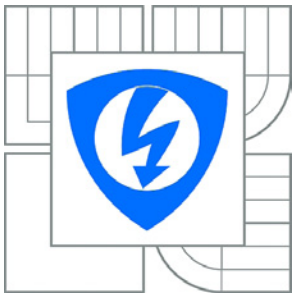
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

MODERNÍ KRYPTOANALÝZA

MODERN CRYPTANALYSIS

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

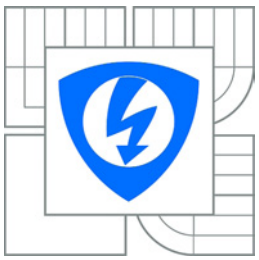
AUTOR PRÁCE — Bc. TOMÁŠ PETŘÍK

AUTHOR

VEDOUCÍ PRÁCE — Ing. ZDENĚK MARTINÁSEK

SUPERVISOR

BRNO 2011



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Tomáš Petřík	***ID:***	70059
Ročník:	2	***Akademický rok:***	2010/2011

NÁZEV TÉMATU:

Moderní kryptoanalýza

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte základní útoky postranními kanály na kryptografický modul. Zaměřte se především na proudový postranní kanál. Navrhněte a realizujte experimentální desku plošných spojů osazenou jen procesorem PIC a potřebnými součástkami k funkčnosti čipu a měření proudového odběru. Pomocí desky realizujte měření proudového odběru procesoru v závislosti na velikosti napájecího napětí, oscilátoru, odporu bočníku, vliv blokovacího kondenzátoru, paracitních kapacit, teploty atd. Procesor bude cyklicky zpracovávat jednu instrukci. Naměřené výsledky přehledně zpracujte.

DOPORUČENÁ LITERATURA:

[1] ALFRED J. MENEYES, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996

[2] KOCHER, P., JAFFE, J., JUN, B.: Introduction to Differential Power Analysis and Related Attacks, San Francisco, 1998. [.pdf dokument]. Dostupný z WWW:http://www.cryptography.com/resources/whitepapers/DPATechInfo.pdf

Termín zadání:	7.2.2011	***Termín odevzdání:***	26.5.2011

Vedoucí práce: Ing. Zdeněk Martinásek

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Problematika této diplomové práce je zaměřena na kryptoanalýzu postranních kanálů. Pozornost je věnována především proudovému postrannímu kanálu, kdy se simuluje útok na kryptografický modul za různých podmínek a pro různé konstrukční vlastnosti tohoto modulu.
Jako kryptografický modul je použit mikroprocesor PIC pracující se symetrickou šifrou AES. Pro tyto účely byl vytvořen návrh experimentální desky plošných spojů. Tato deska pak byla osazena pouze součástkami nezbytnými pro funkci kryptografického modulu. Kryptoanalýza je zaměřena na proudový odběr modulu při vykonávání instrukcí funkce AddRoundKey. Proudový odběr mikroprocesoru se měří v závislosti na velikosti napájecího napětí, velikosti odporu bočníku, velikosti kapacity blokovacího kondenzátoru a také se zkoumá vliv teploty okolního prostředí.
Naměřené hodnoty jsou graficky zpracovány a diskutovány.

KLÍČOVÁ SLOVA

Kryptoanalýza, postranní kanály, proudový postranní kanál, AES, PIC16F84A, vliv konstrukčního řešení kryptografického modulu na proudový postranní kanál.

ABSTRACT

Issues of this thesis are focused on side-channel cryptanalysis. Particularly attention is paid to differential power analysis, when is simulated an attack on the cryptographic module for different conditions and for different structural features of this module.
As the cryptographic module is used a PIC microcontroller, which is operating with AES symmetric encryption algorithm. For this purpose, a design of experimental printed circuit board was created. Then, this PCB was equipped only with the necessary components for the function of the cryptographic module. Cryptanalysis is aimed on current consumption of crypto module that is caused by execution of AddRoundKey instructions. Power consumption of PIC microcontroller is measured in depending on the size of power supply voltage, size of serial resistor, size of bypass capacitor, and this thesis also examines the influence of ambient temperature on power consumption of PIC.
The measured values are graphically presented and then discussed.

KEYWORDS

Side-Channels Cryptanalysis, current side-channel, AES, PIC16F84A, influence of construction solutions onto crypto modules current side-channel.

PETŘÍK, Tomáš *Moderní kryptoanalýza*: diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2011. 59 s. Vedoucí práce byl Ing. Zdeněk Martinásek

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Moderní kryptoanalýza“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

Brno ....

(podpis autora)

Poděkování

Děkuji vedoucímu mé diplomové práce Ing. Zdeňku Martináskovi za velmi užitečnou metodickou, odbornou a pedagogickou pomoc při zpracování práce. Děkuji svým rodičům za umožnění vysokoškolského studia. Děkuji rodině a svým blízkým za podporu, kterou mi poskytovali nejen během studií.

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Diplomová práce se zabývá problematikou kryptoanalýzy postranních kanálů. Jedním z úkolů je seznámení se se základními útoky na postranní kanály a stručné vysvětlení jejich základní charakteristiky. Pozornost je zaměřena především na proudový postranní kanál.

Dalším cílem práce je návrh a realizace experimentální desky plošných spojů. Tato deska je osazena pouze procesorem PIC a potřebnými součástkami k funkčnosti čipu. Pomocí této desky je pak realizována série měření proudového odběru mikroprocesoru při zpracovávání instrukcí implementovaného programu.

DPS spolu s procesorem PIC plní funkci kryptografického modulu. Tento kryptografický modul pracuje se symetrickým šifrovacím algoritmem AES. Cílem je analýza proudového postranního kanálu tohoto modulu při vykonávání operací šifry AES nad blokem otevřeného textu a blokem tajného klíče. V průběhu této operace se zaznamenává průběh aktuální spotřeby proudu v závislosti na hodnotách operandů zpracovávané instrukce. Předmětem zkoumání je analýza a porovnání naměřených závislostí při různých konstrukčních vlastnostech obvodu kryptografického modulu a za dalších podmínek, které mohou mít nějaký vliv na odběr proudu.

Tyto závislosti spotřeby proudu (napětí) jsou pak graficky zpracovány a diskutovány. V závěru práce jsou pak ještě shrnuty způsoby obrany a možná protiopatření znesnadňující útoky, kdy je právě zneužito postranních kanálů.

1 ZÁKLADNÍ POJMY

V této kapitole jsou uvedeny základní pojmy a definice, které se týkají problematiky kryptoanalýzy.

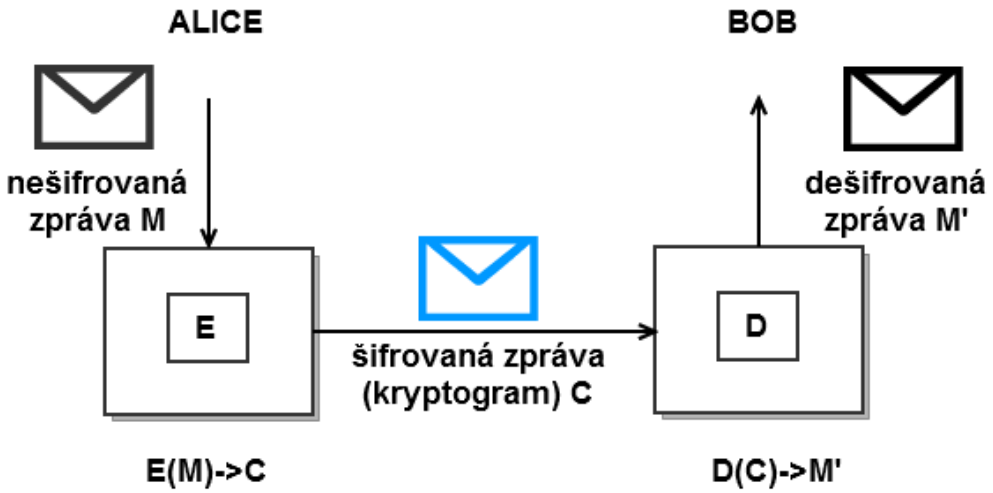
1.1 Kryptologie

Je to vědní obor zabývající se problematikou šifrování, dešifrování, prolamování šifer a analýzy odolnosti kryptografických systémů. Dělí se na dva podobory a to kryptografii a kryptoanalýzu [1].

1.2 Kryptografie

Zabývá se studiem matematických postupů souvisejících s různými aspekty zabezpečení informací. Mezi ně patří ověření a zajištění důvěryhodnosti informací, integrity informací, autentizace subjektů, které nějakým způsobem nakládají s informacemi, jež jsou předmětem zabezpečení, a autentizace původu informací.

Kryptografie není jediným prostředkem umožňujícím zabezpečení informací, ale jen jedna z technik používaných k tomuto účelu [1].



Obr. 1.1: Jednoduché schéma šifrované komunikace.

1.3 Kryptoanalýza

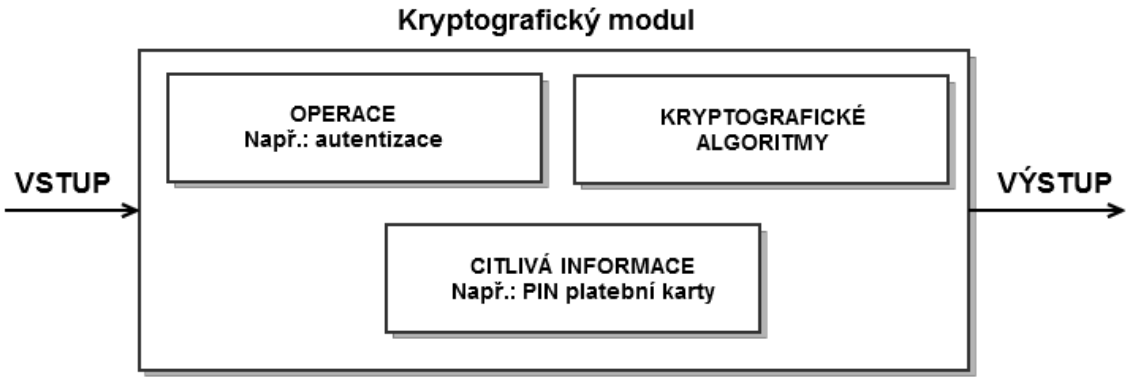
Zabývá se studiem matematických metod umožňujících pokusy o prolomení či testování odolnosti kryptografických technik [1].

1.4 Kryptografický modul

Kryptografický modul je fyzická implementace konkrétního kryptografického algoritmu a používá se pro zajištění všech bezpečnostních požadavků. Jedná se o zařízení, které lze realizovat softwarově i hardwarově. Všechny citlivé operace a procesy, které souvisí například s autentizací, ověřováním, podepisováním, šifrováním nebo dešifrováním, probíhají uvnitř tohoto modulu. Požaduje se po něm rychlé plnění kryptografických služeb, přičemž s okolím může komunikovat jen po definovaných rozhraních. Činnost kryptografického modulu je označení pro všechny operace, které v něm probíhají.

Bezpečnostní požadavky kryptografického modulu jsou:

- fyzická bezpečnost,
- logická bezpečnost,
- bezpečnost prostředí.



Obr. 1.2: Obecné schéma kryptografického modulu.

V praxi se kryptografické moduly objevují například ve formě počítačů, bankomatů, serverů, automatů nebo čipových karet [2].

1.5 Kryptografické algoritmy

Slovem šifra nebo šifrování se označuje kryptografický algoritmus, který převádí čitelnou zprávu neboli prostý text na její nečitelnou podobu neboli šifrový text.

Základní rozdělení algoritmů

- Šifry
  - Symetrické šifry
    Pro šifrování i dešifrování je použit pouze jediný – tajný – klíč.
    - Proudové šifry
      Zpracovávají otevřený text po jednotlivých bitech (např. RC4).
    - Blokové šifry
      Rozdělí otevřený text na bloky stejné velikosti a doplní vhodným způsobem poslední blok na stejnou velikost (např. DES, AES).
  - Asymetrické šifry
    Pro šifrování a dešifrování používají dvojici klíčů, tj. veřejný a soukromý klíč.
    - Veřejný klíč
      Používá se pro zašifrování zprávy, je veřejně dostupný.
    - Soukromý klíč
      Používá se pro dešifrování zprávy a je vlastníkem pečlivě uschován (např. RSA).
- Hashovací funkce
  Jsou to výpočetně jednoduché algoritmy. Vstupem hashovací funkce je zpráva libovolné konečné délky, případně i tajný klíč, a jejich výstupem je $h(x)$ (otisk neboli *hash*), který je už ovšem pevné délky n bitů, kdy n nabývá délky 128, 160, 256, 512 bitů.
  - Bez klíče
    Mají jediný vstupní parametr a to zprávu M.
  - S klíčem
    Mají dva nezávislé vstupní parametry a to zprávu M a klíč K.

1.5.1 AES

Vstupní data algoritmu tvoří nešifrovaná data rozdělená do bloků o délce 128 bitů a klíč, který může nabývat délky 128, 192 nebo 256 bitů. Tento blok dat je v kolech, neboli rundách, modifikován čtyřmi transformacemi: *ByteSub*, *ShiftRow*, *MixColumn* a *AddRoundKey*. Počet rund (dále budeme značit N_r) je závislý na délce klíče (tab. 1.1) a jedná se o počet opakování průchodu dat šifrovacím algoritmem.

Tab. 1.1: Počet rund pro různé délky klíčů.

	$N_k = 4$ (128 bitů)	$N_k = 6$ (192 bitů)	$N_k = 8$ (256 bitů)
N_r	10	12	14

Vstupní blok dat se označuje jako stav. Ten lze zapsat jako matici 4×4 bajtů. Při implementaci se stav reprezentuje jako pole bajtů. Stav je pak mapován do pole po sloupcích v pořadí $a_{0,0}, a_{1,0}, a_{2,0}, a_{3,0}, a_{0,1}, a_{1,1}, a_{2,1}, a_{3,1}, \ldots$ Klíč je rovněž namapován do pole 4×4 bajtů a to v pořadí $k_{0,0}, k_{1,0}, k_{2,0}, k_{3,0}, k_{0,1}, k_{1,1}, k_{2,1}, k_{3,1}, \ldots$ Počet sloupců klíče se značí N_k, počet sloupců stavu je vždy $N_b = 4$ (128 bitů).

$$\mathbf{A} = \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}, \mathbf{K} = \begin{pmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{pmatrix}.$$

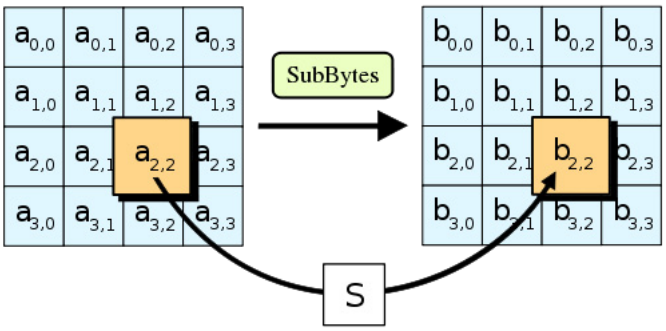
Runda šifry AES

Jedna runda je složena ze čtyř operací, které budou dále krátce popsány. Počet rund, kterými vstupní blok dat projde je tedy závislý na délce použitého klíče (tab. 1.1). V poslední rundě se vynechává operace *MixColumn*.

Operace tvořící rundu algoritmu AES:

Operace *ByteSub*

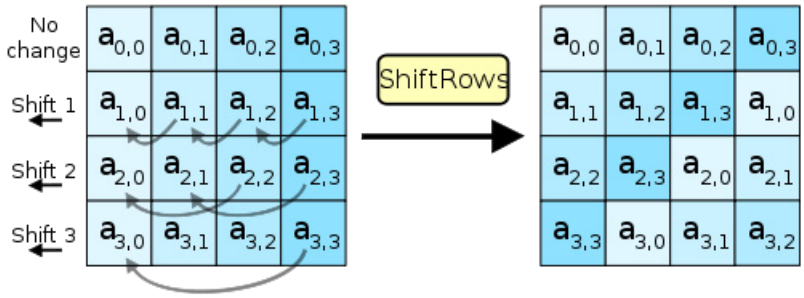
Transformace *ByteSub* je jedinou nelineární operací AES algoritmu. Pomocí substituční tabulky (*S-box*) je transformován každý prvek pole $a_{m,n}$ na prvek $b_{m,n}$ (obr. 1.3).



Obr. 1.3: Operace *ByteSub* [5].

Operace *ShiftRow*

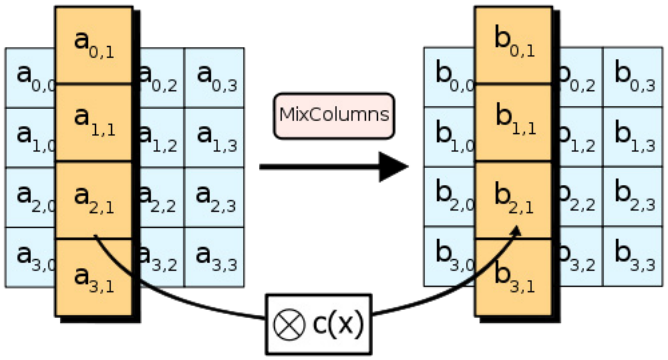
V této operaci jsou bajty v řádku stavu cyklicky posouvány o různé hodnoty. Prvky řádku, které přetečou, se zařadí na konec příslušného řádku. Nultý řádek stavu zůstává nezměněn, v prvním řádku se posunou hodnoty o 1 pozici doleva, ve druhém řádku o 2 pozice doleva a ve třetím řádku se posunou o 3 pozice (obr. 1.4).



Obr. 1.4: Operace *ShiftRow* [5].

Operace *MixColumns*

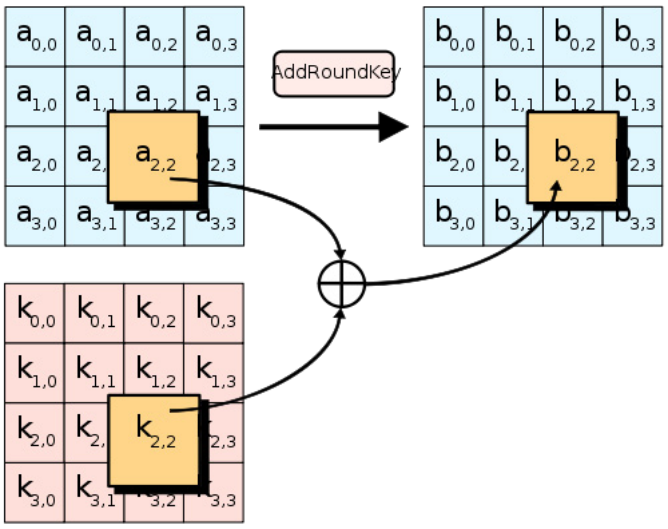
Transformace *MixColumn* (obr. 1.5) uvažuje sloupce stavu jako polynomy, které jsou násobeny fixním polynomem $c(x)$.



Obr. 1.5: Operace *MixColumns* [5].

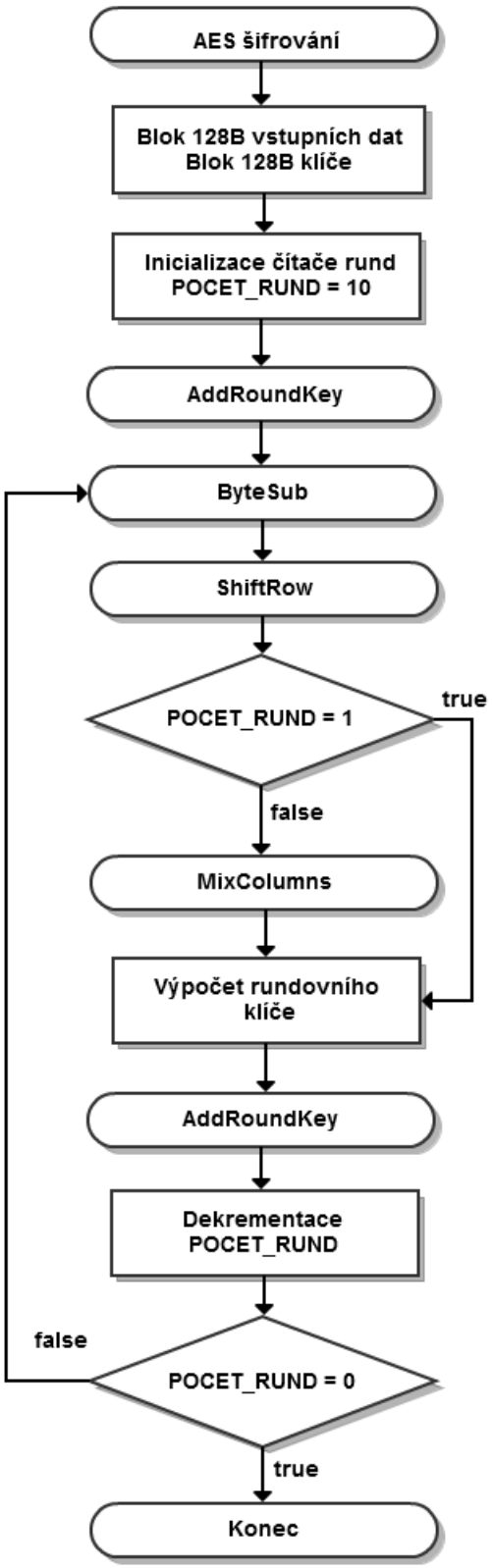
Operace *AddRoundKey*

Tato operace provede přičtení rundovního klíče (pole klíčů, viz obr. 1.6) ke stavu prostřednictvím exkluzivního součtu XOR.



Obr. 1.6: Operace *AddRoundKey* [5].

Na obr. 1.7 je zobrazen zjednodušený vývojový diagram AES algoritmu pro 128-bitovou délku klíče N_r=10.



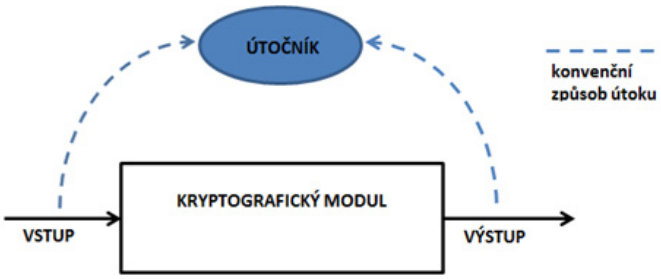
Obr. 1.7: Vývojový diagram AES šifry.

2 KRYPTOANALÝZA

Jedná se o vědní obor zabývající se analýzou matematických mechanizmů použitých za účelem zabezpečení dat. Tento obor hraje čím dál významnější roli při návrhu a konstrukci kryptografických modulů, jelikož na základě aktuálních kryptoanalytických poznatků dochází k neustálému iterativnímu zlepšování mechanizmů šifrování dat.

2.1 Konvenční kryptoanalýza

Využívá útoku na vstupní a výstupní komunikační kanál kryptografického modulu (obr. 2.1), kdy analytik (útočník) na těchto kanálech zachytí zašifrovaná data. Tento typ analýzy je v dnešní době neefektivní a časově náročný, jelikož většina dnes užívaných kryptografických algoritmů je prakticky neprolomitelná v případě, kdy má analytik (útočník) k dispozici pouze šifrovaný text.



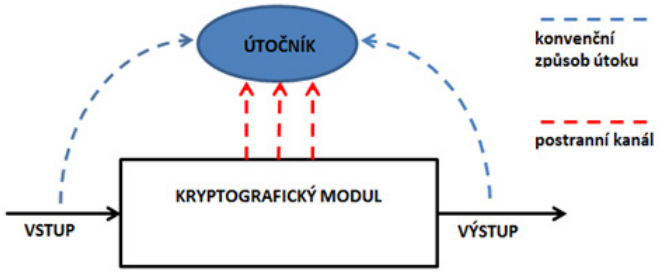
Obr. 2.1: Konveční kryptoanalýza.

2.2 Kryptoanalýza postranních kanálů

S objevem postranních kanálů u kryptografických modulů se dosavadní pohled na jejich bezpečnost zcela změnil. Postranní kanál je definován jako nežádoucí výměna informací mezi kryptografickým modulem a jeho okolím. Novější a pokročilejší metodou oproti konvenční kryptoanalýze je tedy kryptoanalýza postranních kanálů.

S příchodem tohoto nového konceptu útoku začalo docházet k totálním průnikům do kryptografických systémů. Přestože samotné kryptografické mechanizmy mohou být dostatečně silné a odolné vůči napadení, může dojít k výrazné degradaci

bezpečnosti celého systému vlivem nekvalitní implementace těchto mechanizmů. Nevhodnou implementací mohou vzniknout postranní kanály, což je samozřejmě nežádoucí, jelikož útočník už spolu se zachycenou zašifrovanou komunikací může získat i další citlivé informace právě prostřednictvím těchto postranních kanálů (obr. 2.2). Následkem je pak výrazné usnadnění prolomení kryptografického systému [6, 7].



Obr. 2.2: Kryptoanalýza zahrnující využití postranních kanálů.

Přehled známých typů postranních kanálů:

- výkonový (proudový),
- elektromagnetický,
- časový,
- chybový,
- optický (tepelný),
- akustický,
- kleptografický.

Každý z těchto postranních kanálů má přesnou definici způsobu, jakým dochází k nežádoucí výměně citlivých informací kryptografického modulu s jeho okolím. Následně je v rámci útoku nutné získané informace zpracovat a vyhodnotit. V kryptografii se tento proces souhrnně nazývá analýzou kanálu. Existují dva základní druhy analýz a to:

- jednoduchá analýza (Simple Analysis),
- diferenční analýza (Differential Analysis).

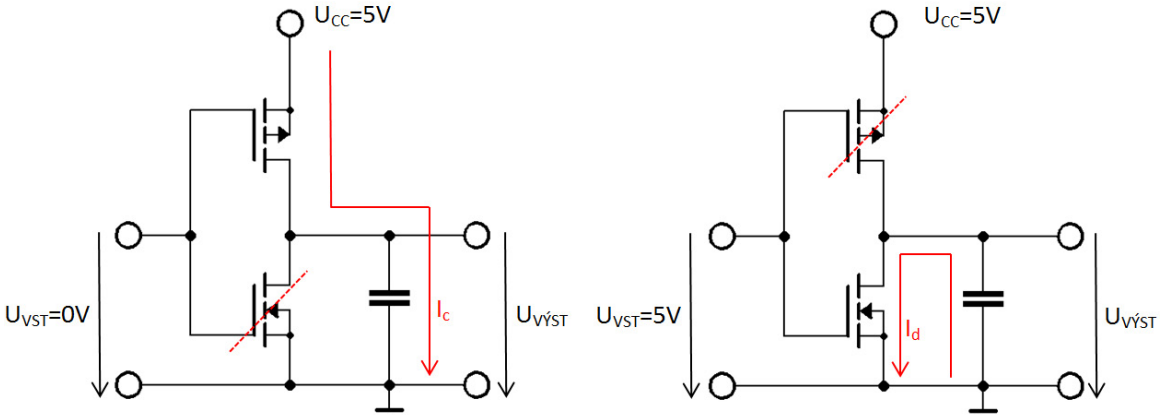
Jednoduchá analýza představuje základní způsob zpracování výsledků. Informace získané z postranního kanálu jsou útočníkem přímo pozorovány a vyhodnoceny. Naopak komplikovanější je metoda diferenční analýzy, jelikož vyžaduje použití matematického aparátu. Často však umožňuje nalézt citlivé informace i z postranních kanálů, kde jejich přítomnost není zřejmá. Výhodou je také možnost automatizace

procesu, což může výrazně snížit potřebný čas nutný k analýze informací získaných z postranního kanálu.

2.2.1 Výkonový (proudový) postranní kanál

Jedná se o fyzikální druh postranního kanálu, kdy se při analýze tohoto postranního kanálu sleduje spotřeba proudu napadeného kryptografického modulu.

Princip funkce výkonového (proudového) postranního kanálu
Většina dnes používaných integrovaných obvodů je založena na využití tranzistorových součástek technologie CMOS. Elementárním stavebním prvkem obvodů typu CMOS je invertor, jehož vnitřní zapojení se skládá ze dvou tranzistorů typu MOSFET. Tyto tranzistory jsou zapojeny jako spínače řízené napětím, viz obr. 2.3:



Obr. 2.3: Model invertoru logiky založené na CMOS.

- Pokud je U_{VST} rovno napětí logické úrovně „0“, je horní tranzistor otevřen a dolní uzavřen.
- V momentě, kdy se na U_{VST} připojí napětí logické úrovně „1“, je dolní tranzistor otevřen a horní uzavřen.

V případě obou stavů popsaných výše je proudová spotřeba nízká, avšak pro každý stav je různá. V obvodu při přechodu mezi těmito stavy nastává výkonová špička, kdy jsou na krátký okamžik otevřeny oba tranzistory současně, a napájení je zkratováno proti zemi. Tento jev se nazývá dynamickou spotřebou a při měření odebíraného proudu se projeví špičkami v průběhu proudu v závislosti na čase. Její velikost závisí na tom, kolik tranzistorů právě přepíná. Proudovou špičku lze změřit tak, že se do série s V_{DD} nebo V_{SS} zapojí rezistor, na kterém se následně změří úbytek napětí, který odpovídá okamžitému odběru proudu. Tranzistory odebírají malý proud i v klidovém stavu, který se pak mění na teplo či záření. Dominantním

zdrojem výkonových změn je nabíjení (I_c) a vybíjení (I_d) interní kapacitní zátěže, která je připojená na výstupy. Mezi zdroje výkonových změn patří:

- Tepelné vyzařování tranzistorů v klidovém stavu a proudový odběr pro stav logické „0“ a pro stav logické „1“. Elektrická energie se mění na teplo.
- Proudové špičky při přechodu mezi stavy logické „0“ a logické „1“.
- Změny proudu při vybíjení a nabíjení parazitní kapacitní zátěže připojené sběrnice při změnách pracovních stavů.

Z toho plyne, že výkonová spotřeba elektronických obvodů přímo závisí na operacích, které v nich probíhají, tedy na množství překlápěných tranzistorů. Analýzou výkonové spotřeby lze tedy zjistit citlivé informace uvnitř kryptografického modulu [2].

Měření proudové spotřeby

Spotřeba proudu mikrokontroléru není s časem konstantní. Při pohledu na průběh odebíraného proudu v čase se může tato závislost zpočátku jevit jako šum, avšak nahodilost průběhu je pouze zdánlivá a při bližším pohledu je vidět opakující se prvky, jisté šablony nebo jistá periodicita.

Změny proudové spotřeby vznikají na úrovni základních elektronických součástek, mezi které patří z velké části tranzistory. Probíhající kryptografické operace přímo ovlivňují činnost těchto prvků. Aktuální spotřeba mikroprocesoru závisí tedy na vykonávaných instrukcích programu a používaných prostředcích mikroprocesoru (ADC, komunikace s periferním zařízením, atd.). Příklad závislosti odebíraného proudu na čase lze vidět v grafu na obr. 2.4, kde je vyobrazen odběr proudu po dobu 8 instrukčních cyklů mikrokontroléru.

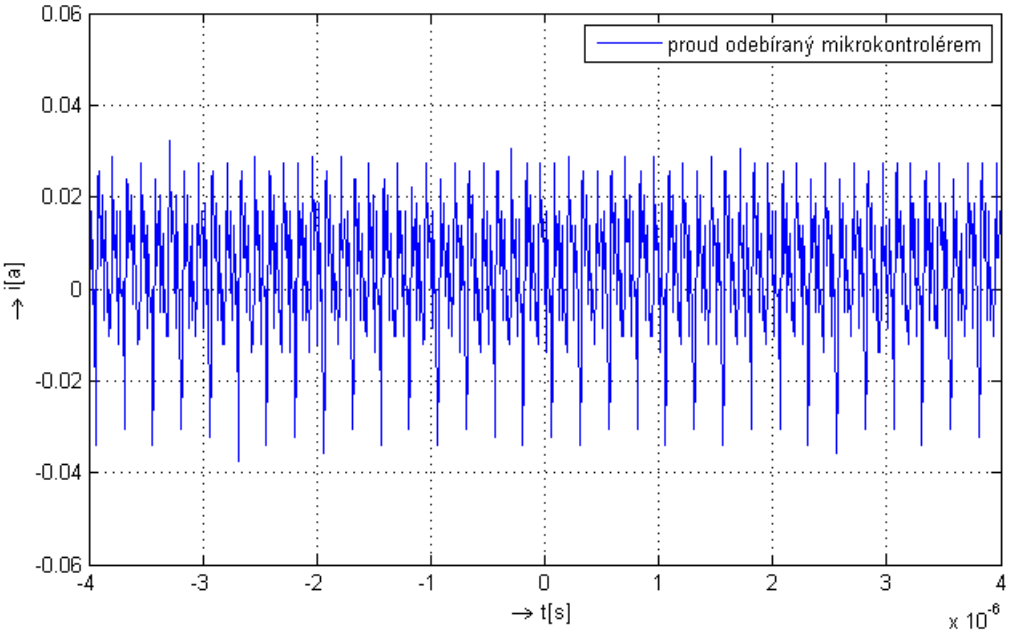
Výkonová analýza (Power Analysis – PA)

Nejpoužívanější jsou dva základní typy analýz tohoto postranního kanálu:

- jednoduchá výkonová analýza – Simple Power Analysis (SPA),
- diferenční výkonová analýza – Differential Power Analysis (DPA).

SPA

Jedná se o techniku útoku realizovanou prostřednictvím výkonového postranního kanálu, kdy je snahou odvodit klíč na základě přímého pozorování aktuální výkonové spotřeby kryptografického modulu. Tento typ analýzy často vyžaduje detailní znalost implementace kryptografického algoritmu, který kryptografický modul používá pro zabezpečení dat. Podmínkou je, že klíč zpracovávaný kryptografickým modulem musí mít (přímo či nepřímo) významný vliv na výkonovou spotřebu daného modulu.



Obr. 2.4: Proudový odběr mikroprocesoru PIC.

Každá operace pak má charakteristický průběh výkonové spotřeby. Pozorováním výkonové spotřeby je určen sled provedených operací závislých na zpracovávaných datech. SPA útoky jsou využívány v případě, kdy je možno uskutečnit pouze jedno či velice málo měření pro určitou sadu vstupních dat (výběr z bankomatu, platba platební kartou, ...).

DPA

Jedná se o techniku útoku realizovanou skrze výkonový postranní kanál, kdy je snahou odvodit klíč na základě velkého počtu zaznamenaných měření aktuální výkonové spotřeby kryptografického modulu při zpracovávání rozdílných bloků dat. DPA útoky jsou nejhojněji používané díky faktu, že na rozdíl od SPA nevyžaduje detailní znalost kryptografického modulu. Útočníkovi dostačuje znát použitý kryptografický algoritmus implementovaný do modulu. DPA se zabývá analýzou závislosti výkonové spotřeby na modulem zpracovávaných datech v určitý časový okamžik [9].

Jednotlivé kroky provedení DPA útoku

Při DPA útoku se vybere střední výsledek hodnot zpracovaných napadeným kryptografickým modulem. Tento výsledek je označen jako funkce $f(d, k)$, kde d je výsledek

zpracovaných dat modulem a k je část klíče použitého k šifrování (dešifrování) těchto dat.

Dalším krokem je měření spotřeby výkonu napadeného modulu při průchodu dat šifrovacím algoritmem. Celkový počet bloků dat, které jsou modulem zpracovány je označen D. K těmto datovým blokům je nutno přiřadit korespondující střední výsledky funkce $f(d, k)$. Tyto výsledky pak lze zapsat jako vektor $\mathbf{d} = (d_1, \ldots, d_D)'$, kde d_i značí výsledek i-tého zpracovaného bloku vstupních dat. Korespondující spotřeba výkonu při zpracování bloku dat d_i je označena jako $\mathbf{t}'_i = (t_{i,1}, \ldots, t_{i,T})'$, kde T je doba trvání naměřeného průběhu spotřeby příslušejícího výsledku d_i. Celkový počet vektorů hodnot spotřeby $\mathbf{t}'_i$ tedy bude D. Hodnoty mohou být zapsány jako matice velikosti $D \times T$. Hodnoty spotřeby výkonu každého sloupce $\mathbf{t}_j$ matice $\mathbf{T}$ by měly být důsledkem vykonání stejné operace napadeným kryptografickým modulem.

Následující krok se vypočítá odhad středního výsledku pro každou možnou hodnotu klíče k. Hodnoty klíče lze zapsat jako vektor $\mathbf{k} = (k_1, \ldots, k_K)'$, kde K je počet všech možných hodnot klíče. Na základě vektoru $\mathbf{d}$ a odhadu klíče $\mathbf{k}$ se vypočítají hypotetické střední hodnoty $f(d, k)$ pro D šifrovacích cyklů (zašifrování či dešifrování D bloků vstupních dat) a pro všech K odhadů klíče. Výsledkem bude matice $\mathbf{V}$ o velikosti $D \times K$. Výpočet jednotlivých hodnot je znázorněn rovnicí

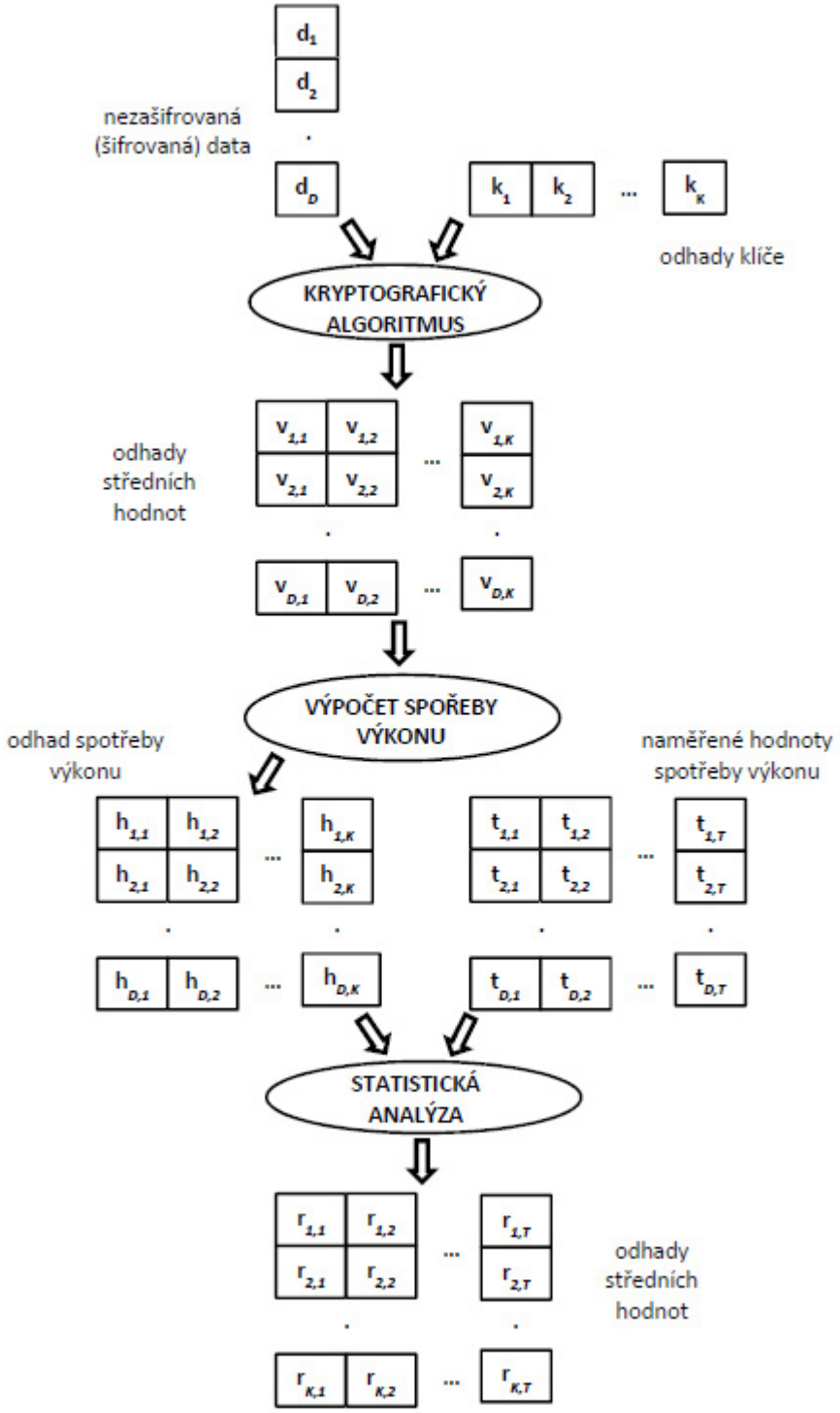
$$v_{i,j} = f(d_i, k_j), \tag{2.1}$$

kde $i = (1, \ldots, D)$ a $j = (1, \ldots, K)$.

Sloupec j matice $\mathbf{V}$ obsahuje střední výsledky, které byly vypočteny na základě odhadu klíče k_j. Předposledním krokem je namapování matice $\mathbf{V}$ do matice $\mathbf{H}$, která reprezentuje hodnoty odhadované spotřeby výkonu. Za tímto účelem se využívá simulace na hypotetickém modelu, který je vytvořen na základě znalosti skutečného napadeného modulu. Pro každou hodnotu $v_{i,j}$ se získá hodnota spotřeby výkonu $h_{i,j}$. Posledním krokem je komparace hodnot získaných z korelace mezi oběma postranními kanály, tj. reálného napadeného modulu a hypotetického modulu. Výsledkem bude matice $\mathbf{R}$ o velikosti $K \times T$, kde každý element $r_{i,j}$ obsahuje výsledek korelace mezi sloupci $\mathbf{h}_i$ a $\mathbf{t}_j$. Výpočet hodnot korelačních koeficientů matice $\mathbf{R}$, dle vzorce (2.2), je nejběžnější variantou determinace lineárních vztahů mezi hodnotami získaných měřením na postranních kanálech při DPA útoku.

$$r_{i,j} = \frac{\sum_{d=1}^{D}(h_{d,i} - \overline{h}_i) \cdot (t_{d,j} - \overline{t}_j)}{\sqrt{\sum_{d=1}^{D}(h_{d,i} - \overline{h}_i)^2 \cdot \sum_{d=1}^{D}(t_{d,j} - \overline{t}_j)^2}}. \tag{2.2}$$

Čím je vyšší hodnota koeficientu $r_{i,j}$, tím je diference mezi hodnotami sloupců $\mathbf{h}_i$ a $\mathbf{t}_j$ menší. Odhad klíče je tedy v tomto případě nejpřesnější [9].



Obr. 2.5: Blokový diagram ilustrující průběh DPA útoku [9].

2.2.2 Elektromagnetický postranní kanál

Při analýze elektromagnetického postranního kanálu se využívá principu, kdy změny proudů v obvodech kryptografických modulů, při jejich činnosti, generují střídavé magnetické pole. V případě, že je generované magnetické pole dostatečně silné, může být detekováno. Útočník umístí do blízkosti zařízení cívku a naměřené elektromagnetické pole posléze analyzuje. Tato problematika bude v blízké budoucnosti velmi exponovanou oblastí.

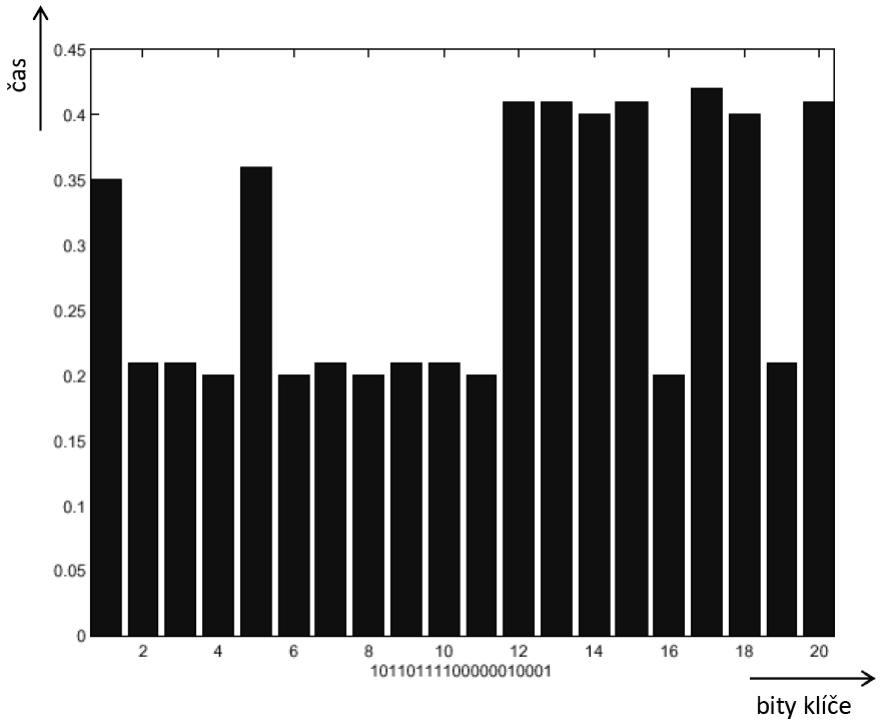
2.2.3 Časový postranní kanál

V případě analýzy časového postranního kanálu se využívá jednoduchý princip, kdy určité operace závislé na tajném klíči trvají různou dobu. Závisí to na konkrétních hodnotách jednotlivých bitů klíče. Na obrázcích 2.6 a 2.7 lze vidět příklad časového útoku na privátní klíč RSA v operaci odšifrování nebo podpisu $y = (m^d) \bmod n$. Na obrázku 2.6 je uveden zdrojový kód pro výpočet modulární mocniny pomocí známého algoritmu „*square and multiply*“, kdy se jednotlivé bity privátního klíče (exponentu d) postupně zpracovávají. Doby průchodu jednotlivých bitů klíče tímto algoritmem jsou pak tedy různé, jak je vidět na obrázku 2.7 [6].

Výpočet y = (m^d mod n) square and multiply:
d=$d_0 d_1$ ... d_{b-1} (nejvyšší bit d_0 = 1)
R = m
for i =1 to b-1
{
    R = R^2 mod n
    *if(d_i ==1) then R=R*m mod n (*)*
}
return R

pozn.: časová náročnost oprerace (*) vyzařuje informaci o bitu klíče d_i

Obr. 2.6: Algoritmus „*square and multiply*“.



Obr. 2.7: Čas průchodu algoritmem pro jednotlivé bity klíče d [6].

2.2.4 Chybový postranní kanál

Využití chybového postranního kanálu se ukázalo být velice efektivním způsobem útoku na kryptografické zařízení. Chybový postranní kanál je založený na chybových hlášeních a systémových selháních, kdy kryptografický modul musí komunikovat s okolím. V běžném provozu jsou tato hlášení nutná pro správnou funkci systému. V dalším případě může útočník tento stav vyvolat uměle, kdy postupným opakováním chybných požadavků dojde ke zjištění některých citlivých informací [2].

2.2.5 Optický postranní kanál

Hlavní myšlenka analýzy optického postranního kanálu je velice jednoduchá. Vychází z faktu, že jednou z nejpoužívanějších součástí integrovaných obvodů jsou tranzistory, jejichž fyzické stavy jsou reprezentovány jedním ze dvou logických stavů „0“ nebo „1“. Kdykoliv tranzistor změní svůj stav, část energie využité tranzistorem se uvolní prostřednictvím fotonů, které tranzistor emituje do svého okolí. Avšak využití kryptoanalýzy postranního kanálu tohoto typu je velice finančně nákladné, časově náročné a rovněž také velice obtížně proveditelné. Zařízení umožňující tuto analýzu se nazývá PICA a nachází se v několika málo laboratořích na světě [8].

2.2.6 Akustický postranní kanál

Vyskytuje se u většiny aplikací kryptografických systémů, kde se používá klávesnice pro zadávání citlivých údajů (bankomaty, klávesnice PC, klávesnice mobilního telefonu). Dále lze také využít analýzu akustického postranního kanálu například u tiskáren (tiskárny PINů a hesel).

2.2.7 Kleptografický postranní kanál

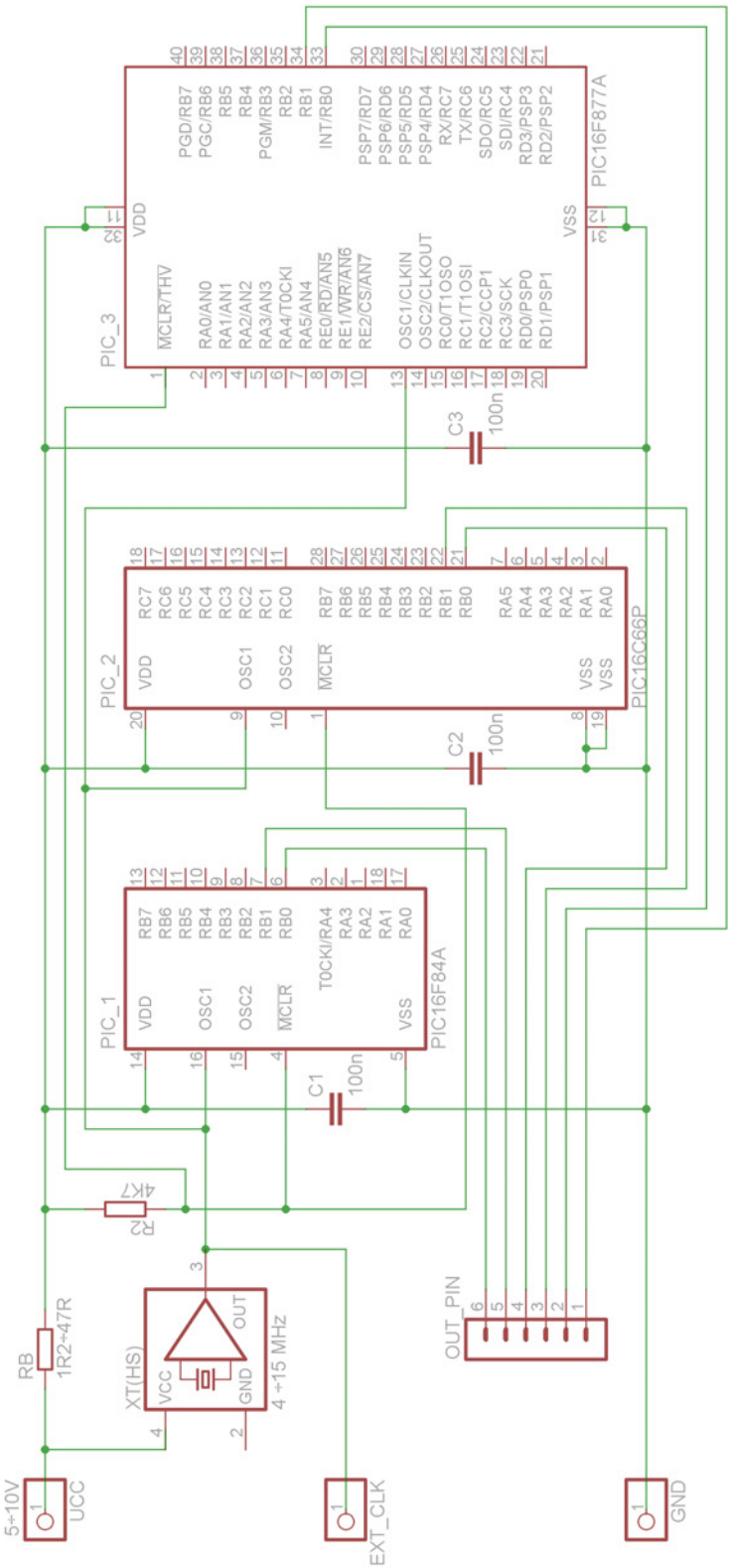
V tomto případě se jedná o zvláštní příklad postranního kanálu. Může být zařazen mezi tzv. podprahové kanály. Podprahový kanál je kanál, který je v kryptografickém modulu záměrně vytvořen útočníkem bez vědomí uživatele za účelem vynášení citlivých informací. Jedná se o informace, které jsou pod úrovní rozlišovací schopnosti daného modulu, protokolu, typu spojení atp. Problematika těchto kanálů je zatím poměrně nová, která se do budoucnosti stane velice diskutovanou podobně jako oblast elektromagnetických postranních kanálů [6].

3 PRACOVIŠTĚ A POSTUP MĚŘENÍ

Pro účely měření byl vytvořen návrh experimentální desky plošných spojů (DPS), která spolu s mikroprocesorem PIC představuje kryptografický modul, jenž bude podroben diferenční výkonové analýze v závislosti na různých podmínkách, nastavení a parametrech tohoto obvodu. V této části práce je především vysvětleno nastavení a postup pro měření výkonového postranního kanálu kryptografického modulu.

3.1 Experimentální DPS

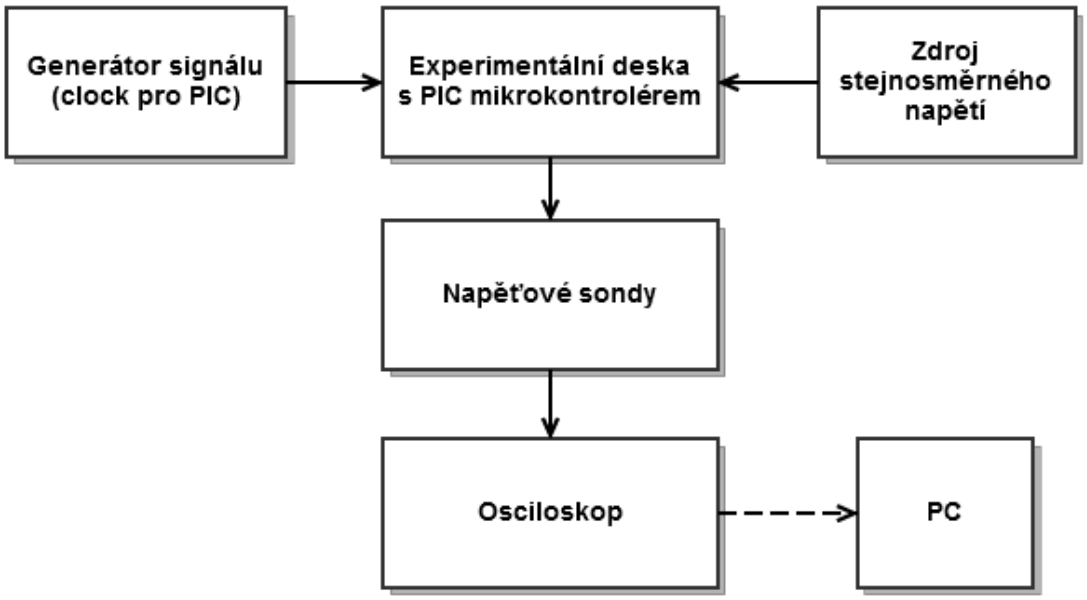
Na obrázku 3.1 je schéma DPS, která byla osazena pouze součástkami nezbytnými pro chod mikroprocesoru, třemi paticemi (18pinová, 28pinová, 40pinová), pro možnost měření na různých typech mikroprocesorů, a odporovým bočníkem R_B, který je zapojen v sérii mezi zdrojem stejnosměrného napětí U_{CC} a vstupem V_{DD} kryptografického modulu. V průběhu simulace útoku je deska vždy osazena pouze jediným mikroprocesorem. Útok je realizován měřením napětí na bočníku R_B pomocí napěťové sondy. Konektor pro měřený vstupní signál sondy je připojen mezi zdroj stejnosměrného napětí a vstup bočníku R_B. Zemnící konektor sondy je pak připojen mezi výstup bočníku a vstup V_{DD} mikroprocesoru. Změřený průběh napětí na bočníku je pak podle Ohmova zákona přímo úměrný protékajícímu proudu bočníkem. Měřené průběhy tedy budou zobrazeny jako závislost průběhu napětí v čase. Útok byl realizován pro různé velikosti napájecího napětí U_{CC}, pro odlišné takty hodinového signálu, pro různé velikosti odporu bočníku R_B, různé velikosti kapacit blokovacích kondenzátorů C_1 (C_2, C_3) a pro různou teplotu okolí. DPS proto byla v průběhu měření modifikována tak, že se osazovala součástkami různých velikostí hodnot. Kryptografický modul může být taktován buďto krystalovým oscilátorem XT (HS) nebo externě generátorem signálu připojeným na pin EXT_CLK. Součástka OUT_PIN je lišta s šesticí konektorů, na které jsou přivedeny výstupy mikroprocesoru RB0 a RB1 (pro každou patici). Na daném výstupu (RB0) je rovněž připojena sonda osciloskopu. Signál na tomto výstupu bude sloužit k synchronizaci signálu měřeného na bočníku R_B. Tento pseudo-hodinový signál bude generován kryptografickým modulem. Podrobněji bude vysvětleno dále.



Obr. 3.1: Schéma experimentální DPS.

3.2 Experimentální pracoviště

Na obrázku 3.2 je blokové schéma experimentálního pracoviště. Proces simulace útoku je bez přímé účasti PC. PC je použito především k implementaci šifrovacího algoritmu do kryptografického modulu a k následnému vyhodnocování výsledků naměřených osciloskopem.

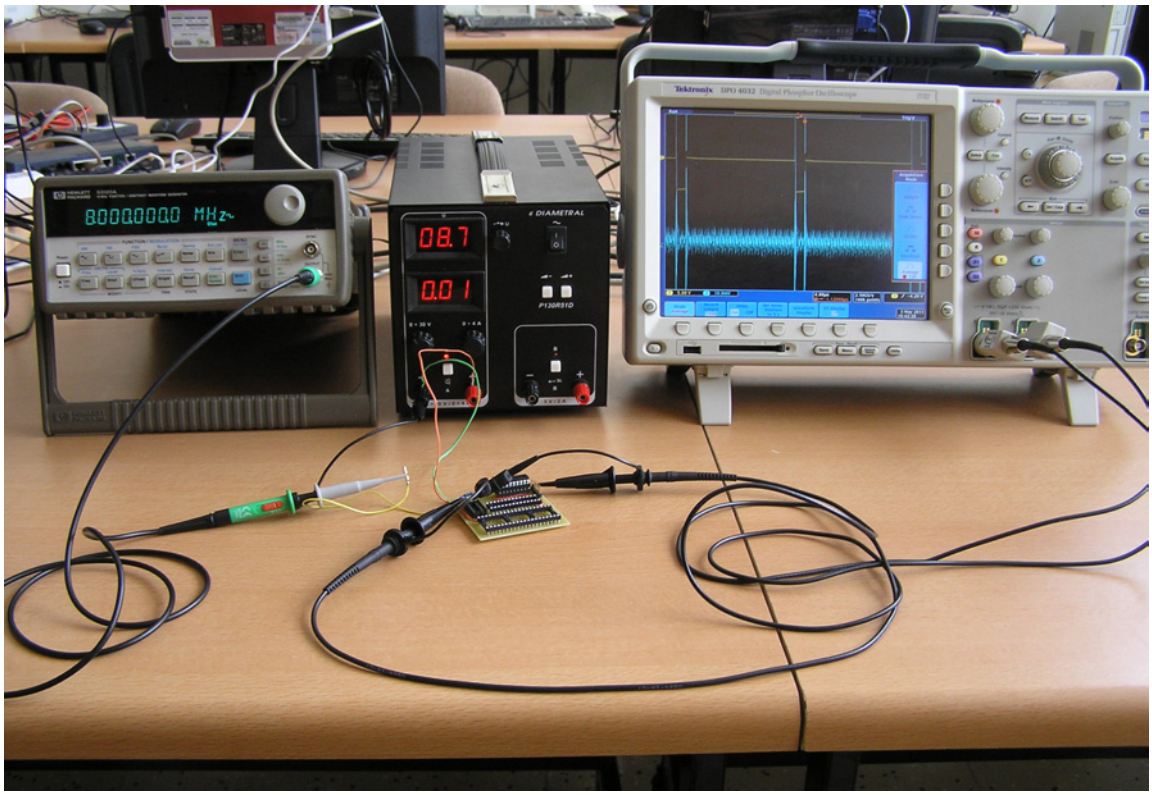


Obr. 3.2: Blokové schéma experimentálního pracoviště.

Seznam přístrojů a přípravků:

- Osciloskop Tektronix DPO4032 (vzorkovací frekvence 350MHz)
- Napěťové sondy Tek P6139A
- Generátor signálu Hewlett Packard 33120A
- Laboratorní zdroj P130R51D
- Programovatelná deska Microchip PICDEM 2 PLUS board
- Debugger Microchip MPLAB ICD 2
- Mikroprocesor PIC16F84A
- Mikroprocesor PIC16F877A
- Přípravek pro měření napětí na bočníku
- PC s programovým prostředím MPLAB IDE v8.63 a MATLAB

Implementace šifrovacího algoritmu se uskutečňuje pomocí programovatelné desky, která je osazena mikroprocesorem, jenž bude plnit funkci kryptografického modulu. Tato deska je připojena k PC přes debugger a komunikuje s programovým prostředím MPLAB. Po úspěšné implementaci je PIC z programovatelné desky přepojen do experimentální DPS. Jeden kanál osciloskopu je poté připojen na bočník. Druhý kanál je pak použit pro synchronizaci, kdy sonda tohoto kanálu je připojena na výstup RB0 (pin 6, pin 4 nebo pin 2 na konektoru OUT_PIN).

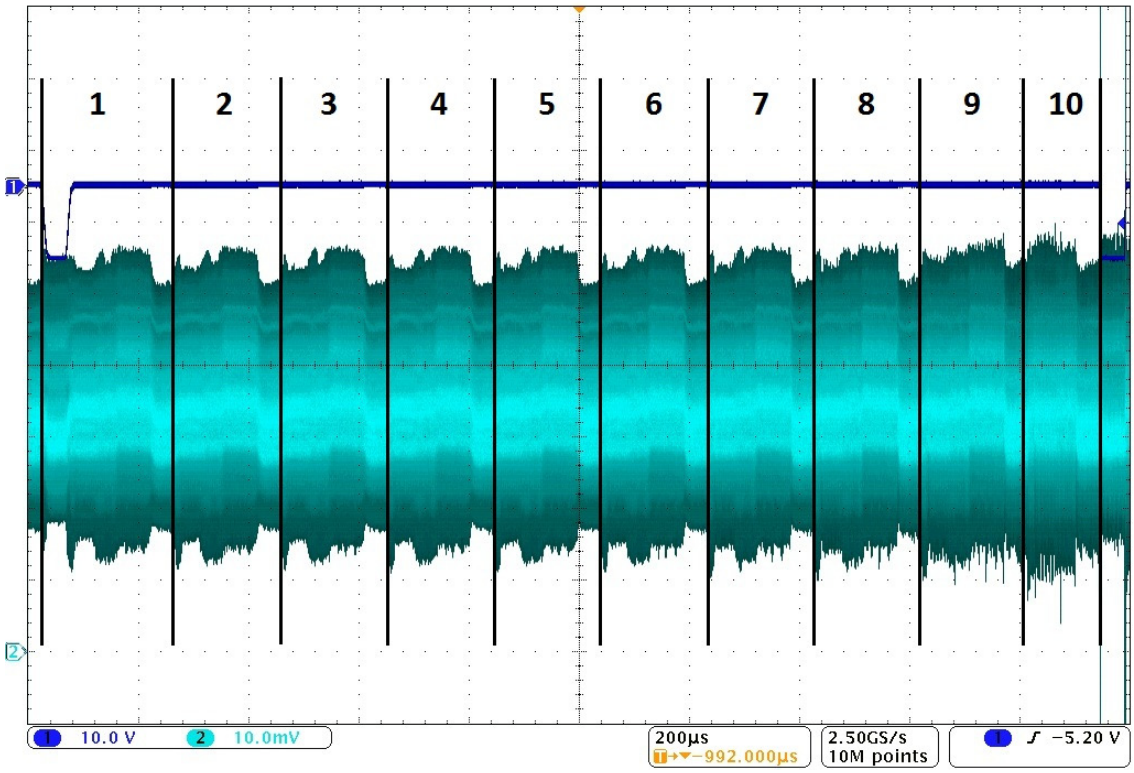


Obr. 3.3: Realizace experimentálního pracoviště.

Na osciloskopu bylo nastaveno průměrování a počet vzorků pro průměrování byl nastaven na 128. Pomocí módu průměrování se redukuje úroveň šumu a odstraní se další nahodilosti z vykreslované závislosti. Zvolený počet vzorků, které se průměrují, by neměl být příliš velký. V případě nevhodné volby dochází k nežádoucímu zkreslení zobrazovaného průběhu, což má za následek znehodnocení měřené závislosti. Atenuační faktor sond byl 1:10, proto byl potřeba upravit na osciloskopu násobitel zobrazení na hodnotu 10×, aby došlo ke shodě zobrazované hodnoty napětí s reálnou hodnotou na vstupu sondy. Na obrázku 3.3 je použit pro taktování mikroprocesoru generátor signálu. Generovaný průběh je obdélníkový se střídou 50%.

3.2.1 Implementace šifrovacího algoritmu

Ve své původní podobě pracuje AES algoritmus s bloky dat o délce 128 bitů jak pro otevřený text, tak i pro tajný klíč. AES šifra pro délku klíče o 128 bitech zpracovává bloky otevřeného textu v deseti rundách (viz tab. 1.1). Na obrázku 3.4 je vidět průběh napětí na bočníku R_B při šifrování dat, které jsou spolu s klíčem uloženy přímo na čipu v paměti dat. V průběhu jsou vyznačeny jednotlivé rundy. První runda, inicializační, je nejdelší, jelikož hned v úvodu se navíc provádí operace *AddRoundKey*, kdy se uskutečňuje exkluzivní součet otevřeného textu přímo s hodnotami tajného klíče. Následuje 8 rund, ve kterých se operace *AddRoundKey* provádí nad blokem otevřeného textu a rundovního klíče. V poslední rundě se vynechává operace *MixColumn* (vývojový digram na obrázku 1.3).



Obr. 3.4: Průběh napětí na bočníku pro jeden šifrovací cyklus AES.

Do mikroprocesoru byl pro účely měření implementován program pracující s modifikovaným algoritmem AES. Jedná se o část původního algoritmu, kdy mikroprocesor bude cyklicky provádět pouze operaci *AddRoundKey* nad blokem otevřeného textu a blokem tajného klíče. Na obrázku 3.4 v okně rundy 1 se jedná o průběh napětí na druhém kanálu osciloskopu v době trvání logické úrovně 0 na vstupu prvního kanálu osciloskopu (log. 0 = $-U_{CC}$, log. 1 = 0 V). Měření každého průběhu

je provedeno ve dvou fázích. Ty se liší pouze v hodnotách použitého tajného klíče, s kterými funkce *AddRoundKey* pracuje. V obou případech je matice otevřeného textu nulová (tzn. každé slovo má hodnotu 00h). V první fázi je matice tajného klíče nulová. V druhé fázi pak tato matice nabývá hodnot od 01h po FFh, kdy Hammingova váha w prvku následujícího je vždy větší o 1 oproti prvku předchozímu. Hodnota prvního slova klíče $k_{0,0}$ je tedy rovna 01h. Následující prvek v matici má hodnotu 03h, $w(k_{0,1}) = 2$. Prvek $k_{1,3}$ pak nabývá hodnoty FFh, $w(k_{1,3}) = 8$. Prvek $k_{2,0}$ má hodnotu 01h a následující prvky mají opět w vždy větší o 1 oproti hodnotě prvku předchozího. Matice **A** otevřeného textu, matice **K** tajného klíče a výsledná matice **B** tedy budou vypadat následovně (hexadecimální zápis):

1. fáze:

$$\mathbf{A} = \begin{pmatrix} 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{pmatrix}, \mathbf{K} = \begin{pmatrix} 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{pmatrix},$$

$$\mathbf{B} = \begin{pmatrix} 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{pmatrix}.$$

2. fáze:

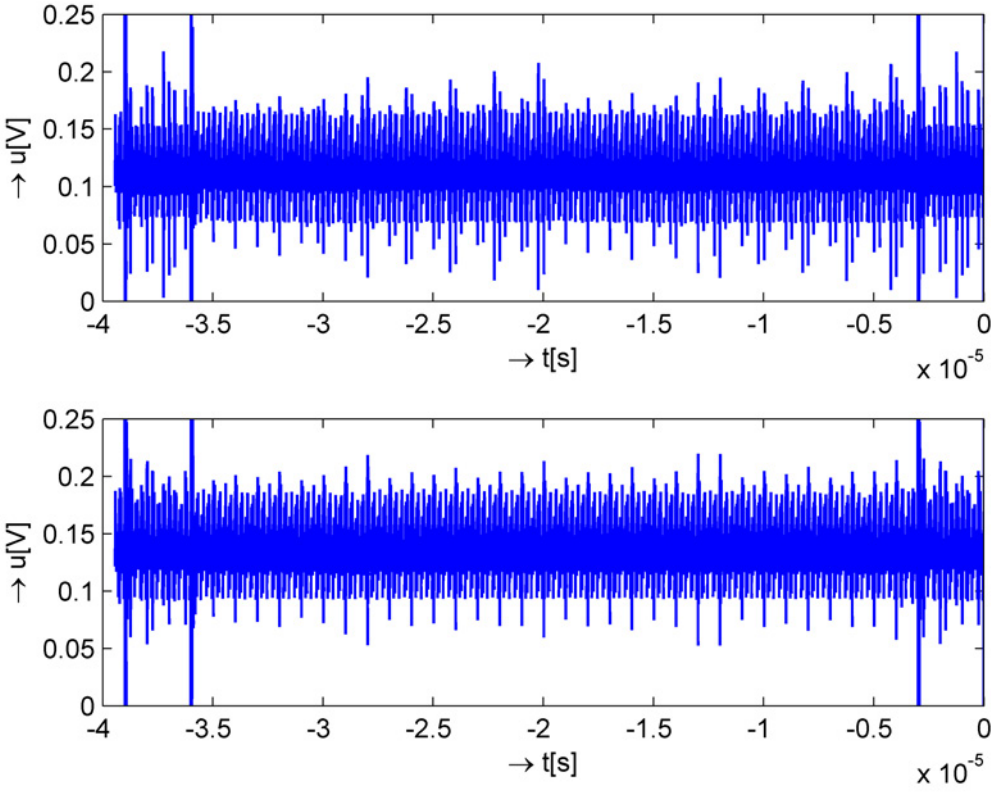
$$\mathbf{A} = \begin{pmatrix} 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{pmatrix}, \mathbf{K} = \begin{pmatrix} 01 & 03 & 07 & 0F \\ 1F & 3F & 7F & FF \\ 01 & 03 & 07 & 0F \\ 1F & 3F & 7F & FF \end{pmatrix},$$

$$\mathbf{B} = \begin{pmatrix} 01 & 03 & 07 & 0F \\ 1F & 3F & 7F & FF \\ 01 & 03 & 07 & 0F \\ 1F & 3F & 7F & FF \end{pmatrix}.$$

Funkce *AddRoundKey*:

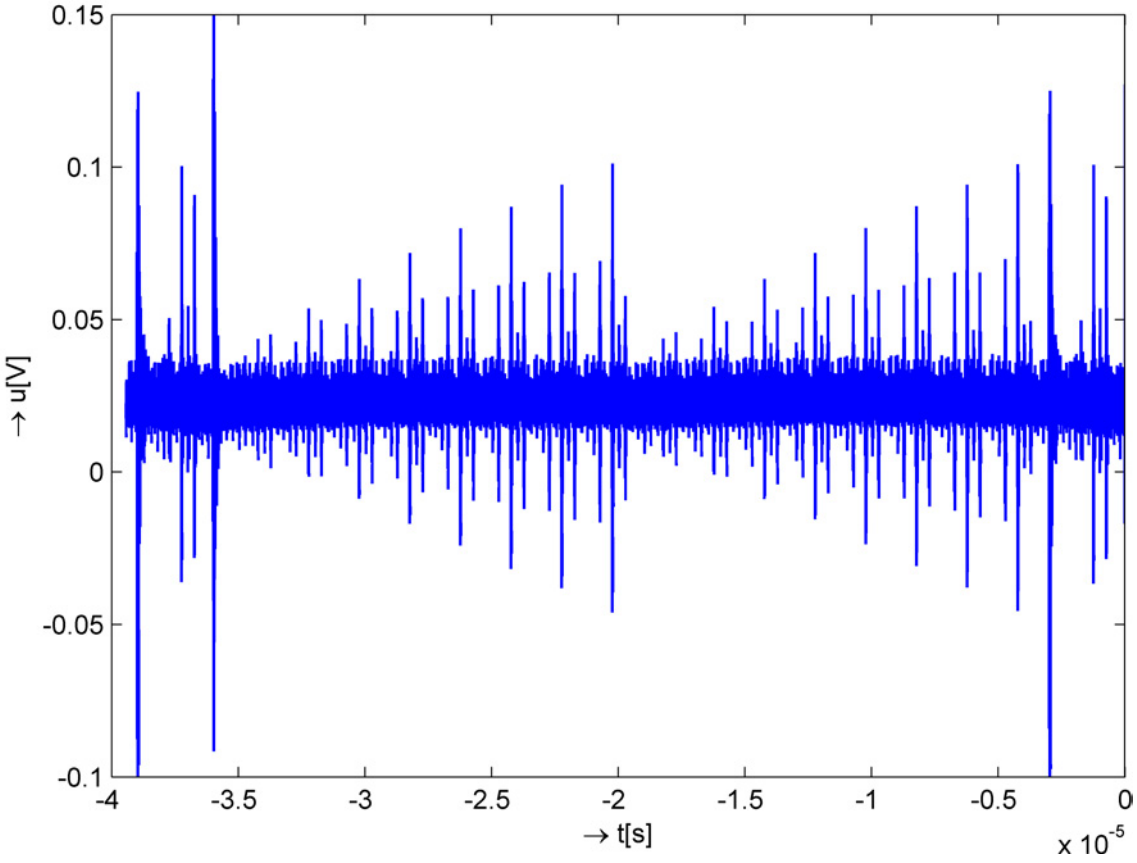
$$\begin{aligned} [b_{0,0}, b_{1,0}, b_{2,0}, b_{3,0}] &= [a_{0,0}, a_{1,0}, a_{2,0}, a_{3,0}] \oplus [k_{0,0}, k_{1,0}, k_{2,0}, k_{3,0}], \\ &\vdots \\ [b_{0,3}, b_{1,3}, b_{2,3}, b_{3,3}] &= [a_{0,3}, a_{1,3}, a_{2,3}, a_{3,3}] \oplus [k_{0,3}, k_{1,3}, k_{2,3}, k_{3,3}]. \end{aligned} \tag{3.1}$$

V první fázi jsou do kryptografického modulu uložena data otevřeného textu, nulová matice **A**, a data klíče, nulová matice **K**. Průběh napětí na bočníku je osciloskopem zaznamenán. V druhé fázi jsou do kryptografického modulu uložena data otevřeného textu, nulová matice **A**, a data klíče, nenulová matice **K**. Průběh je opět zaznamenán osciloskopem. Měřené průběhy z těchto dvou fází se poté zpracují v programu Matlab. Výsledný průběh se následně vypočte prostým rozdílem průběhů napětí z těchto dvou fází, tzn. průběh napětí z první fáze (horní graf na obrázku 3.5) se odečte od průběhu napětí z druhé fáze (spodní graf na obrázku 3.5).



Obr. 3.5: Napětí na bočníku v 1. a 2. fázi měření.

Tímto se získá výkonová spotřeba v závislosti na Hammingově váze slov, s kterými pracuje funkce *AddRoundKey*. Na obrázku 3.6 je pak zobrazen výsledný průběh (rozdíl průběhu z 1. a 2. fáze).



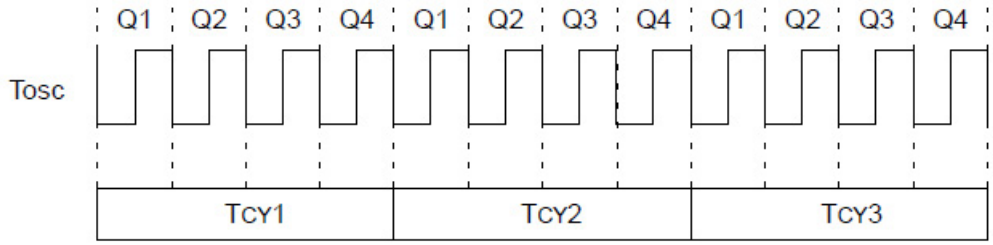
Obr. 3.6: Výsledný průběh diferenčního signálu (napětí).

3.3 Princip vykonávání instrukcí mikroprocesoru

Pro následnou analýzu získaných průběhů proudového odběru (napětí) mikroprocesoru je nutné pochopit princip taktování jeho vnitřních obvodů a princip vykonávání instrukcí.

3.3.1 Schéma vnitřního taktování

Každý instrukční cyklus T_{CY} se skládá ze čtyř hodinových cyklů vnějšího taktovacího obvodu (XT, HS nebo EXT_CLK). Tento vstupní hodinový signál (na vstupu OSC1) je přiveden na děličku hodinového signálu, kdy jsou z původního hodinového signálu vytvořeny čtyři dílčí navzájem se nepřekrývající hodinové signály Q1, Q2, Q3 a Q4. Jejich součet pak tvoří interní hodinový signál T_{OSC} (obr. 3.7) [12].



Obr. 3.7: Vztah mezi instrukčním cyklem a vnitřním hodinovým signálem.

3.3.2 Schéma zpracování instrukcí

Hodinové cykly Q poskytují časování pro vykonávání čtyř dílčích operací:

- Q1 - cyklus dekódování instrukce,
- Q2 - cyklus načtení dat (operandů),
- Q3 - cyklus zpracování dat,
- Q4 - cyklus zápisu dat.

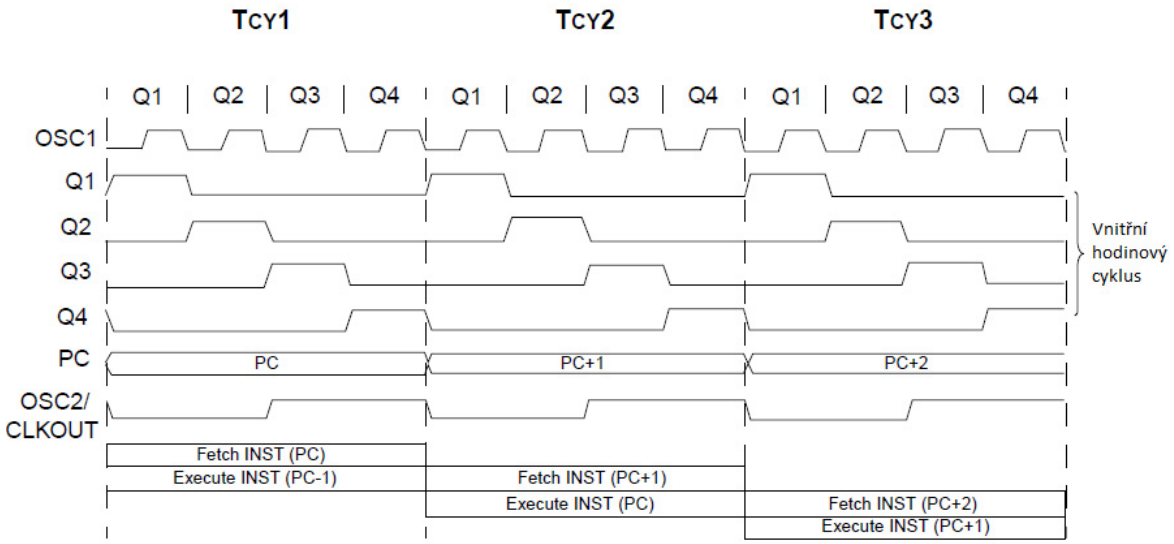
Architektura mikroprocesorů PIC využívá technologie „*pipelining*“ (tj. zřetězené zpracování, či překrývání strojových instrukcí). Princip této technologie spočívá v paralelním zpracování instrukcí (jsou zpracovávány vždy dvě instrukce během dvou instrukčních cyklů). Programový čítač (Program Counter – PC) mikroprocesoru pak obsahuje adresu instrukce PC, která se bude vykonávat v následujícím instrukčním cyklu. Programový čítač je inkrementován každou nástupní hranou Q1. Během doby trvání jednoho instrukčního cyklu proběhne načtení instrukce (Fetch) na adrese PC+1 a vykonání instrukce (Execute) ležící na adrese PC (obr. 3.8).

Z výše uvedeného tedy vyplývá, že vykonání jedné instrukce vyžaduje nejméně dva instrukční cykly, avšak díky využití zřetězení instrukcí se v podstatě jedna instrukce vykoná za dobu trvání jednoho instrukčního cyklu [12].

Doba trvání instrukčního cyklu

Jeden instrukční cyklus tedy trvá 4 takty hodinového signálu na vstupu OSC1. Doba trvání instrukčního cyklu pro $f_{\mathrm{OSC1}} = 4\,\mathrm{MHz}$ je

$$T_{CY} = 4\frac{1}{f_{OSC1}} = 4\frac{1}{4 \cdot 10^{-6}} = 1\,\mu s. \tag{3.2}$$



Obr. 3.8: Vykonávání instrukcí založené na architektuře „*pipelining*“.

Tab. 3.1: Doba trvání 1 instrukčního cyklu.

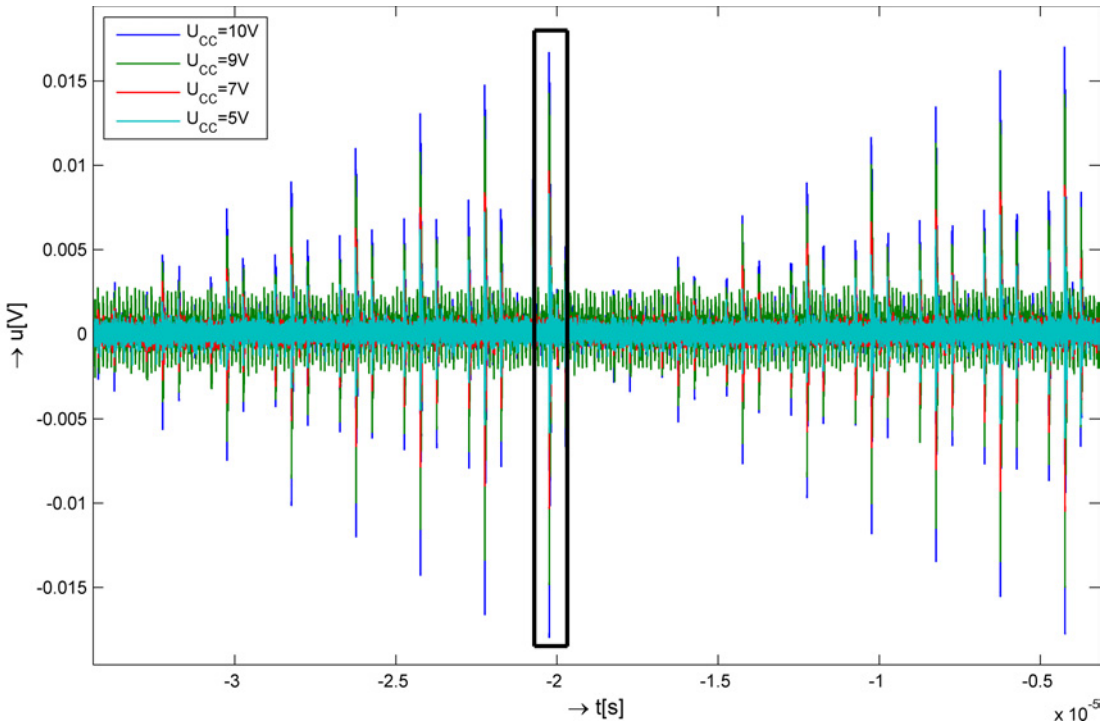
f_{OSC1} [MHz]	4	8	15
T_{CY} [μs]	1	0,5	0,27

4 MĚŘENÍ

Měření proudového odběru je realizováno jako série měření, kdy se zjišťuje průběh napětí na bočníku R_B v závislosti na velikosti napájecího napětí U_{CC}, na taktu vnějšího hodinového signálu f_{OSC1}, na velikosti odporu R_B, na velikosti blokovacího kondenzátoru C_1 (případně C_2, C_3) a na teplotě okolí t_O. Pro většinu měření je jako kryptografického modulu použito mikroprocesoru PIC16F84A, případně PIC16F877A.

4.1 Vliv napájecího napětí

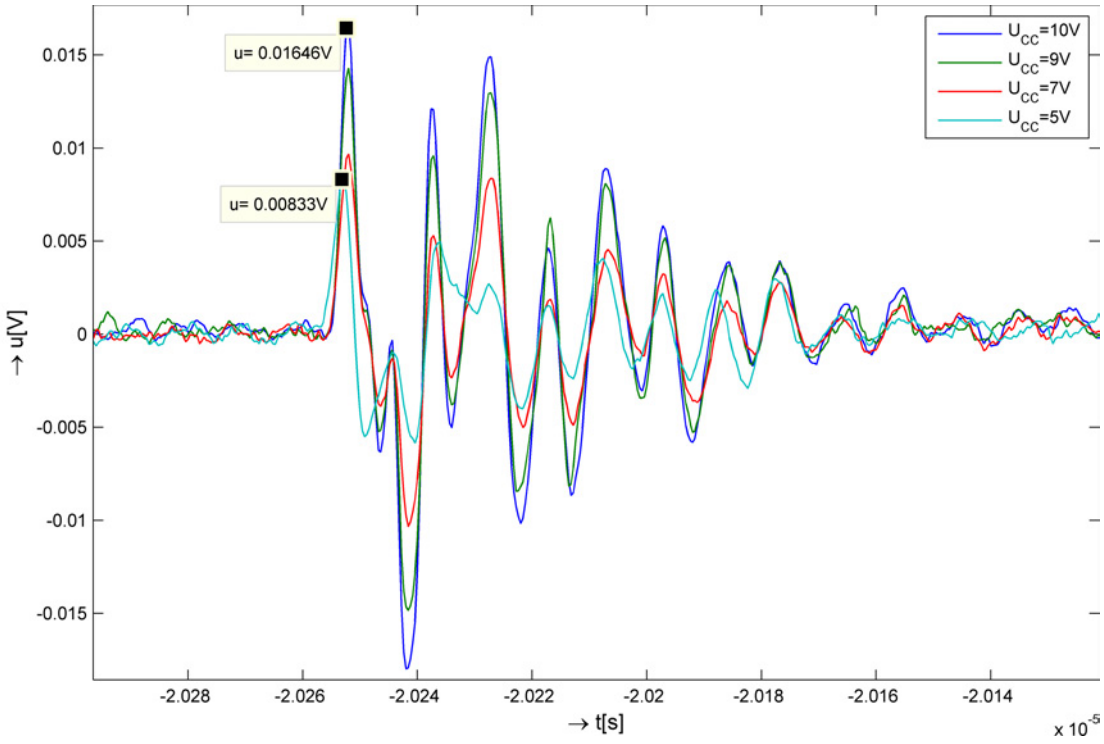
V grafu na obrázku 4.1 jsou zobrazeny průběhy závislosti napětí na bočníku R_B pro různé hodnoty napájecího napětí U_{CC}. Hodnoty byly naměřeny pro odpor bočníku $R_B = 1\,\Omega$, frekvenci hodinového signálu $f_{OSC1} = 4\,\text{MHz}$, $C_1 = 100\,\text{nF}$.



Obr. 4.1: Závislost napětí na bočníku pro různá napájecí napětí.

S rostoucím napětím U_{CC} narůstá hodnota proudu odebíraného mikroprocesorem. Tento proud je přímo úměrný napětí na bočníku. Na obrázku 4.2 je zobrazený průběh napětí ve výřezu z grafu na obrázku 4.1 (černý obdélník). Tyto napěťové špičky vznikají při operaci XOR mezi slovy 00h a FFh. Pro $U_{CC} = 5\,\text{V}$ je velikost

diference napětí na bočníku oproti hodnotě ustálené přibližně 8 mV. Pro U_{CC}= 10 V je tato diference dvojnásobná, tj. 16 mV.



Obr. 4.2: Diference napětí na bočníku oproti napětí ustálenému.

4.2 Vliv frekvence hodinového signálu

V obrázku 4.3 jsou zobrazeny průběhy závislosti napětí na bočníku R_B pro odlišný takt hodinového signálu na vstupu OSC1 mikroprocesoru. Hodnoty byly naměřeny pro odpor bočníku R_B= 1 Ω, napájecí napětí U_{CC}= 10 V a kapacitu blokovacího kondenzátoru C_1= 100 nF. Frekvence hodinového signálu f_{OSC1} byly 4, 8 a 15 MHz. Funkce *AddRoundKey* je tvořena celkem 35 instrukcemi, kdy 34 instrukcí vyžaduje pro vykonání každé z nich jeden instrukční cyklus a jedna instrukce, instrukce skoku *goto*, vyžaduje dva instrukční cykly. V následující tabulce je doba T_{ARK} potřebná pro vykonání funkce *AddRoundKey* (36 instrukčních cyklů) pro různé takty oscilátoru:

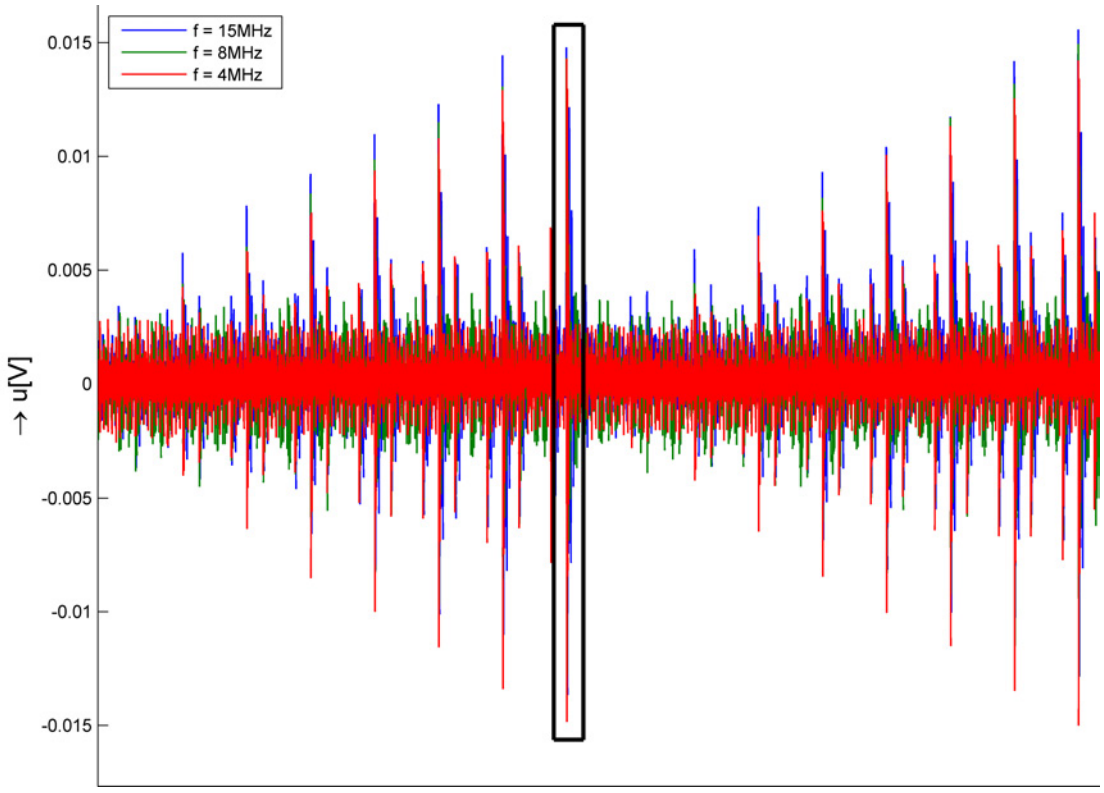
Tab. 4.1: Doba trvání vykonání *AddRoundKey*.

f_{OSC1} [MHz]	4	8	15
T_{ARK} [μs]	36	13	9,6

V hodnotách amplitudy napětí (Peak-to-Peak) na obrázku 4.4 je minimální rozdíl. S rostoucí frekvencí se ovšem zvýrazňuje oscilace napěťového signálu na bočníku, což je pro analýzu signálu nežádoucí, jelikož to vnáší jistou míru nepřesnosti. Z hlediska bezpečnosti je proto výhodnější použití oscilátoru s vyšším taktem. Navíc při vyšším taktu se snižuje kvalita měření osciloskopem, resp. se zmenšuje hodnota poměru dle vzorce

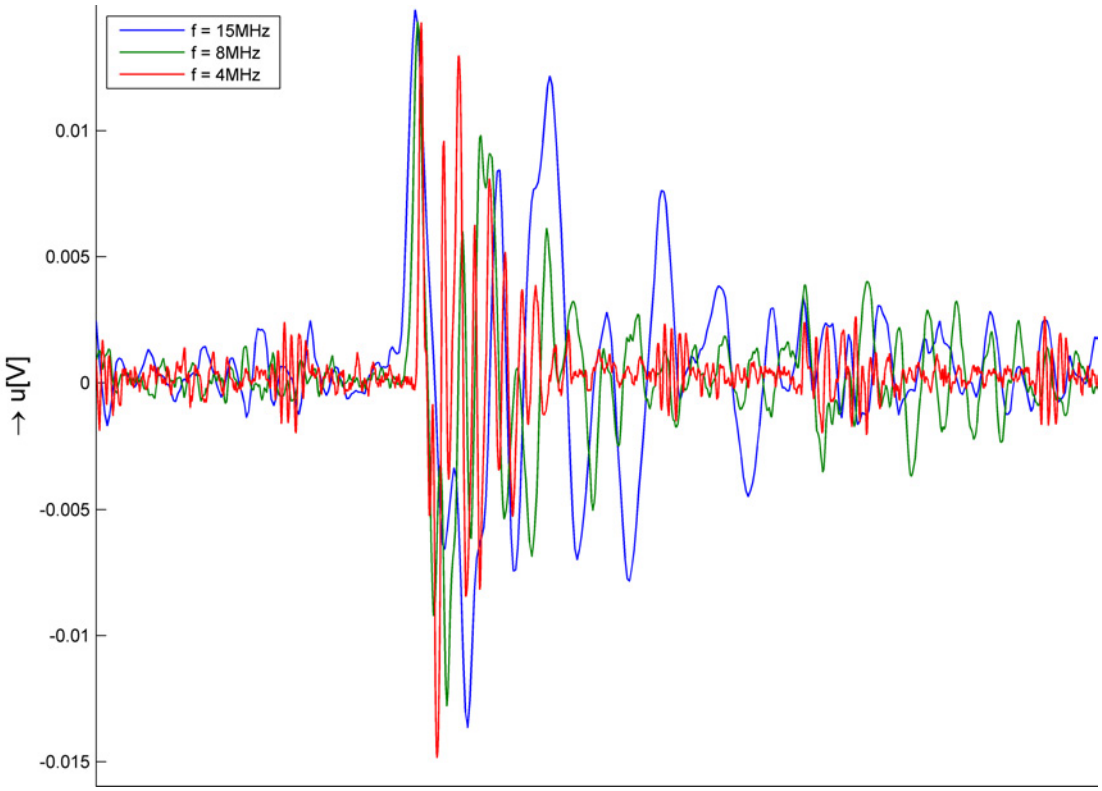
$$\frac{f_{VZ}}{f_{OSC1}} \geq 2, \tag{4.1}$$

kde f_{VZ} je vzorkovací frekvence osciloskopu a f_{OSC1} je frekvence na vstupu OSC1 mikroprocesoru. Rovnice tohoto poměru vychází z Nyquistova teorému. Se vzrůstající hodnotou frekvence f_{OSC1} vzorkovací schopnost osciloskopu klesá. V ideálním případě by pro zvýšení bezpečnosti bylo výhodné použití takové frekvence taktu hodinového signálu, která by při analýze útočníkem způsobovala aliasing rekonstruovaného signálu.



Obr. 4.3: Peak-to-Peak hodnoty napětí pro různé takty hod. signálu.

Na obrázku 4.4 je detail okna z obrázku 4.3, kde jsou vidět výraznější přechody mezi stavy vnitřních obvodů mikroprocesoru pro nižší frekvence f_{OSC1}.

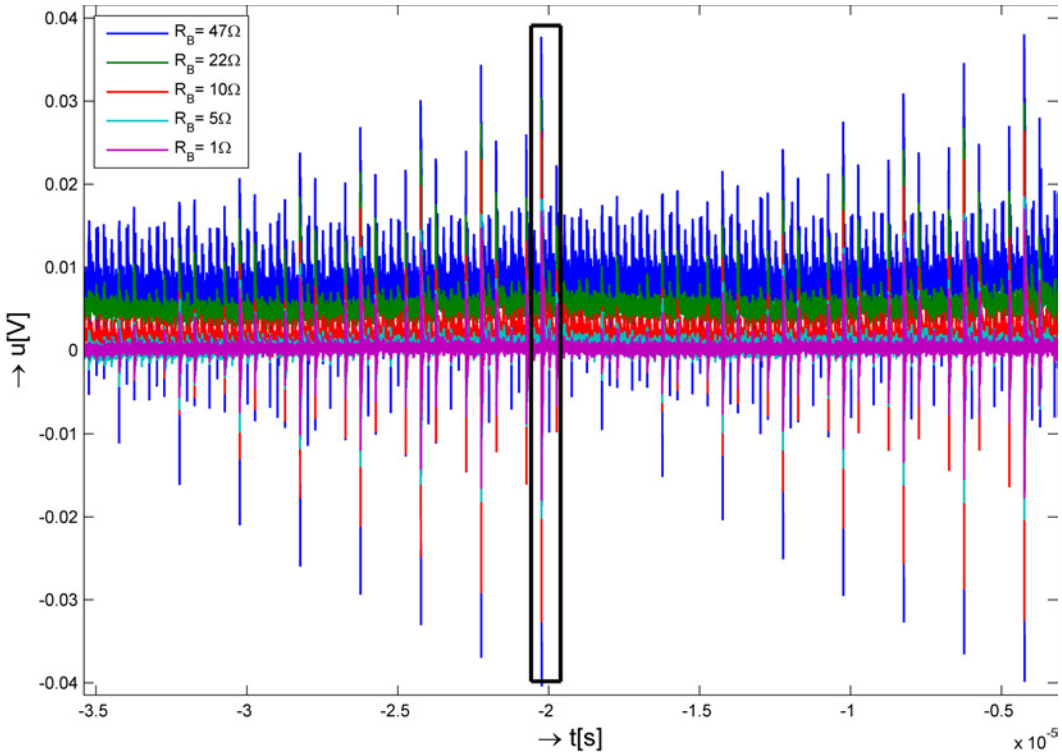


Obr. 4.4: Detail Peak-to-Peak hodnot napětí pro různé takty hod. signálu.

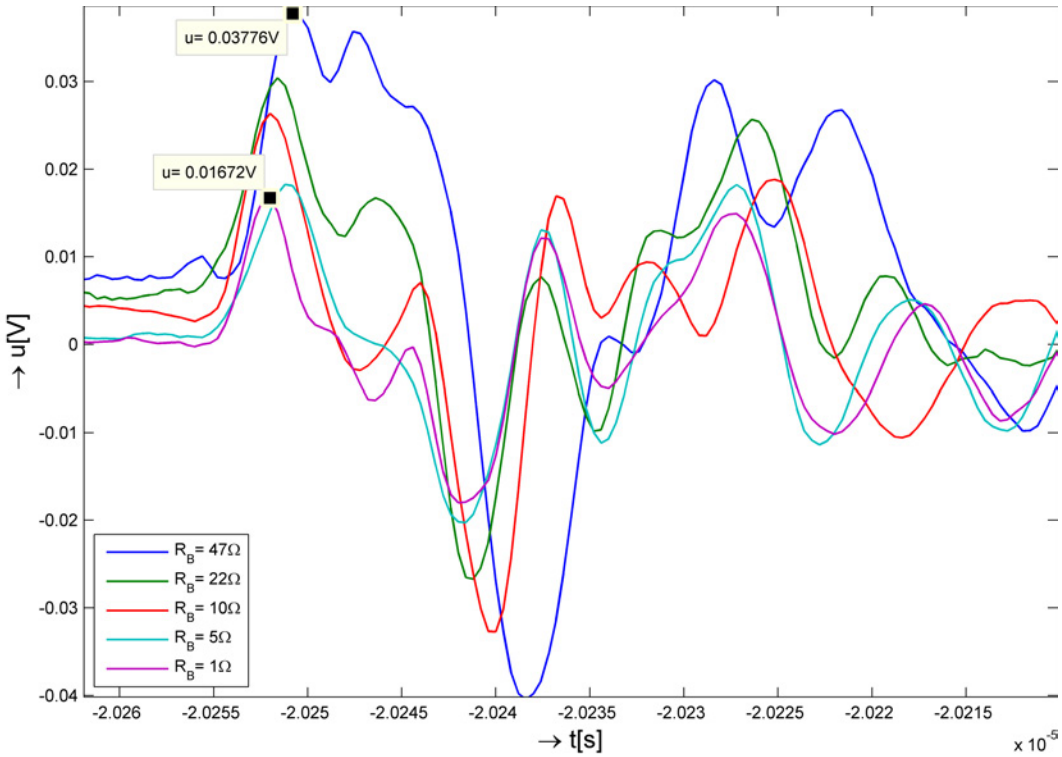
4.3 Vliv odporu bočníku

V grafu na obrázku 4.5 jsou zobrazeny průběhy závislosti napětí na bočníku R_B pro různé hodnoty velikosti odporu. Hodnoty byly naměřeny pro napájecí napětí U_{CC}= 10 V, frekvenci hodinového signálu f_{OSC1}= 4 MHz a kapacitu blokovacího kondenzátoru C_1= 100 nF.

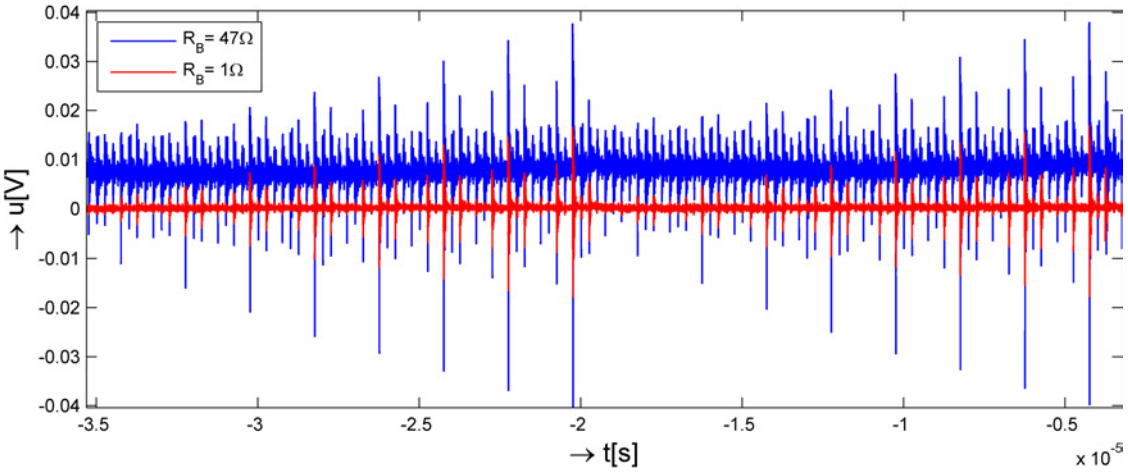
Z grafu na obrázku 4.5 je patrné, že se vzrůstajícím odporem bočníku se zvyšuje Peak-to-Peak hodnota diferenčního signálu na bočníku. Přechody ze stavu log. 1 do log. 0 jsou sice výraznější, avšak klesá hodnota poměru S/N (Signal-to-Noise Ratio), tj. poměr užitečného signálu a signálu šumu, viz obr. 4.7. Pro R_B= 1 Ω je amplituda diferenčního signálu U= 0,01672 V a pro R_B= 47 Ω je amplituda diferenčního signálu U= 0,03776 V (obr. 4.6).



Obr. 4.5: Závislost napětí na bočníku pro různé velikosti odporu bočníku.



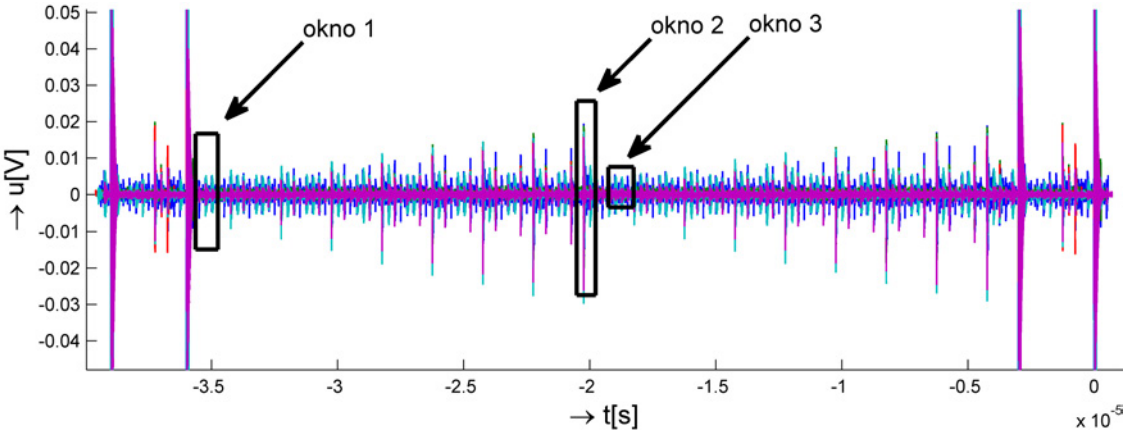
Obr. 4.6: Detail Peak-to-Peak hodnot napětí pro různé velikosti odporu bočníku.



Obr. 4.7: Srovnání průběhů diferenčního signálu pro R_{B}= 1 Ω a R_{B}= 47 Ω.

4.4 Vliv kapacity blokovacího kondenzátoru

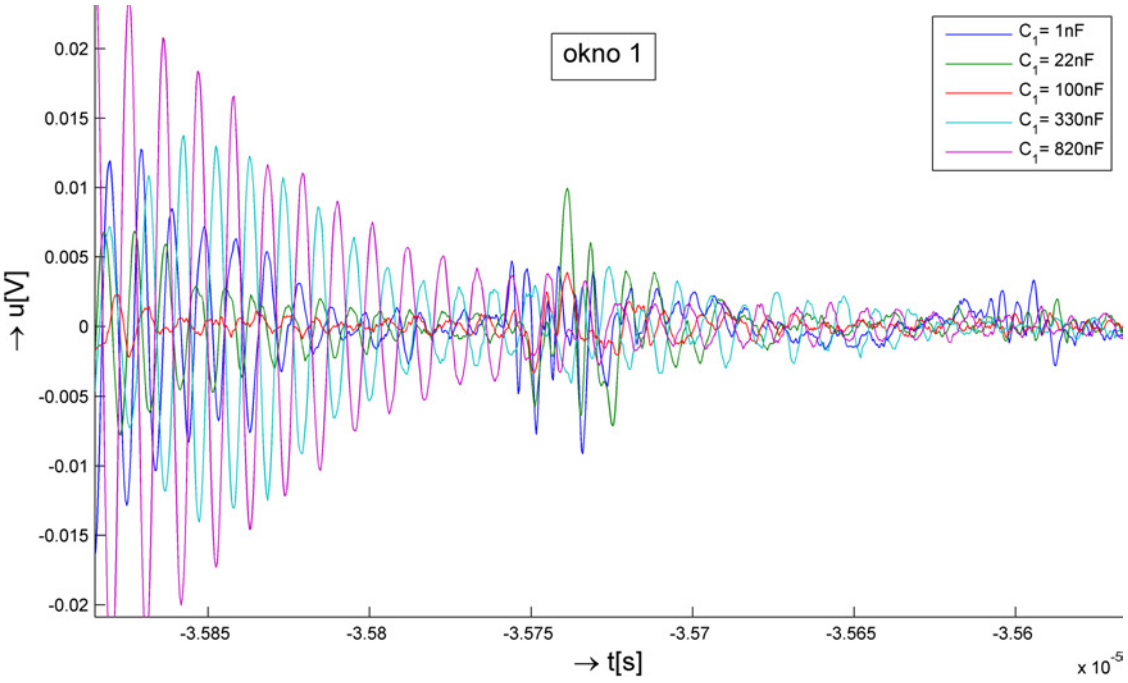
V grafu na obrázku 4.8 jsou zobrazeny průběhy závislostí napětí na bočníku $\mathrm{R_B}$ pro různé hodnoty kapacity blokovacího kondenzátoru $\mathrm{C_1}$. Hodnoty byly naměřeny pro napájecí napětí U_{CC}= 10 V, frekvenci hodinového signálu f_{OSC1}= 4 MHz a odpor bočníku R_{B}= 1 Ω. Kapacity blokovacího kondenzátoru $\mathrm{C_1}$ byly v hodnotách 1, 22, 100, 330 a 820 nF. Doporučená hodnota kapacity C_1= 100 nF (dle manuálových stránek PIC16F84A).



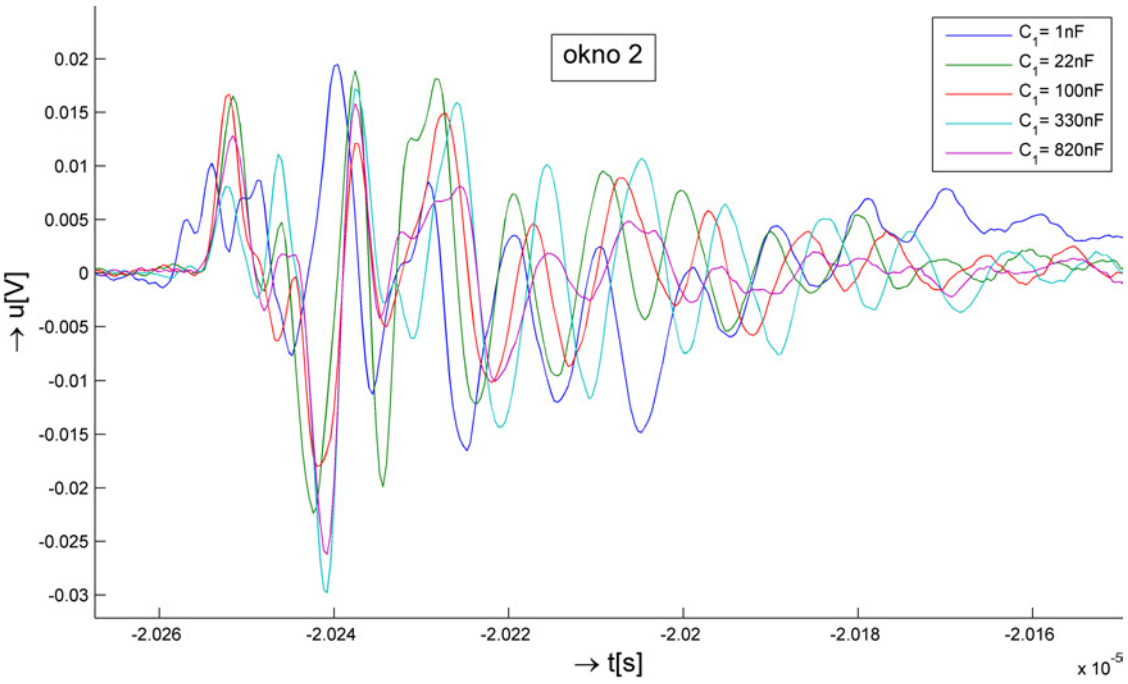
Obr. 4.8: Oblasti analýzy vlivu velikosti kapacity.

Okno 1 zobrazuje průběh diferenčního signálu po vykonání instrukce *bsf* RB0. Pin RB0 mikroprocesoru se nastaví na hodnotu log. 1 (napájecí napětí mikroprocesoru), což je doprovázeno vysokou napěťovou špičkou v průběhu diferenčního signálu.

Pro velikost kapacity výrazně vyšší 100 nF je patrná výrazná oscilace signálu. Stejně tak to platí pro hodnoty nižší.

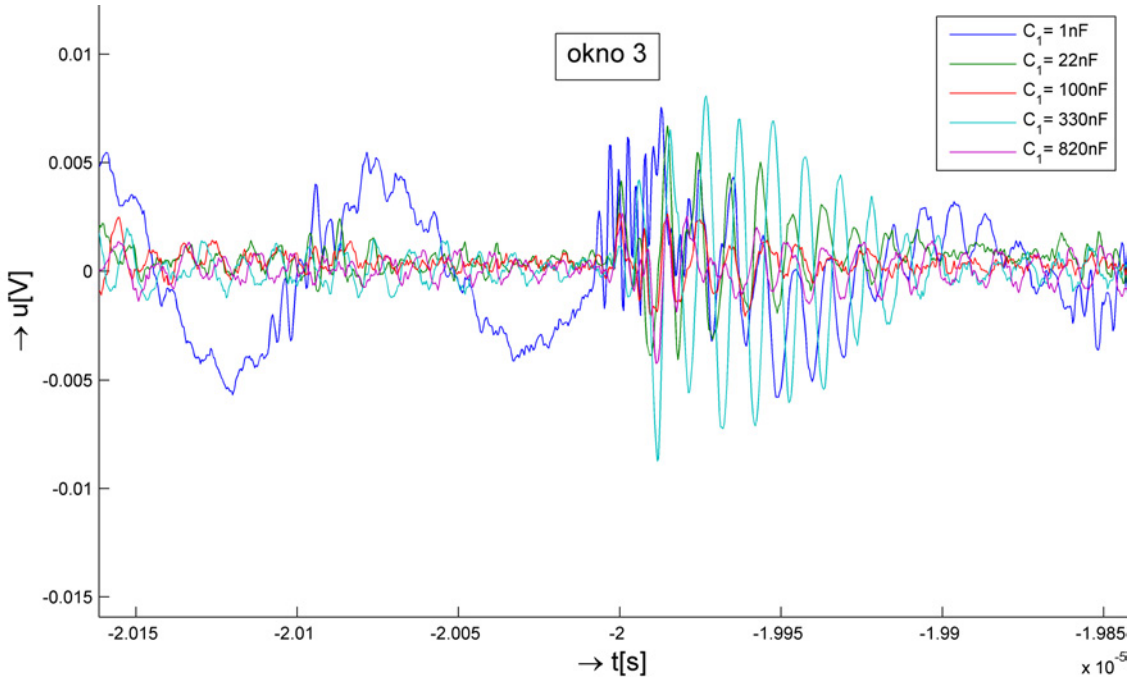


Obr. 4.9: Detail okna 1.



Obr. 4.10: Detail okna 2.

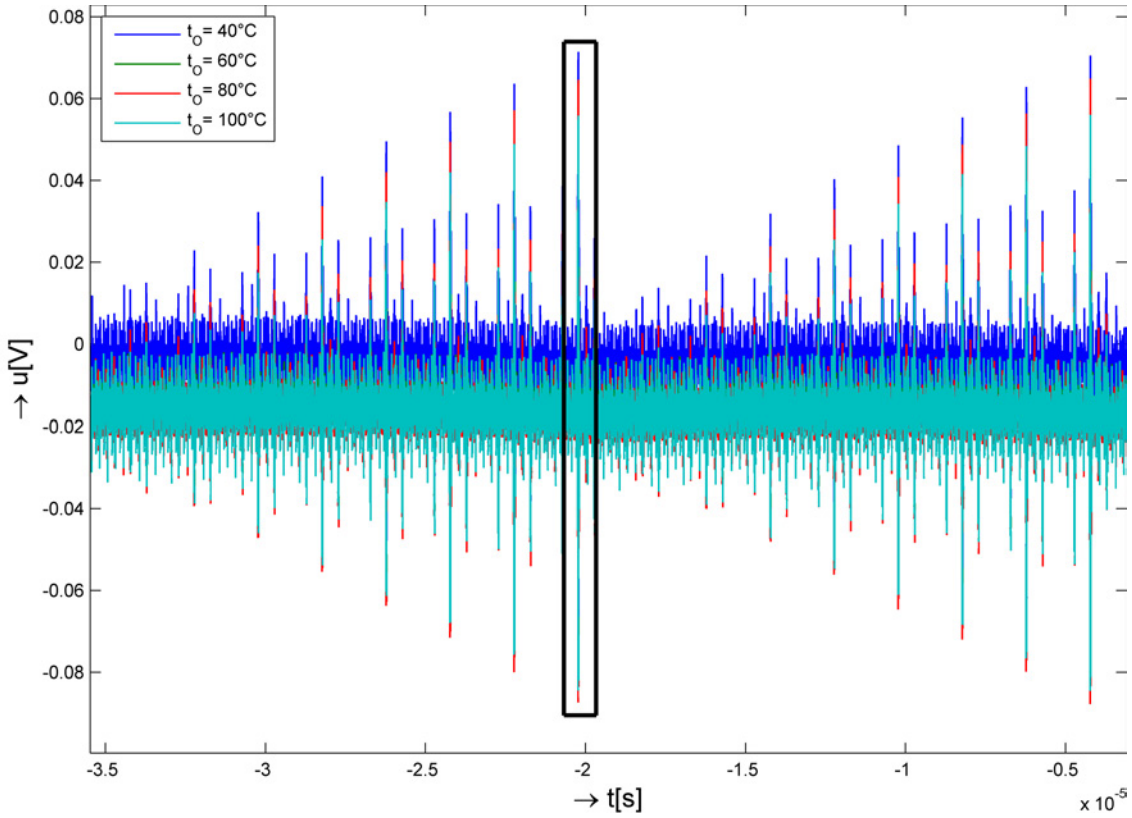
V detailu okna 2 a okna 3 (obr. 4.10 a obr. 4.11) je výrazná oscilace signálu při $C_1 = 1\,\text{nF}$. Volba této hodnoty je ovšem z konstrukčního hlediska naprosto nevhodná, i když z hlediska obrany proti kryptoanalýze se může jevit jako logická. Je spíše vhodné a taky se doporučuje použití vyšších hodnot kapacit blokovacích kondenzátorů. Neméně důležitým aspektem u kondenzátorů je také technologie výroby, resp. použitý materiál. Proto se mohou závislosti lišit pro různé typy kondenzátorů.



Obr. 4.11: Detail okna 3.

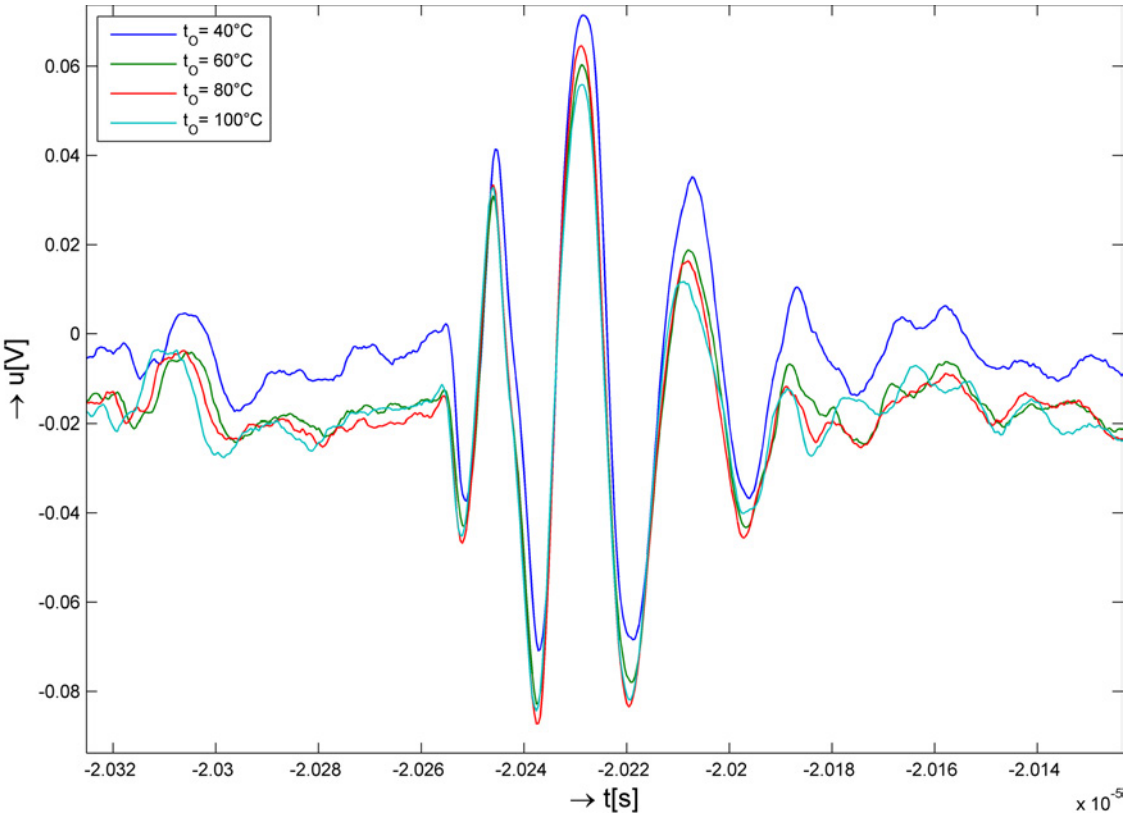
4.5 Vliv teploty okolí

V grafu na obrázku 4.12 jsou zobrazeny průběhy závislosti napětí na bočníku R_B pro odlišné teploty okolí t_O. Hodnoty byly naměřeny pro napájecí napětí $U_\text{CC} = 10\,\text{V}$, frekvenci hodinového signálu $f_\text{OSC1} = 4\,\text{MHz}$, odpor bočníku $R_\text{B} = 47\,\Omega$, kapacitu blokovacího kondenzátoru $C_1 = 100\,\text{nF}$. Typ použitého mikroprocesoru pro měření je PIC16F84A -04I/P, který spadá do řady průmyslových mikroprocesorů. Dle manuálových stránek je pracovní teplota t_A pro tento typ PIC v rozsahu $-40\,^\circ\text{C} \leq t_A \geq +85\,^\circ\text{C}$. Rozmezí teploty okolí t_O potom může nabývat hodnot $-55\,^\circ\text{C} \leq t_O \geq +125\,^\circ\text{C}$. Měření průběhu diferenčních signálu se uskutečňovalo pro teploty v rozsahu od $+40\,^\circ\text{C}$ do $+100\,^\circ\text{C}$.



Obr. 4.12: Závislost napětí na bočníku pro různé teploty okolí.

V průběhu měření byl kryptografický modul zcela ponořen v olejové lázni. Kapalina se postupně ohřívala a poté se teplota udržovala po dobu přibližně 5 min na požadované hodnotě. Po ustálení teploty (po uběhnutí 5 min) byl průběh závislosti napětí na bočníku zaznamenán osciloskopem. Měření první fáze proběhlo při zvyšování teploty a měření druhé fáze se uskutečnilo při postupném samovolném ochlazování kapaliny. Na obrázku 4.12 je detail napěťové špičky diferenčního signálu pro různou teplotu t_{O}, kdy je patrný pouze posun signálu. Průběh je jinak praktický totožný. Posun samotný je s největší pravděpodobností způsoben zvoleným postupem měření. Ideální by bylo měření diferenčního signálu provádět v jeden okamžik, tj. první i druhou fázi měření uskutečnit v co nejkratším časovém úseku od sebe. Postup měření, kdy se nejprve při ohřevu kapaliny měřily hodnoty první fáze a poté při ochlazování se měřily hodnoty fáze druhé, způsobil situaci, kdy sice teplota okolí t_{O} byla shodná, avšak pracovní teplota t_{A} mikroprocesoru byla odlišná, tj. $t_{\mathrm{O}} \neq t_{\mathrm{A}}$. Po následném zpracování naměřených průběhů je pak výsledný diferenční signál posunut v ose y (tj. napětí u).

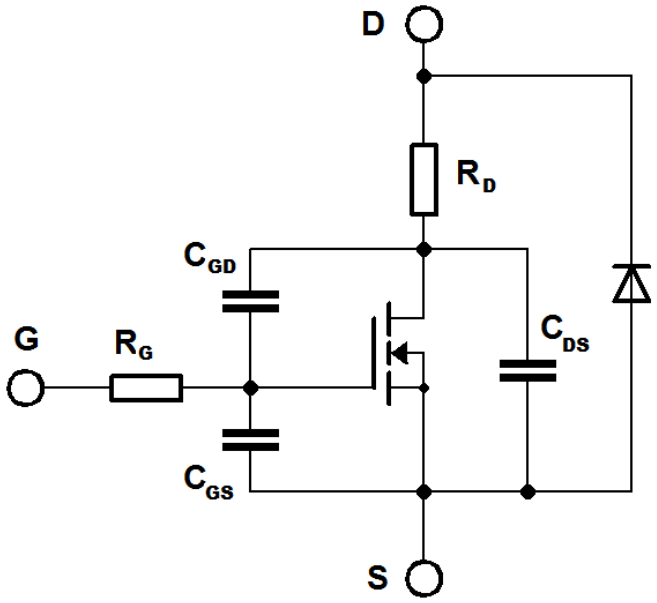


Obr. 4.13: Detail Peak-to-Peak hodnot napětí při různé teplotě okolí.

Nicméně lze konstatovat, že vliv teploty okolí v měřeném rozsahu se na průběhu diferenčního signálu napětí na bočníku prakticky neprojevil.

4.6 Vliv parazitních kapacit

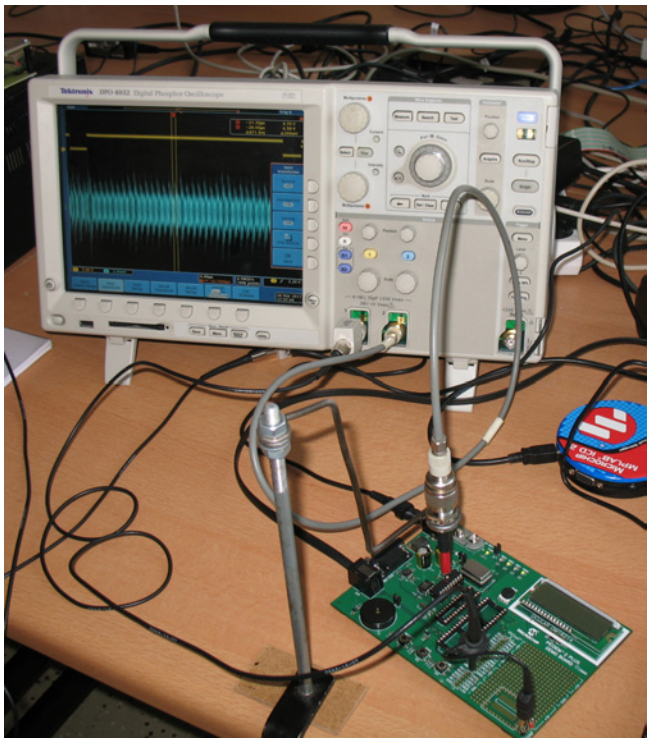
Parazitní kapacity se vyskytují mezi jednotlivými vodivými cestami na DPS, mezi přívodními kabely (napájecí, měřicími), mezi protilehlými kontakty rezistorů o vyšších hodnotách odporu. Dále se parazitní kapacity vyskytují uvnitř IO v tranzistorech i mezi vodivými cestami na čipu IO. S vyšší frekvencí hodinového signálu se také zvyšuje rychlost spínání FET tranzistorů. S vyššími frekvencemi hodinového signálu se pak také ovšem výrazněji uplatňují parazitní kapacity hradla tranzistoru (obr. 4.14). Dynamické chování tranzistoru potom záleží především na době potřebné k vytvoření vodivého kanálu. Záleží tedy na době potřebné k nabíjení a vybíjení těchto parazitních kapacit (C_{GD}, C_{DS}, C_{GS}). Při překročení mezního kmitočtu hodinového signálu pak tranzistory již nestíhají spínat a dochází tak nefunkčnosti obvodu.



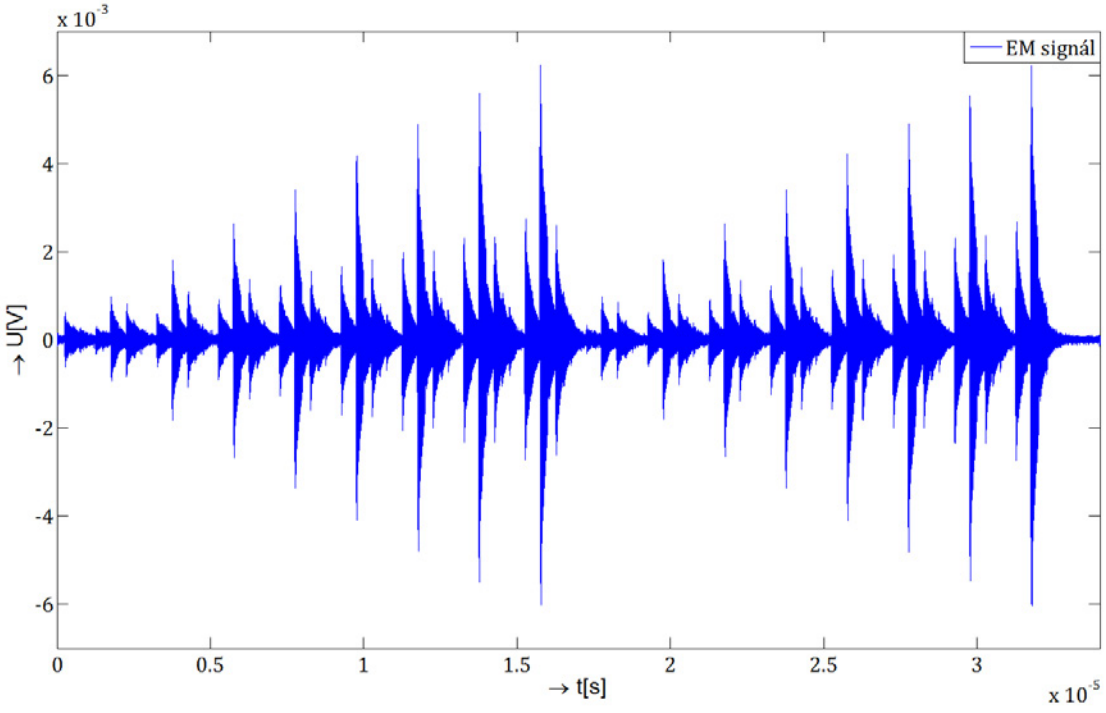
Obr. 4.14: Náhradní schéma tranzistoru MOSFET.

4.7 Porovnání průběhu PA s průběhem EMA

Pro porovnání je na obrázku 4.15 průběh diferenčního signálu, který byl naměřen metodou EMA (Elektromagnetická analýza). Toto napětí bylo naindukováno na cívce sondy osciloskopu elektromagnetickým polem, které je produkováno obvody kryptografického modulu (obr. 4.14). Z obrázku je zřejmá korespondence průběhů PA a EMA. Průběh signálu naměřený EMA je dokonce méně ovlivněn šumem oproti průběhu měřeného PA. Korelace elektromagnetického postranního kanálu a stavu vnitřních obvodů mikroprocesoru je výraznější než v případě proudového postranního kanálu.



Obr. 4.15: Měřicí pracoviště EMA.



Obr. 4.16: Elektromagnetický postranní kanál mikroprocesoru.

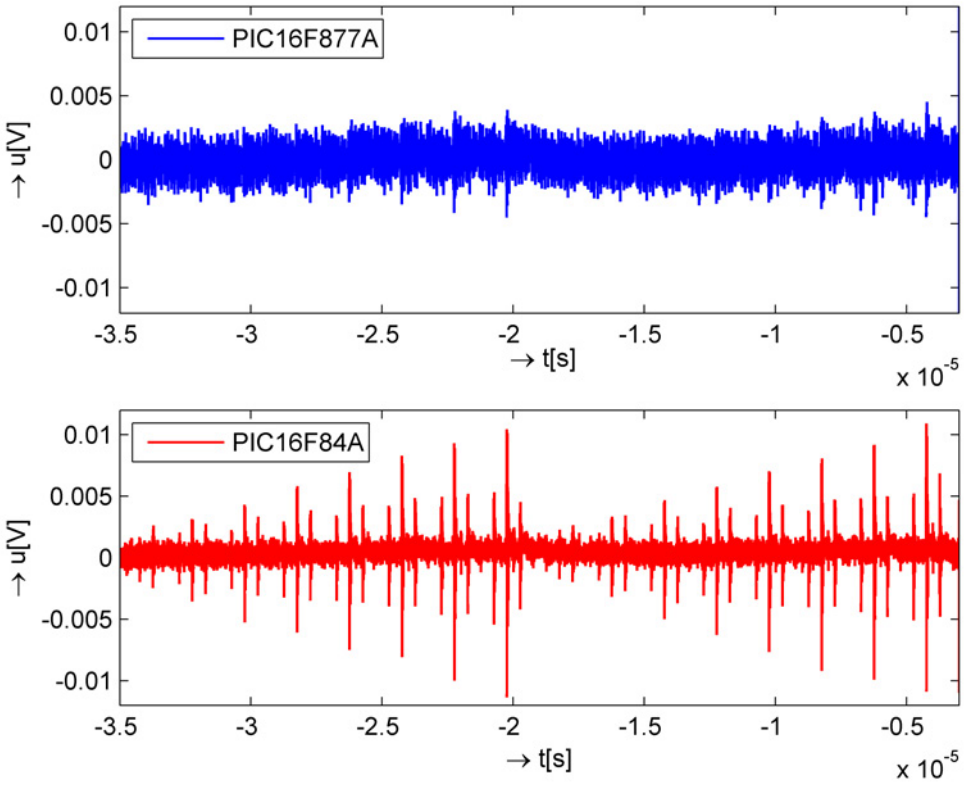
5 PROTIOPATŘENÍ

Protiopatření se dají rozdělit do dvou základních kategorií a to na protiopatření softwarová a protiopatření hardwarová. Primárním cílem, ať už se jedná o softwarovou či hardwarovou implementaci protiopatření, je potlačení korelace mezi postranním kanálem a citlivou informací, která je v daný moment kryptografickým modulem zpracovávána.

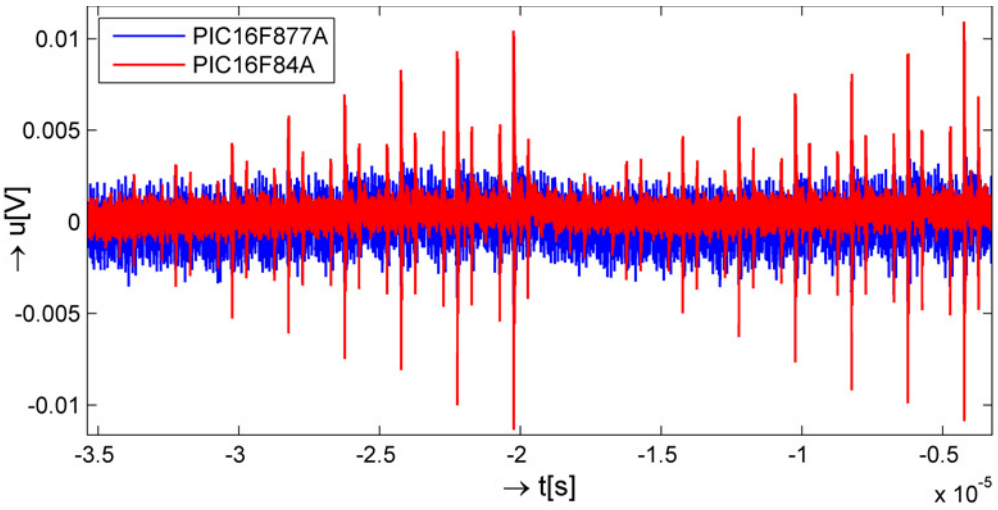
5.1 Hardwarová implementace

U implementací protiopatření spadající do této kategorie jsou opatření, kdy je snahou co nejvíce redukovat množství informací vyzařované postranními kanály. Cílem je dosáhnout jisté pravidelnosti v průběhu signálu vyzařovaného postranním kanálem. Příkladem může být zavedení signálu šumu do postranního kanálu. Zavedení šumu pak vyhlazuje průběh signálu postranního kanálu a posléze již nejsou tolik patrné přechody mezi různými stavy obvodu kryptografického modulu. V ideálním případě se signál jeví jako zcela náhodný šum, což de facto znemožní kryptoanalýzu postranního kanálu. Výsledky analýzy takového průběhu pak pro útočníka prakticky nemají žádnou hodnotu. Na obrázku 5.1 jsou průběhy diferenčního signálu pro různé mikroprocesory. U mikroprocesoru PIC16F877A je již implementována ochrana znesnadňující kryptoanalýzu postranních kanálu. Oba mikroprocesory zpracovávají zcela totožný program, avšak výsledné průběhy jsou zcela odlišné. Na obrázku 5.2 je pak srovnání těchto dvou průběhů.

Dalším tipem opatření jsou opatření, kdy se zavádějí tzv. čekací stavy (*wait states*). Jedná se o metodu opatření, která je relativně účinná proti útokům, kdy se využívá statistických výpočtů (např. DPA). Pro účely statistických výpočtů je nutno jednotlivé průběhy signálů postranního kanálu „srovnat“. Vkládání těchto čekacích stavů (s náhodnou dobou čekání) při vykonávání instrukcí programu, pak znesnadňuje toto srovnání průběhů – signál totiž ztrácí svou předchozí vlastnost – periodicitu. Praktický totožný účel také plní zavedení nestabilního hodinového signálu, tj. proměnlivého taktovacího signálu obvodů kryptografického modulu. Toto způsobí rovněž desynchronizaci signálů postranních kanálů, které se snaží útočník analyzovat [13].



Obr. 5.1: Diferenční průběh napětí funkce *AddRoundKey*.



Obr. 5.2: Srovnání diferenčních průběhů pro různé PIC.

5.2 Softwarová implementace

Obdobou čekacích stavů u hardwarové implementace protiopatření jsou tzv. „*dummy*“ cykly. Jedná se rovněž o stavy čekání, které jsou však implementovány softwarově.

Co se týče softwarových opatření, tak často používanou metodou je metoda maskování. Princip lze jednoduše vysvětlit na příkladu RSA podpisu, který se standardně vypočítá dle vztahu [13]:

$$S \ = \mu(m)^d \bmod N, \tag{5.1}$$

kde S je podpis, m je otevřený text, $\mu(m)$ je hash otevřeného textu, d je soukromý klíč a N je modulo.

Vztah pro RSA podpis po implementaci maskování může vypadat následovně:

$$S' = \left[(\mu(m) + r_1 N)^{d + r_2 \phi(N)} \bmod (r_3 N)\right] \bmod N, \tag{5.2}$$

kde S' je podpis, $\phi(N)$ je Eulerova funkce. Hondoty r_1, r_2 a r_3 jsou náhodná čísla. Platí $S = S'$.

5.3 Shrnutí

V ideálním případě, pokud to okolnosti umožňují, je zcela žádoucí implementace protiopatření založené na kombinaci softwarové i hardwarové implementace. Je zapotřebí nepodceňovat zabezpečení kryptografických modulů a dalších zařízení, pracujícími s citlivými informacemi, jejichž únik by byl nežádoucí. Je třeba mít na vědomí, že únik informací neprobíhá jen v jedné rovině, jedním postranním kanálem, ale ve vícero rovinách, několika postranními kanály.

6 ZÁVĚR

Pro účely měření byl vytvořen a následně realizován návrh DPS. DPS byla osazena součástkami nezbytně nutnými pro správnou funkci mikroprocesoru. Poté byla realizována série měření, kdy bylo použito dvou mikroprocesorů. Zvoleny byly mikroprocesory PIC16F84A a PIC16F877A. První jmenovaný mikroprocesor nepodporoval hardwarovou implementaci protiopatření zamezující analýzu prostřednictvím postranních kanálů. Druhý jmenovaný mikroprocesor již hardwarovou ochranu implementovánu měl. Práce se zabývala především vlivem konstrukčních parametrů, nastavení obvodu kryptografického modulu a dalších podmínek na proudový odběr mikroprocesoru. Zkoumal se vliv velikosti napájecího napětí, vliv velikosti frekvence hodinového signálu, vliv velikosti odporu bočníku, vliv velikosti kapacity blokovacích kondenzátorů a vliv teploty okolí.

Se vzrůstajícím napájecím napětím mikroprocesoru se Peak-to-Peak hodnoty napětí diferenčního průběhu zvyšovaly, avšak šumová složka se prakticky nezměnila. S vyššími hodnotami napájecího napětí je tedy kryptoanalýza proudového postranního kanálu mnohem účinnější.

Volba frekvence hodinového signálu se rovněž výrazným způsobem projevovala na výsledném průběhu diferenčního signálu. V tomto případě je vhodnější volba frekvence hodinového signálu co možná nejvyšší. S vyššími hodnotami kmitočtu je diferenční průběh napětí více zarušen šumem – výraznější oscilace napětí na bočníku. To má za následek obtížnější analýzu proudového postranního kanálu.

Vliv velikosti odporu bočníku na proudový odběr byl také dosti značný. S rostoucí hodnotou velikosti odporu se sice Peak-to-Peak hodnoty diferenčního signálu zvyšovaly, avšak rovněž narůstala velikost šumové složky ve výsledném průběhu, tj. klesal poměr S/N. Volba menší hodnoty odporu bočníku výrazně usnadňuje analýzu proudového postranního kanálu.

V případě analýzy vlivu velikosti kapacity blokovacích kondenzátorů se jako vhodnější jeví volba vyšších hodnot kapacity. Z konstrukčního hlediska je doporučována hodnota 100 nF. V případě této volby je pak výsledný průběh diferenčního signálu nejméně zarušen šumem a přechody mezi stavy vnitřních obvodů mikroprocesoru jsou pak mnohem zřetelnější. U příliš nízkých, nebo naopak vysokých hodnot kapacit, je u diferenčního signálu výraznější oscilace při změnách stavů obvodů v mikroprocesoru.

Teplota okolí se v měřeném rozsahu prakticky neprojevila na výsledném průběhu signálu.

Parazitní kapacity se projevují nepříznivým způsobem jak na analýze proudového odběru, tak na samotné funkčnosti kryptografického modulu. Vliv na funkčnost modulu mají jak parazitní kapacity mezi spoji na DPS, tak parazitní kapacity

ve vnitřních obvodech PIC. Při překročení mezního kmitočtu hodinového signálu tranzistory nestíhají spínat a dochází tak k nefunkčnosti obvodu. Parazitní kapacity jsou tedy nežádoucím jevem jak z hlediska funkčnosti mikroprocesoru, tak z hlediska kryptoanalýzy.

Jako protiopatření vůči kryptoanalýze (nejen proudových) postranních kanálů se doporučuje protiopatření založené na hardwarové i softwarové implementaci.

LITERATURA

[1] MENEZES, A., J., VAN OORSCHOT, P., C., VANSTONE, S., A.: Handbook of Applied Cryptography, CRC Press LLC, 816 stran, 1996, ISBN 0-8493-8523-7.

[2] OBRUČNÍK, O. Proudový postranní kanál mikroprocesorů. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. 64 s. Vedoucí diplomové práce Ing. Zdeněk Martinásek.

[3] KLÍMA, V. Moderní kryptografie I. *CRYPTO - WORLD* [online]. 11.4.2007, 4, [cit. 2010-12-07]. Dostupné z WWW: <http://www.crypto-world.info/klima/mffuk/Symetricka_kryptografie_I_2007.pdf>.

[4] KOCHER, P, JAFFE, J., JUN, B.: Introduction To Differential Power Analysis and Related Attacks. In Power Analysis and Related Attacks [online]. San Francisco, CA : [s.n.], 1998 [cit. 2010-12-07].

[5] *Http://en.wikipedia.org* [online]. 1. 10. 2010 [cit. 2010-12-07]. Advanced Encryption Standard. Dostupné z WWW: <http://en.wikipedia.org/wiki/Advanced_Encryption_Standard>.

[6] KLÍMA, V., ROSA, T.: Vybrané aspekty moderní kryptoanalýzy. In Trendy [online]. [s.l.] : [s.n.], 2003 [cit. 2010-12-07]. Dostupné z WWW: <http://www.crypto-world.info>.

[7] ROSA, T.: Kryptografie v klidu a bezpečí (1 až 6), Chip, únor až září 2001

[8] HLAVÁČ, M. *Využití postranních kanálů v symetrické a asymetrické kryptoanalýze* [online]. [s.l.], 2010. 56 s. Dizertační práce. Univerzita Karlova v Praze.

[9] MANGARD, S., OSWALD, E., POPP, T. *Power Analysis Attack: Revealing the Secrets of Smart Cards.* [s.l.] : [s.n.], 2007. 337 s.

[10] NOUZÁK, J. Postranní kanály mikroprocesorů. Praha, 2007. 48 s. České vysoké učení technické v Praze, Fakulta elektrotechnická. Vedoucí bakalářské práce Ing. Jan Schmidt, Ph.D.

[11] *Překlad manuálu k PIC 16F84A.* [online]. [2001] [cit. 2009-11-03]. Dostupné z WWW: <http://www.copsu.cz/mikrop/download.php?headr=pic16f84a&plusDB=1>.

[12] *PICmicro Mid-Range MCU Family Reference Manual.* [online]. U.S.A: Microchip Technology Inc., 1997 [cit. 2011-05-19]. Dostupné z WWW: <http://www.microchip.com/downloads/en/devicedoc/33023a.pdf>.

[13] CETIN KAYA, K., et al. Cryptographic Engineering. U.S.A: Springer, 2009. 522 s.

[14] *Advanced Encryption Standard Using the PIC16XXX.* [online]. U.S.A: Microchip Technology Inc., 2002 [cit. 2011-05-19]. Dostupné z WWW: <http://www.microchip.com/downloads/en/AppNotes/00821a.pdf>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

ADC	analogově digitální převodník – Analog-to-Digital Converter
AES	šifrovací algoritmus – Advanced Encryption Standard
C_1, C_2, C_3	blokovací kondenzátory
C_{DS}	parazitní kapacita tranzistoru MOSFET mezi piny DRAIN a SOURCE
C_{GD}	parazitní kapacita tranzistoru MOSFET mezi piny GATE a DRAIN
C_{GS}	parazitní kapacita tranzistoru MOSFET mezi piny GATE a SOURCE
CMOS	výrobní technologie integrovaných obvodů – Complementary Metal Oxide Semiconductor
d	soukromý klíč RSA
DES	šifrovací algoritmus – Data Encryption Standard
DPA	diferenční výkonová analýza – Differential Power Analysis
DPS	deska plošných spojů
EMA	elektromagnetická analýza – ElectroMagnetic Analysis
EXT_CLK	konektor pro připojení externího hodinového signálu
f_{OSC1}	kmitočet hodinového signálu na vstupním pinu OSC1
f_{VZ}	vzorkovací frekvence osciloskopu
$\phi(N)$	Eulerova funkce
HS	krystalový oscilátor (pro $f_{OSC1} \geq 4000\,\text{kHz}$)
m	otevřený text
MOSFET	unipolární tranzistor – Metal Oxide Semiconductor Field Effect Transistor
$\mu(m)$	hash otevřeného textu m
N	modulo, součástí soukromého i veřejného klíče RSA
OSC1	vstupní pin pro přivedení vnějšího hodinového signálu

OUT_PIN	konektor s vyvedenými výstupními piny PIC
PA	výkonová analýza – Power Analysis
PC	programový čítač – Program Counter
PIC	mikroprocesor – Peripheral Interface Controller
PIN	osobní identifikační číslo – Personal Identification Number
PICA	picosekundová zobrazovací obvodová analýza – Picosecond Imaging Circuit Analysis
Q1–Q4	dílčí hodinové signály PIC tvořící T_{OSC}
r_1, r_2, r_3	náhodná čísla, parametry maskovací funkce RSA podpisu
R_B	odporový bočník pro měření napětí, resp. proudového odběru
RB0, RB1	výstupní piny PIC
RC4	symetrická proudová šifra
RISC	redukovaná instrukční sada – Reduced Instruction Set Computer
RSA	asymetrický šifrovací algoritmus – Rivest-Shamir-Adleman
S, S'	podpis – Signature
SPA	jednoduchá výkonová analýza – Simple Power Analysis
S/N	poměr užitečného signálu a šumu – Signal-to-Noise Ratio
t_A	pracovní teplota PIC
T_{ARK}	doba, za kterou se vykoná funkce *AddRoundKey*
t_O	teplota okolí
T_{OSC}	perioda vnitřního hodinového signálu PIC
U_{CC}	napětí na výstupu zdroje stejnosměrného napětí
V_{DD}	vstupní pin pro napájecí napětí PIC
XOR	exklusivní součet – Exclusive OR
XT	krystalový oscilátor (pro f_{OSC1}= 400 - 8000 kHz)