasifikaci je tedy požadavek na co největší pravděpodobnost u správného odhadu klíče. Z obr. 3.9, který zobrazuje maximální hodnoty pravděpodobností je patrné, že maximální pravděpodobnosti 14%, 18% a 20% nejsou vyjímkou. Proto bylo přistoupeno k další analýze výsledků a obr. 3.10 zobrazuje histogram všech maximálních pravdě-

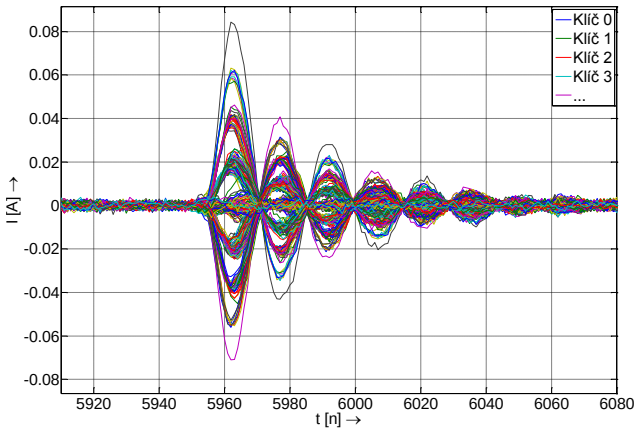
podobností klasifikace. Z histogramu lze vyčíst, že pravděpodobnosti do 10% se vyskytují dvacetjednakrát a pravděpodobnosti 10% až 20% se vyskytují třicetosmkrát, což součtu odpovídá 23%. Pravděpodobnosti 20% až 60% se vyskytují nejčastěji a to stosedmdesátkrát, což odpovídá 66% z cekového počtu. Maximální pravděpodobnosti 70% až 90% se vyskytují jen 27 krát, což z celkového počtu klíčů odpovídá deseti procentům. Celkový počet potencionálně náchylných klíčů k chybné klasifikaci je asi 23%, což by znamenalo, že navržená metoda by pracovala asi s **80%** úspěšností. Z výše popsané analýzy výsledků klasifikace navržené metody byla navržena optimalizace, která umožní snížení chybné klasifikace a to tím, že se pokusí zvýšit maximální pravděpodobnost klasifikace a snížit pravděpodobnost chybné klasifikace.

### Optimalizace navržené metody

Cílem optimalizace je získat trénovací vzory proudové spotřeby pro všechny varianty tajného klíče $k_i$ s většími diferencemi pro jednotlivé průběhy. Zvýšení diference mezi jednotlivými průběhy umožní přesnější klasifikaci. Z obr. 3.3 je patrné, že proudové průběhy jsou si velmi podobné a liší se v místech práce s registry. Pro zvýšení diference mezi průběhy byla použita metoda, která byla implementována k zvýraznění proudových průběhu jednotlivých instrukcí mikroprocesoru. Metoda byla navržena a testována v pojednání o disertační práci, ale jen pro několik průběhů tří instrukcí mikroprocesoru, konkrétně se jednalo o instrukci `XOR`, `SWAP` a `AND`. Následně probíhalo i testování této metody s neuronovými sítěmi [5], které podnítilo návrh optimalizace.




Obr. 3.11: Průběh proudové spotřeby `AddRoundKey` pro všechny hodnoty klíče.




Obr. 3.12: Průběh proudové spotřeby `AddRoundKey` pro všechny hodnoty klíče.

Samotné zvýšení diferencí je docíleno předzpracováním naměřených dat. Naměřené průběhy proudové spotřeby ve fázi přípravy vzorů jsou zpracovány následujícím způsobem. Nejprve je vypočten průměrný průběh proudové spotřeby pro všechny hodnoty tajného klíče. Průběhy proudové spotřeby jsou funkcí s diskrétním časem, označme proudové průběhy odpovídající jednotlivým bajtům klíče $k_i[n] = f[n]$ pro $[n] = \{0, \ldots, t\}$ a každý bajt může nabývat hodnotu 0 až 255, tedy 256 průběhů pro první bajt. Průběh průměrné proudové spotřeby je definován:

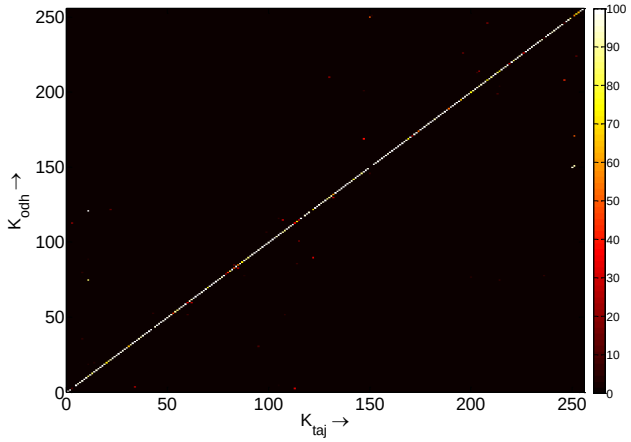
$$\bar{K_i}[n] = \frac{1}{256} \sum_{j=0}^{256} k_i^j[n]. \tag{3.13}$$

Následně jsou vypočítány učící vzory jako rozdíly $\bar{K_i}$ a proudových spotřeb pro jednotlivé tajné klíče. Ve skutečnosti jsou brány opět průměry proudových spotřeb a to kvůli snížení elektronického šumu. Celkový výpočet vzorů tedy můžeme vyjádřit:

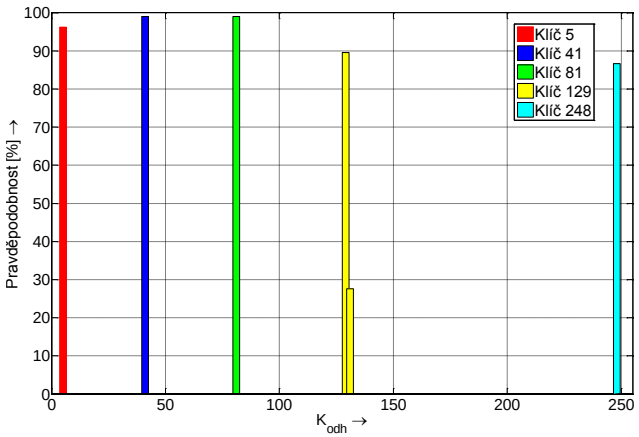
$$V_I = \bar{P} - \frac{1}{s} \sum_{l=0}^{s} k_i^l[n] = \frac{1}{256} \sum_{j=0}^{256} k_i^j[n] - \frac{1}{s} \sum_{l=0}^{s} k_i^l[n], \tag{3.14}$$

kde $s$ je počet měření jednotlivých proudových průběhů (16). Tímto výpočtem se docílí požadované zvětšení diference mezi jednotlivými proudovými průběhy. Obr. 3.11 zobrazuje kompletní sadu naměřených a následně početně upravených proudových průběhů. Z porovnání průběhů 3.3 a 3.11 je zřejmé, že jsou zobrazeny jen

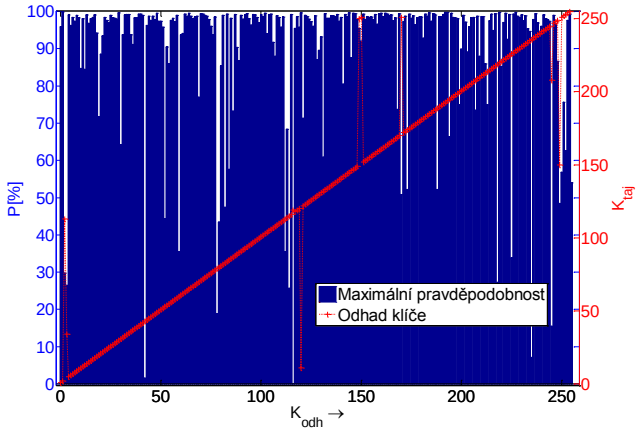
diference mezi jednotlivými průběhy. Stejně tak, jak v předchozím případě, je zobrazen detail proudové špičky na obr. 3.12. Dle předpokladu jsou proudové průběhy rozděleny do skupin a to i v záporných hodnotách. Vytvoření neuronové sítě a učení probíhalo stejným způsobem jak v předchozí kapitole. Pro ověření metody byly opět použity naměřené proudové průběhy odpovídající všem hodnotám tajného klíče a následně byly tyto průběhy analyzovány neuronovou sítí. Z důvodu porovnání metod byla použita stejná sada měření jak v předchozí kapitole. Tímto způsobem se získaly opět výsledky pro všechny možné hodnoty klíče a představa do jaké míry je metoda úspěšná.



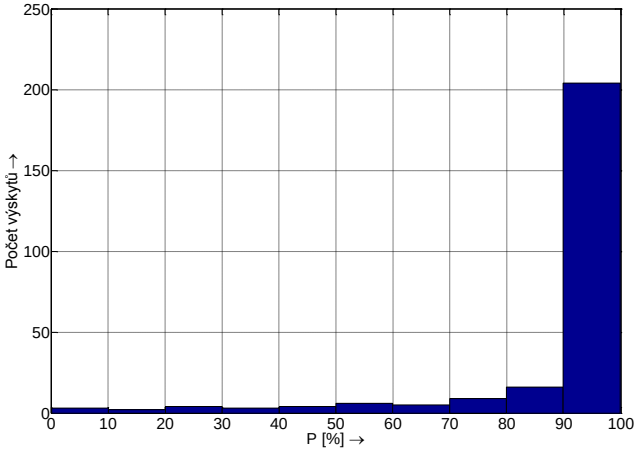

Obr. 3.13: Grafické znázornění kompletních výsledků klasifikace $\mathbf{VD_{cel}}$.




Obr. 3.14: Výsledky klasifikace pro 5 náhodně vybraných klíčů.




Obr. 3.15: Maximální hodnoty pravděpodobnosti a určené odhady klíče.




Obr. 3.16: Histogram maximálních hodnot pravděpodobností po optimalizaci.

Výsledkem analýzy pro všechny hodnoty klíče byla matice $\mathbf{VD_{cel}}$ o rozměrech $256 \times 256$. Hodnota indexu řádku odpovídala hodnotě tajného klíče, pro který byla měřena proudová spotřeba a index sloupce představoval odhad klíče přiřazeného neuronovou sítí. Část výsledné matice je zobrazena v tab. 3.3 a celá matice je graficky zobrazena na obr.u 3.13. Z tabulky je patrno, že neuronová síť klasifikovala proudovou spotřebu pro tajný klíč s hodnotou 0 s pravděpodobností $96,00\%$ pro odhad klíče 0 a pro proudový průběh odpovídající hodnotě tajného klíče 1 klasifikovala odhad klíče 1 s pravděpodobností $99,87\%$. Z porovnání části výsledků pro obě metody zobrazených v tab. 3.1 a 3.3 je patrné navýšení pravděpodobnosti pro správné odhady klíče. Například pro správné odhady klíče 0 a 1 byla pravděpodobnost navýšena z $36,77\%$ a $66,42\%$ na hodnoty $96,00\%$ a $99,87\%$. Z porovnání obrázku obr. 3.7 a 3.13 je také patrno na první pohled markantní zlepšení výsledků klasifikace a funkce $K_{odh} = K_{taj}$ je tvořena hodnotami pravděpodobnosti mezi 90% a 100%. Z obrázků je také patrné snížení alternativních variant klasifikace, tedy absence rovnoběžných úseček s funkcí $K_{odh} = K_{taj}$, které jsou jasně patrné na obr. 3.7. Z těchto dílčích výsledků je patrné zlepšení klasifikace, ale je nezbytné zhodnotit všechny výsledky a všechny pravděpodobnosti matice $\mathbf{VD_{cel}}$, jestli nedošlo ke zvýšení pravděpodobností u nesprávných odhadů.

Pro ověření o změnách ve výsledcích klasifikace neuronové sítě je zobrazen obr. 3.14, který udává výsledky klasifikace pro stejně vybraných pět proudových spotřeb kryptografického modulu korespondující s pěti hodnotami tajného klíče jako v předchozí kapitole. Na ose `x` jsou zobrazeny odhady klíče, tzn. výstup neuronové sítě a osa `y` koresponduje s jakou pravděpodobností se odhad klíče rovná tajnému. Barevně jsou zobrazeny jednotlivé průběhy odpovídající tajnému klíči. Z porovnání obrázků 3.14 a 3.8 je na první pohled zřejmé, že došlo ke zlepšení klasifikace. Například pro tajný klíč 5 byl správný odhad tajného klíče upraven z 35% na 96% a ostatní varianty tajného klíče byly zcela potlačeny. Tato žádaná vlastnost, tedy potlačení potencionálních možných variant klíče se potvrdila i u ostatních 3 tajných klíčů. U tajného klíče 129 byly alternativní varianty kromě jedné také potlačeny, ale byla také zvýšena maximální pravděpodobnost z 70% na 90%.

Tab. 3.3: Výsledky analýzy - část matice $\mathbf{VD_{cel}}$.

| | | Pravděpodobnost odhadu klíče $K_{odh}$ | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| Hodnota tajného klíče $K_{taj}$ | ⋮ | ... | ... | ... | ... | ... | ... | ... |
| | 6 | 0,00% | 0,00% | 0,00% | 0,00% | 0,00% | 0,00% | 98,39% |
| | 5 | 0,00% | 0,00% | 0,00% | 0,00% | 0,00% | 96,24% | 0,00% |
| | 4 | 0,00% | 0,00% | 0,00% | 0,00% | 99,09% | 0,00% | 0,00% |
| | 3 | 0,00% | 0,00% | 0,00% | 0,00% | 0,00% | 0,00% | 0,00% |
| | 2 | 0,00% | 0,00% | 9,28% | 0,00% | 0,00% | 0,00% | 0,00% |
| | 1 | 0,00% | 99,87% | 0,00% | 0,00% | 0,00% | 0,00% | 0,00% |
| | 0 | 96,00% | 0,00% | 0,00% | 0,00% | 0,00% | 0,00% | 0,00% |

Obr. 3.15 ukazuje maximální hodnoty pravděpodobností odhadů klíče pro jednotlivé hodnoty tajného klíče pro optimalizovanou metodu. Graf je zobrazen se dvěma osami stejně jako při první implementaci metody (viz graf na obr. 3.9). Z porovnání výsledků pro obě metody (obr. 3.9 a obr. 3.15) je na první pohled patrné požadované zvýšení maximální pravděpodobnosti u všech odhadů klíčů. Průběh funkce $K_{odh} = K_{taj}$ je takřka hladký a obsahuje jen devět chybně klasifikovaných klíčů, tzn. snížení počtu chyb z 16 na 9, to odpovídá zlepšení o 43%. Z těchto výsledků se jasně prokázala funkčnost a vhodnost předzpracování naměřených proudových průběhů pro klasifikaci neuronovou sítí. Navržená a optimalizovaná metoda klasifikovala devět odhadů klíčů chybně, všechny hodnoty jsou uvedeny v následující tab. 3.4.

Tab. 3.4: Chybně určené odhady klíčů.

| $K_{taj}$ | 2 | 3 | 116 | 120 | 149 | 150 | 170 | 247 | 249 |
|---|---|---|---|---|---|---|---|---|---|
| $K_{odh}$ | 112 | 33 | 118 | 10 | 249 | 250 | 250 | 207 | 149 |
| P[%] | 29,75 | 26,51 | 0,11 | 99,62 | 95,43 | 92,12 | 50,84 | 15,47 | 48,48 |

Z výsledku klasifikace se potvrdilo, že chyby se vyskytly opět u odhadů klíčů, které byly klasifikovány s nižší pravděpodobností. Uvedená metoda způsobila i zvýšení pravděpodobnosti u chybně klasifikovaných klíčů a to na průměrnou hodnotu 50%. Z celého souboru naměřených proudových průběhů neuronová síť klasifikovala devět odhadů chybně. Ze všech možných testovaných variant tajného klíče to odpovídá $3,5\%$ chybných klasifikací. Navržená metoda určila hodnotu tajného klíče v **96,5%** případů. Při opětovném testování dosahovala optimalizovaná metoda obdobných výsledků klasifikace a to **95 - 98%**.

Pro detailnější analýzu maximálních pravděpodobností obr. 3.16 zobrazuje histogram všech maximálních pravděpodobností klasifikace optimalizované metody. Z histogramu lze vyčíst, že pravděpodobnosti od 10% do 70% se vyskytují každá jen pět krát. Pravděpodobnosti 70% až 80% se vyskytují desetkrát a patnáctkrát a největší zastoupení ve vybraných maximálních pravděpodobnostech mají pravděpodobnosti 90% až 100%, které se vyskytují dvěstěpětkrát. Průběh histogramu opět potvrzuje zvýšení maximálních pravděpodobností, tedy zvýšení počtu výskytů pravděpodobností nad 90%. Z celkového počtu 256 testovaných klíčů to odpovídá

80% kíčů klasifikovaných s pravděpodobností nad 90%. Celkový počet potencionálně náchylných klíčů k chybné klasifikaci je snížen po optimalizaci z cca 20% na 5%.

### Opakovatelnost měření a zhodnocení metody

Pro analýzu opakovatelnosti a realizovatelnosti metody byl naměřen větší soubor proudových spotřeb kryptografického modulu a metoda byla otestována. Cílem bylo ověřit zda i pro opakované měření proudových spotřeb dojde ke správné klasifikaci tajného klíče. Bylo naměřeno 2560 průběhů proudové spotřeby, odpovídající všem hodnotám tajného klíče a tyto průběhy nebyly měřeny postupně, ale náhodně v jiné dny (z důvodu eliminace vlivu metody měření). Pro každou hodnotu tajného klíče bylo nezávisle uloženo 10 průběhů a následně byly tyto průběhy klasifikovány neuronovou sítí. Tímto způsobem se získaly výsledky pro všechny možné hodnoty klíče opakovaně z nezávislých měření a představa do jaké míry je metoda úspěšná i pro opakované měření a klasifikaci. Výsledky klasifikace tohoto objemu dat shrnuje následující tab. 3.5.

Tab. 3.5: Výsledky klasifikace pro 2560 proudových průběhů.

| Použitá metoda klasifikace | Počet chybných klasifikací z celkového počtu 2560 | Úspěšnost [%] |
|---|---|---|
| bez optimalizace | 378 | **85,23** |
| s optimalizací | 139 | **94,57** |

Výsledky potvrdily, že opakované měření nemá na výsledky klasifikace vliv a je tedy možné metodu použít. Výsledky potvrdily získané dílčí výsledky z předchozích analýz, které byly provedeny se souborem 256 proudových spotřeb. Neoptimalizovaná metoda dosáhla 85% úspěšné klasifikace a optimalizovaná metoda klasifikovala tajné klíče s 95% úspěšností i z obsáhlého souboru naměřených dat. Pro doplnění výsledků klasifikace je uvedena tab. 3.6, která udává výsledky klasifikace pro sedm vybraných klíčů. Prvních pět vybraných klíčů (5, 41, 81, 129 a 248) koresponduje s klíči vybranými v předchozích kapitolách a určené maximální pravděpodobnosti jsou takřka totožné. Jako příklad chybné klasifikace jsou zobrazeny klíče 19 a 20, kde se vyskytovaly řádově nižší pravděpodobnosti a byly zde větší rozdíly v hodnotách pravděpodobností. Neuronová síť klasifikovala z těchto 20 průběhů 12 chybně a po optimalizaci 8. Opět se potvrdila funkčnost zvýšení diference mezi jednotlivými proudovými průběhy.

Při porovnání metody využívající neuronové sítě s používanými metodami DPA a SPA je hlavní výhoda v tom, že i pro algoritmus odolný proti konvenční analýze je metoda schopna určit první bajt tajného klíče s pravděpodobností kolem **96% pomocí jednoho průběhu proudové spotřeby.** DPA útoky potřebují k realizaci několik stovek nebo tisíc měření proudových spotřeb. Tento typ útoku proudovým postranním kanálem, který je zaměřen na určení hodnoty tajného klíče nebyl dosud publikován, jedná se tedy o zcela novou myšlenku. Podobná myšlenka byla publikována, ale byla zaměřena jen na rozpoznávání jednotlivých otisků proudových spotřeb jednotlivých instrukcí mikroprocesoru [5] a [19]. Metoda využívá snížení elektronického šumu v naměřeném proudovém průběhu a zvyšuje diferenci mezi proudovými průběhy pomocí předzpracování naměřených průběhů. Navržená metoda může pracovat co nejrychleji a útočník může provést útok i na modul, který se mu podařilo získat jen na krátký čas. Dosavadní metody předpokládají plnou kontrolu nad modulem.

Nevýhodou je nutnost prvotního trénování neuronové sítě, kdy útočník musí vytvořit trénovací množinu proudových spotřeb. Počet proudových spotřeb musí odpovídat všem možným kombinacím tajného klíče, v našem případě se jednalo o první bajt AES, tzn. 256 proudových průběhů. Pro následující útoky již stačí jen jeden konkrétní proudový průběh. V reálném útoku je za kritickou část považována synchronizace naměřených proudových průběhů. Ideální metodou je vložení identického synchronizačního signálu jako při měření vzorových dat. Pokud tuto možnost útočník nemá, nezbývá než naměřit celý průběh zkoumaného algoritmu a následnou postupnou analýzu průběhu určit důležité operace a ty synchronizovat na první proudovou špičku. Důležitým faktorem je taká stejná implementace algoritmu, pokud by byl algoritmus implementován odlišnými

Tab. 3.6: Výsledky opakované klasifikace pro 7 klíčů.

| $K_{taj}$ | **5** | **41** | **81** | **129** | **248** | **19** | **20** |
|---|---|---|---|---|---|---|---|
| Bez optimalizace $P_{max}$[%] | 28,74 | 38,20 | 79,92 | 67,46 | 30,07 | 7,67 | 23,49 |
| | 27,21 | 41,48 | 79,99 | 67,68 | 39,26 | 17,27 | 13,49 |
| | 27,10 | 39,78 | 80,51 | 67,87 | 36,55 | 11,49 | 18,23 |
| | 28,96 | 42,19 | 80,15 | 69,02 | 31,05 | 9,30 | 25,07 |
| | 23,03 | 41,37 | 79,93 | 68,02 | 38,97 | 7,73 | 17,90 |
| | 28,81 | 31,34 | 77,83 | 67,94 | 37,95 | 12,63 | 25,07 |
| | 23,75 | 36,28 | 80,03 | 67,83 | 34,38 | 8,73 | 25,94 |
| | 26,95 | 37,32 | 77,32 | 66,56 | 36,04 | 13,85 | 28,05 |
| | 22,02 | 33,39 | 80,30 | 67,91 | 39,25 | 8,27 | 26,28 |
| | 28,44 | 38,25 | 80,43 | 67,99 | 34,82 | 7,81 | 13,73 |
| S optimalizací $P_{max}$[%] | 98,28 | 98,99 | 98,25 | 97,14 | 81,85 | 28,43 | 76,20 |
| | 97,99 | 98,98 | 98,40 | 98,13 | 99,42 | 98,77 | 5,61 |
| | 98,52 | 99,07 | 99,29 | 97,87 | 98,96 | 92,58 | 32,79 |
| | 98,19 | 99,04 | 99,06 | 77,21 | 87,86 | 76,18 | 73,42 |
| | 97,04 | 99,12 | 98,16 | 96,65 | 99,45 | 49,10 | 40,15 |
| | 98,48 | 98,37 | 82,53 | 96,63 | 99,25 | 95,40 | 85,24 |
| | 97,04 | 99,01 | 98,15 | 97,01 | 97,55 | 69,45 | 87,14 |
| | 98,56 | 99,00 | 61,90 | 98,90 | 98,58 | 96,86 | 92,34 |
| | 95,05 | 98,70 | 98,96 | 97,90 | 99,44 | 39,62 | 85,76 |
| | 98,74 | 98,95 | 98,92 | 98,28 | 97,22 | 51,72 | 7,44 |

instrukcemi, výsledky analýzy by byly chybné. Další pokračování v práci spočívá v ověření funkčnosti metody pro různé kryptografické moduly a pro následující bajty tajného klíče.

Přínosy a nevýhody metody lze shrnout do následujících bodů:

- Přínosy
  - klasifikace se provádí z jednoho naměřeného proudového průběhu stejně jako u SPA útoků,
  - metoda je aplikovatelná na algoritmy odolné proti SPA,
  - ne nutnost měření stovek proudových průběhů jako u DPA,
  - realizace útoku velmi rychlá v porovnání s DPA (předpoklad naučená neuronová síť),
  - implementovaná metoda určila první bajt tajného klíče algoritmu AES s pravděpodobností kolem 96%,
  - metoda je opakovatelná, tedy prakticky realizovatelná (testováno na 2560 proudových průbězích s úspěšností 95%),
  - při předzpracování proudových průběhů (optimalizace) jsou minimalizovány chybné klasifikace odpovídající podobným proudovým průběhům,
- Nevýhody
  - nevýhoda metody spočívá v přípravě trénovací množiny pro neuronovou síť,
  - pro specifický kryptografický modul (stejný typ procesoru, čipové karty atd.) je zapotřebí mít naučenou neuronovou síť,
  - za kritickou část útoku se považuje správná synchronizace naměřených proudových průběhů, toho se dá využít při implementaci protiopatření ovlivňující časovou oblast proudové spotřeby.

# 4 ZÁVĚR

Disertační práce se zabývá problematikou postranních kanálů, které umožňují útočníkovi z kryptografického modulu získat senzitivní informace netradiční cestou. Nedílnou součástí práce je také rozbor protiopatření, které tomuto útoku zabraňují. V úvodu práce je uveden souhrn dosavadních metod kryptoanalýzy postranními kanály, je provedeno jejich zhodnocení a klasifikace. V uvedené oblasti zatím neexistuje jednotná terminologie, je proto nutné jasně definovat jednotlivé typy postranních kanálů a jejich základní principy. Podrobněji je v práci rozebrán proudový postranní kanál, ze kterého posléze vychází nově navržená metoda kryptoanalýzy. Návrh a experimentální ověření nové metody je hlavním cílem disertační práce. Navrhovaná metoda využívá neuronové sítě k odhalení hodnoty šifrovacího klíče. Myšlenka využití neuronových sítí v kryptoanalýze proudovým postranním kanálem je původní, poprvé byla autorem publikována v roce 2010 [5]. Další vývoj v oblasti proudové analýzy ukázal, že neuronové sítě jsou vhodným nástrojem [30, 4].

Pro správnou funkci nově navržené metody kryptoanalýzy je stěžejní způsob snímání proudové spotřeby kryptografického modulu. Při nevhodném způsobu měření může dojít v snímání proudového odběru k odfiltrování senzitivních informací. Proto byly pro ověření teoretických znalostí navrženy a experimentálně ověřeny různé způsoby měření. Metody měření jsou popsány v kapitole 3 a byly publikovány v odborných časopisech i na tuzemských a mezinárodních konferencích [3, 11, 4, 8, 9, 2, 7].

K návrhu nové metody a jejímu testování byl vybrán algoritmus AES a to z důvodu jeho známe odolnosti proti konvenčnímu způsobu kryptoanalýzy. Implementace metody byla provedena v programovém prostředí MATLAB, získané výsledky jsou detailně popsány v kapitole 3.1. Navržená metoda určila hodnotu tajného klíče algoritmu AES v 93% případů, ale z opakovaných testů a podrobné analýzy výsledků klasifikace vyplynula teoretická funkčnost metody jen 80%, a proto byla navržená metoda dále optimalizována. Optimalizace metody byla založena na zvýšení diference mezi jednotlivými průběhy proudové spotřeby. Pro zvýšení diference bylo použito předzpracování proudových průběhů využívající rozdíl jednotlivých průběhů od vypočteného průměrného průběhu proudové spotřeby. Takto optimalizovaná metoda úspěšně klasifikovala hodnotu tajného klíče v 96% případů.

Následně byla provedena analýza opakovatelnosti a realizovatelnosti obou metod. Bylo naměřeno 2560 průběhů proudové spotřeby odpovídající všem hodnotám tajného klíče a tyto průběhy byly klasifikovány neuronovými sítěmi. Tímto způsobem byly získány výsledky klasifikace pro všechny možné hodnoty tajného klíče opakovaně z nezávislých měření. Úspěšnost klasifikace potvrdila získané dílčí výsledky z předchozích analýz, které byly provedeny se souborem 256 proudových spotřeb. Neoptimalizovaná metoda dosáhla 85% úspěšné klasifikace a optimalizovaná metoda klasifikovala tajné klíče s 95% úspěšností i z obsáhlejšího souboru proudových průběhů. Z výsledků je patrný pozitivní vliv předzpracování proudových průběhů na úspěšnost klasifikace.

Při porovnání navržené metody využívající neuronové sítě s obecně používanými metodami DPA a SPA je hlavní výhoda nové metody v tom, že i pro algoritmus odolný proti konvenční analýze je metoda schopna určit první bajt tajného klíče s pravděpodobností kolem 96% pomocí jen jednoho průběhu proudové spotřeby. Navržená metoda může pracovat rychle a útočník může provést útok i na kryptografický modul, který se mu podařilo získat jen na krátký čas. Nevýhodou metody je nutnost prvotního trénování neuronové sítě, kde útočník musí vytvořit trénovací množinu proudových spotřeb pro konkrétní kryptografický modul. Za kritickou část je považována správná synchronizace naměřených proudových průběhů. Tohoto faktu lze využít k implementaci protiopatření zabraňující kryptoanalýze, lze např. znemožněním správné synchronizace ovlivněním časové oblasti proudové spotřeby. Další pokračování v práci spočívá v ověření funkčnosti metody pro různé kryptografické moduly (stejný typ) a pro následující bajty tajného klíče bez nutnosti trénování neuronové sítě. Předpokládá se identická implementace algoritmu pro následující bajty tajného klíče viz algoritmus AES operace `AddRoundKey`. Všechny stanovené cíle disertační práce považuji za splněné a dosažené výsledky byly publikovány v odborných časopisech i na tuzemských a mezinárodních konferencích [10, 1, 12, 8].

# LITERATURA


[1] Akkar, M.-L., Bevan, R., Dischamp, P., Moyart, D. Power analysis, what is now possible... In *Advances in Cryptology - ASIACRYPT 2000*, T. Okamoto, Ed., vol. 1976 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2000, pp. 489–502.

[2] Akkar, M.-L., Goubin, L. A generic protection against high-order differential power analysis. In *Fast Software Encryption, 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003, Revised Papers* (2003), vol. 2887 of *Lecture Notes in Computer Science*, Springer, pp. 192–205.

[3] Ambrose, J., Aldon, N., Ignjatovic, A., Parameswaran, S. Anatomy of differential power analysis for aes. In *Symbolic and Numeric Algorithms for Scientific Computing, 2008. SYNASC '08. 10th International Symposium on* (sept. 2008), pp. 459 –466.

[4] Bartkewitz, T., Lemke-Rust, K. Efficient template attacks based on probabilistic multi-class support vector machines. In *Proceedings of the 11th international conference on Smart Card Research and Advanced Applications* (2013), CARDIS'12, Springer-Verlag, pp. 263–276.

[5] Brier, E., Clavier, C., Olivier, F. Correlation power analysis with a leakage model. In *CHES* (2004), pp. 16–29.

[6] Chari, S., Jutla, C., Rao, J. R., Rohatgi, P. A cautionary note regarding evaluation of aes candidates on smart-cards. In *In Second Advanced Encryption Standard (AES) Candidate Conference*, pp. 133–147.

[7] Clavier, C., Feix, B., Gagnerot, G., Roussellet, M., Verneuil, V. Improved collision-correlation power analysis on first order protected aes. In *Cryptographic Hardware and Embedded Systems - CHES 2011*, B. Preneel T. Takagi, Eds., vol. 6917 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2011, pp. 49–62.

[8] Coron, J.-S., Naccache, D., Kocher, P. Statistics and secret leakage. *ACM Trans. Embed. Comput. Syst. 3*, 3 (Aug. 2004), 492–508.

[9] Eck, W. V., Laborato, N. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security* (1985), 269–286.

[10] Fei, Y., Luo, Q., Ding, A. A statistical model for dpa with novel algorithmic confusion analysis. In *Cryptographic Hardware and Embedded Systems - CHES 2012*, E. Prouff P. Schaumont, Eds., vol. 7428 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2012, pp. 233–250.

[11] Fiona, A. H. Y. *ERG4920CM Thesis II Keyboard Acoustic Triangulation Attack*. PhD thesis, Department of Information Engineering the Chinese University of Hong Kong, 2006.

[12] Gandolfi, K., Mourtel, C., Olivier, F. Electromagnetic analysis: Concrete results. In *CHES '01: Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems* (London, UK, 2001), Springer-Verlag, pp. 251–261.

[13] Herbst, C., Oswald, E., Mangard, S. An aes smart card implementation resistant to power analysis attacks. In *Applied Cryptography and Network Security, Second International Conference, ACNS 2006, volume 3989 of Lecture Notes in Computer Science* (2006), Springer, pp. 239–252.

[14] Heuser, A., Zohner, M. Intelligent machine homicide - breaking cryptographic devices using support vector machines. In *COSADE* (2012), pp. 249–264.

[15] Hospodar, G., Gierlichs, B., Mulder, E. D., Verbauwhede, I., Vandewalle, J. Machine learning in side-channel analysis: a first study. *J. Cryptographic Engineering 1*, 4 (2011), 293–302.

[16] Kim, H.-M., Kang, D.-J., Kim, T.-H. Flexible key distribution for scada network using multi-agent system. *Bio-inspired, Learning, and Intelligent Systems for Security, ECSIS Symposium on* (2007), 29–34.

[17] Kocher, P. C., Jaffe, J., Jun, B. Differential power analysis. In *CRYPTO '99: Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology* (London, UK, 1999), Springer-Verlag, pp. 388–397.

[18] Kolofík, J. Optický postranní kanál. bakalařská práce, Vysoké učení technické v Brně, fakulta elektrotechniky a komunikačních technologií, 2010.

[19] Kur, J., Smolka, T., Svenda, P. Improving resiliency of java card code against power analysis. In *Mikulaska kryptobesidka, Sbornik prispevku* (2009), pp. 29–39.

[20] Lerman, L., Bontempi, G., Markowitch, O. Side channel attack: an approach based on machine learningn. In *COSADE 2011 - Second International Workshop on Constructive Side-Channel Analysis and Secure Design* (2011), pp. 29–41.

[21] Lian, S., Sun, J., Wang, Z. One-way hash function based on neural network. *CoRR abs/0707.4032* (2007).

[22] Liu, N., Guo, D. Security analysis of public-key encryption scheme based on neural networks and its implementing. In *Computational Intelligence and Security, 2006 International Conference on* (nov. 2006), vol. 2, pp. 1327 –1330.

[23] Machů, P. Nové postranní kanály v kryptografii. diplomová práce, Vysoké učení technické v Brně, fakulta elektrotechniky a komunikačních technologií, 2010.

[24] Mangard, S., Oswald, E., Popp, T. *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

[25] Messerges, T. Using second-order power analysis to attack dpa resistant software. In *Cryptographic Hardware and Embedded Systems - CHES 2000*, C. Paar, Eds., vol. 1965 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2000, pp. 238–251.

[26] Mislovaty, R., Perchenok, Y., Kanter, I., Kinzel, W. Secure key-exchange protocol with an absence of injective functions. *Phys. Rev. E 66* (Dec 2002), 066102.

[27] Moradi, A., Salmasizadeh, M., Manzuri Shalmani, M. T., Eisenbarth, T. Vulnerability modeling of cryptographic hardware to power analysis attacks. *Integr. VLSI J. 42*, 4 (Sept. 2009), 468–478.

[28] Nabney, I. T. *NETLAB: algorithms for pattern recognition*. Advances in Pattern Recognition. Springer-Verlag New York, Inc., New York, NY, USA, 2002.

[29] Peeters, E., Standaert, F.-X., Quisquater, J.-J. Power and electromagnetic analysis: Improved model, consequences and comparisons. *Integration, the VLSI Journal 40*, 1 (2007), 52 – 60. Embedded Cryptographic Hardware.

[30] Quisquater, J.-J., Samyde, D. Automatic code recognition for smart cards using a kohonen neural network. In *Proceedings of the 5th conference on Smart Card Research and Advanced Application Conference - Volume 5* (Berkeley, CA, USA, 2002), CARDIS'02, pp. 6–6.

[31] Schindler, W., Lemke, K., Paar, C. Paar: A stochastic model for differential side channel cryptanalysis. In *Cryptographic Hardware and Embedded Systems - CHES 2005, Springer, LNCS 3659* (2005), Springer, pp. 30–46.

[32] Tiu, C. C., Tiu, C. C. A new frequency-based side channel attack for embedded systems. master degree thesis, deparment of electrical and computer engineering,university of waterloo,waterloo. Tech. rep., 2005.

[33] Waddle, J., Wagner, D. Towards efficient second-order power analysis. In *Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings* (2004), vol. 3156 of *Lecture Notes in Computer Science*, Springer, pp. 1–15.

[34] Walter, C. D., Çetin Kaya Koç, Paar, C., Eds. *Cryptographic Hardware and Embedded Systems - CHES 2003, 5th International Workshop, Cologne, Germany, September 8-10, 2003, Proceedings* (2003), vol. 2779 of *Lecture Notes in Computer Science*, Springer.

[35] Wang, Y.-h., Shen, Z.-d., Zhang, H.-g. Pseudo Random Number Generator Based on Hopfield Neural Network. pp. 2810–2813.

[36] Zhuang, L., Zhou, F., Tygar, J. D. Keyboard acoustic emanations revisited. In *Proceedings of the 12th ACM conference on Computer and communications security* (New York, NY, USA, 2005), CCS '05, ACM, pp. 373–382.

# LITERATURA

[1] Martinasek, Z., CLupek, V., Trasy, K. General scheme of differential power analysis. In *In 36nd International Conference on Telecommunications and Signal Processing - TSP' 20013.* in print.

[2] Martinasek, Z., Clupek, V., Zeman, V., Sysel, P. Základní metody diferenciální proudové analýzy. *Elektrorevue - Internetový ăasopis (http://www.elektrorevue.cz 2013*, 3 (2013), 1 – 10.

[3] Martinasek, Z., Macha, T., Raso, O., Martinasek, J., Silhavy, P. Optimization of differential power analysis. *PRZEGLAD ELEKTROTECHNICZNY 87*, 12 (2011), 140 – 144.

[4] Martinasek, Z., Macha, T., Stancikk, P. Power side channel information measurement. In *Research in telecommunication technologies RTT2010* (September 2010).

[5] Martinasek, Z., Macha, T., Zeman, V. Classifier of power side channel. In *Proceedings of NIMT2010* (September 2010).

[6] Martinasek, Z., Machu, P. New side channle in cryptography. In *Proceedings of the 17th Conference Student EEICT 2011* (April 2011).

[7] Martinásek, Z., Nečas, O., Zeman, V., Martinásek, J. Diferenciální elektromagnetická analýza. *Elektrorevue - Internetový časopis (http://www.elektrorevue.cz 2011*, 60 (2011), 1 – 6.

[8] Martinasek, Z., Petrik, T., Stancik, P. Conditions affecting the measurement of power analysis. In *Research in telecommunication technologies RTT2011* (September 2011).

[9] Martinásek, Z., Petřík, T., Stančík, P. Parametry ovlivňující proudovou analýzu mikroprocesoru vykonavajícího funkci addroundkey. *Elektrorevue - Internetovy časopis (http://www.elektrorevue.cz 2011*, 51 (2011), 1 – 6.

[10] Martinasek, Z., Zeman, V. Innovative method of the power analysis. *Radioengineering 22*, 2 (2013).

[11] Martinasek, Z., Zeman, V., Sysel, P., Trasy, K. Near electromagnetic field measurement of microprocessor. *PRZEGLAD ELEKTROTECHNICZNY 89*, 2a (2013), 203 – 207.

[12] Martinasek, Z., Zeman, V., Trasy, K. Simple electromagnetic analysis in cryptography. *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems 1*, 1 (2012), 1 – 6.

*Curriculum Vitae*

# Zdeněk Martinásek

---


**Kontaktní údaje:**

| | |
|---|---|
| Bydliště: | Školní 349, Otnice, 683 54 |
| E-mail: | martinasek@feec.vutbr.cz |
| GSM: | +420 774 303 173 |


**Vzdělání:**

| | |
|---|---|
| od 2008 | VUT FEKT v Brně, doktorské studium<br>Fakulta Elektrotechniky a komunikačních technologií<br>Obor: Teleinformatika<br>Dizertační práce: Kryptoanalýza postranními kanály |
| 9.2011–1.2012 | Technische Universität Wien, odborná stáž<br>Department of Teleinformatik<br>Práce na dizertační práci (Power analysis) |
| 2006–2008 | VUT FEKT v Brně, magisterské studium<br>Fakulta Elektrotechniky a komunikačních technologií<br>Obor: Telekomunikační a informační technika<br>Diplomová práce: Tenký měřič plošného teplotního rozdělení s maticí negastorů |
| 2003–2006 | VUT FEKT v Brně, bakalářské studium<br>Fakulta Elektrotechniky a komunikačních technologií<br>Obor: Teleinformatika<br>Bakalářská práce: Vybrané obvody zpracování senzorových signálů |

**Současná pozice:**

od 2008 odborný asistent, Ústav telekomunikací, VUT v Brně

**Účast na projektech**

| | |
|---|---|
| 2012-2014 | TA02011260: Systém pro kryptografickou ochranu elektronické identity. Řešitel prof. Ing. Kamil Vrba, CSc. |
| 2012-2014 | FR-TI4/647: Integrační server s kryptografickým zabezpečením. Řešitel prof. Ing. Kamil Vrba, CSc. |
| 2010-2013 | FR-TI2/220: Výzkum modulárního systému pro komunikační technologie a ověření na 2N communication serveru. Řešitel prof. Ing. Kamil Vrba, CSc. |
| 2011-2013 | TA01031072, Inteligentní telematický informační systém veřejné dopravy. Řešitel doc. Ing. Václav Zeman, Ph.D. |
| 2008-2010 | FT-TA5/012: Decentralizované čistění odpadních vod s telemetrickým řídícím systémem pro malé obce. Řešitel prof. Ing. Kamil Vrba, CSc. |
| 2011 | 3046/2011/G1: Zavedení problematiky postranních kanálů |

| | |
|---|---|
| | laboratorních cvičení předmětu Kryptografie v informatice. Řešitel Ing. Peter Stančík |
| 2010 | 2383/2011/F1a: Inovace laboratorních úloh v kurzech zaměřených na datovou komunikaci. Řešitel Ing. Martin Koutný |
| 2010 | 2829/2010/G1: Autentizační kryptografické moduly Řešitel Ing. Jiří Sobotka |
| 2010 | 2534/2009/F1: Modernizace výuky předmětu Kryptografie v informatice. Řešitel doc. Ing. Otto Dostál, CSc. |

**Vyžádané recenze pro vědecké časopisy a konference:**

- Conference on Telecommunications and Signal Processing (TSP)
- Conference on Student Electrical Engineering, Information and Communication Tech-nologies (EEICT)
- Conference on Research in Telecommunication Technologies (RTT)
- Elektrorevue - Internet Journal
- International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems - Internet Journal

**Výsledky vědecké činnosti:**

Počet článků v impaktovaných časopisech: **1**
Počet příspěvků na konferencích indexovaných ve Web of Science: **4**
Ostatní odborné časopisy a konference: **18**
H-index podle Web of Science: **1**

Poslední aktualizace: 11. října 2012

## ABSTRAKT

Postranní kanály v oblasti kryptografie zásadním způsobem mění pohled na bezpečnost celého kryptografického systému. Již nestačí analyzovat bezpečnost algoritmu pouze z matematického hlediska pomocí abstraktních modelů, ale stejný důraz musí být kladen na implementaci algoritmů. Disertační práce v úvodu vysvětluje základní pojmy, princip útoku postranními kanály a jejich základní dělení. V následující části jsou určeny cíle dizertační práce. Hlavním cílem disertační práce je navrhnout a experimentálně ověřit novou metodu analýzy proudovým postranním kanálem, která bude využívat neuronové sítě. Tento hlavní cíl vznikl z rozboru používaných analýz proudovým postranním kanálem uvedených v následujících kapitolách. Tyto kapitoly obsahují podrobný rozbor současně používaných analýz proudovým postranním kanálem a rozbor šifrovacího algoritmu AES. Algoritmus AES byl vybrán, z důvodu odolnosti proti konvenčnímu způsobu analýz. Následující kapitola popisuje získané dílčí experimentální výsledky optimalizace stávajících metod, vliv parametrů ovlivňující proudovou spotřebu a výsledky navržené analýzy pomocí neuronových sítí včetně diskuze získaných výsledků. Tento typ útoku proudovým postranním kanálem nebyl dosud publikován, jedná se tedy o zcela novou myšlenku. Posledním cílem práce bylo shrnutí možných ochran proti analýze a útoku postranním kanálem.