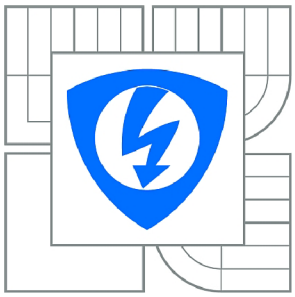
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

PROUDOVÝ POSTRANNÍ KANÁL

POWER SIDE CHANNEL

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

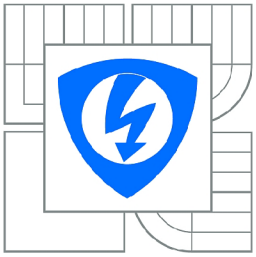
AUTOR PRÁCE — ONDŘEJ ZAPLETAL

AUTHOR

VEDOUCÍ PRÁCE — Ing. ZDENĚK MARTINÁSEK

SUPERVISOR

BRNO 2012



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Ondřej Zapletal	***ID:***	125707
Ročník:	3	***Akademický rok:***	2011/2012

NÁZEV TÉMATU:

Proudový postranní kanál

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte útok proudovým postranním kanálem na kryptografický modul. Navrhněte a realizujte experimentální desku plošných spojů osazenou jen procesorem PIC16f84 (popřípadě PIC18F77) a potřebnými součástkami k funkčnosti čipu. K analýze proudového postranního kanálu použijte sondu tekxtronic CT-6 a osciloskop. Na procesor nahrajte funkci AddRoundKey šifrovacího algoritmu AES a analyzujte proudový odběr pro napájecí napětí mikroprocesoru 10, 9, 7 a 5V a pro frekvenci oscilátoru 4 a 8MHz při napájecím napětí 5 a 10 V. Na kryptografický modul implementujte šifrovací algoritmus AES a realizujte diferenciální proudovou analýzu pro první bajt tajného klíče. 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:	6.2.2012	***Termín odevzdání:***	31.5.2012

Vedoucí práce: Ing. Zdeněk Martinásek
Konzultanti bakalářské práce:

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

ABSTRAKT

Tato bakalářská práce se věnuje kryptoanalýze prostřednictvím postranních kanálů. Je zaměřena především na útok proudovým postranním kanálem na kryptografický modul. Jako kryptografický modul je použit mikrokontrolér PIC vykonávající šifrování symetrickou šifrou AES. Pro účely jednoduché a diferenciální proudové analýzy modulu byla použita experimentální deska plošných spojů. Analýza proudového odběru mikrokontroléru PIC provádějícího operaci `AddRoundKey` a `SubBytes` byla provedena proudovou sondou Tektronix CT-6. Data získaná měřením byla zpracována na počítači s příslušným programovým vybavením k nalezení důležité informace o použitém šifrovacím klíči.

KLÍČOVÁ SLOVA

Kryptoanalýza, proudový postranní kanál, proudová analýza, AES, mikrokontrolér PIC

ABSTRACT

This thesis deals with side-channel cryptoanalysis. It is focused on power side-channel attack on cryptographic device. The microcontroller PIC is used as the cryptographic device. This microcontroller performs encryption through the symmetrical algorithm AES. For the purpose of simple and differential power analysis, we designed and constructed an experimental printed circuit board. The power consumption of the microcontroller PIC working with instruction AddRoundKey and SubBytes was scanned by a Tektronix CT-6 current probe. Data obtained by measuring were processed on the computer with relevant software and provided important information about the encryption key that was used.

KEYWORDS

Cryptanalysis, power side-channel, power analysis, AES, PIC microcontroller

ZAPLETAL, Ondřej *Proudový postranní kanál*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2012. 60 s. Vedoucí práce byl Ing. Zdeněk Martinásek

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Proudový postranní kanál“ jsem vypracoval samostatně pod vedením vedoucího bakalářské 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 bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské 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 bakalářské práce panu Ing. Zdeňku Martináskovi za odborné vedení, konzultace a cenné rady při zpracování této práce.

Brno ....

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

ÚVOD

Bakalářská práce se zabývá kryptoanalýzou postranními kanály se zaměřením na proudový postranní kanál. Útoky postranními kanály na kryptografické systémy představují v současnosti jeden z nejrozšířenějších postupů k získávání informací o procesech probíhajících uvnitř napadeného kryptografického systému.

První část bakalářské práce se zabývá vysvětlením pojmu kryptologie a kryptoanalýza. Dále je vysvětlen pojem kryptografický modul a požadavky na něj kladené. Popsány jsou rovněž základní typy útoků na šifrovací algoritmy.

V další kapitole se práce zaměřuje na nejrozšířenější způsob získávání informací o činnosti kryptografického modulu – k útoku postranními kanály. Zejména je zde popsán obecný princip jednoduché a diferenciální proudové analýzy.

V teoretickém úvodu lze nalézt informace o šifrovacím standardu AES a vysvětlení principů fungování použitého mikrokontroléru PIC. Pochopení jeho činnosti je klíčem ke správnému provedení praktické části bakalářské práce.

V praktické části je popsán návrh a realizace jednoduchého kryptografického modulu s mikrokontrolérem PIC. Dále jsou zde uvedeny technické parametry proudové sondy použité při jednoduché a diferenciální proudové analýze a princip její činnosti. Popsáno je i samotné měřicí pracoviště, včetně jeho vybavení a měřicí techniky.

Závěrečná část práce je věnována proudové analýze sestaveného kryptografického modulu při vykonávání operací `AddRoundKey` a `SubBytes`, které tvoří část šifrovacího algoritmu AES.

1 KRYPTOLOGIE

Kryptologie je vědní obor zabývající se problematikou šifrování a dešifrování. Zahrnuje v sobě dva podobory, a to kryptografii a kryptoanalýzu. Kryptografie se zaobírá problematikou návrhu šifer. Cílem kryptoanalýzy je naopak snaha tyto šifry prolomit a pokusit se rozluštit zašifrovaný text či zprávu. Využívá se též k testování odolnosti používaných šifer. V následujících kapitolách je věnována pozornost právě kryptoanalýze.

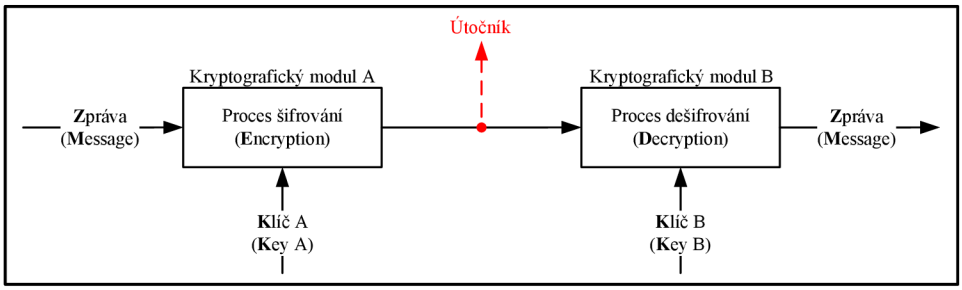
Základy kryptoanalýzy

Hlavním úkolem kryptografických systémů je poskytnout zabezpečený přenos informací mezi jejich uživateli. K tomu poskytují níže uvedené funkce.

- **Důvěrnost:** Utajení přenášených zpráv před neoprávněným uživatelem.
- **Autentičnost:** Uživatel má možnost ověřit si původ zprávy.
- **Integrita:** Zpráva nesmí být během přenosu modifikována.
- **Nepopiratelnost:** Schopnost prokázat totožnost uživatele, který zprávu odeslal (např. digitální podpis).

Výše uvedené funkce kryptografického systému jsou zajišťovány kryptografickým modulem, který má v sobě implementován konkrétní šifrovací algoritmus. Tento modul může být realizován softwarově či hardwarově. Základním bezpečnostním požadavkem je, aby veškerá komunikace s okolím probíhala pouze prostřednictvím jeho definovaných rozhraní. Dále se také klade důraz na rychlost provádění kryptografických operací (autentizace, ověřování správnosti, šifrování, dešifrování atd.).

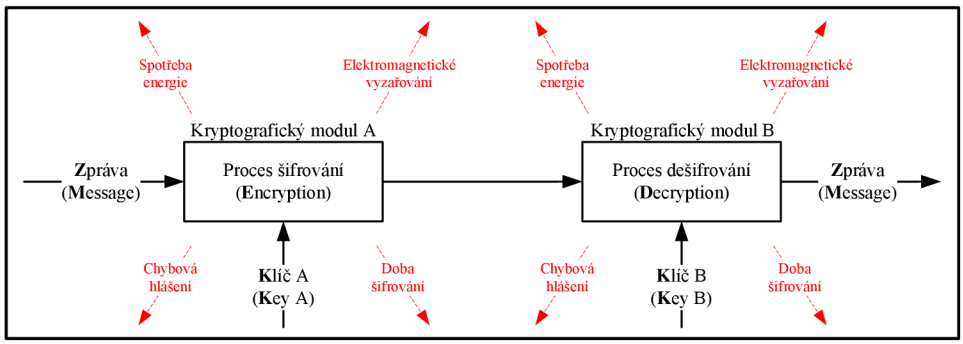
Kryptoanalýza využívá pro prolomení šifrovacího algoritmu uvnitř modulu dva základní typy útoků. První se označuje jako útok hrubou silou a představuje konvenční neboli tradiční model útoku (viz obr. 1.1).



Obr. 1.1: Konvenční model útoku na kryptografický modul.

Útok hrubou silou na šifrovací algoritmus spočívá v systematickém zkoušení všech existujících možností šifrovacího klíče. Klíč, který vstupuje do šifrovacího procesu jako vnitřní parametr, může dosahovat bitové délky např. 1024 bitů. S narůstající délkou klíče výrazně klesá praktická proveditelnost tohoto typu útoku, protože se zvyšují nároky na potřebný výpočetní výkon a čas, a to exponenciálně. Současné šifrovací algoritmy jsou z hlediska možnosti prolomení pomocí hrubé síly považovány za bezpečné.

Konvenční model útoku na šifrovací algoritmy se tedy postupem času ukázal jako neefektivní. Kryptoanalýza proto obrátila svou pozornost na samotné kryptografické moduly a jejich fyzikální projevy při procesu šifrování či dešifrování. Vznikl rozšířený model útoku zahrnující postranní kanály (viz obr. 1.2).



Obr. 1.2: Rozšířený model útoku na kryptografický modul.

Tento model útoku se nespoléhá na teoretické slabiny v návrhu šifrovacího algoritmu, ale na informace, které lze získat postranními kanály z kryptografického modulu. Mohou to být informace o celkové době potřebné k zašifrování (dešifrování) zprávy kryptografickým modulem, jeho proudová spotřeba, elektromagnetické vyzařování, nedefinované chybové stavy aj. Získané informace jsou poté využity k odhalení klíče a dešifrování tajných zpráv. Útokům postranními kanály se podrobněji věnuje následující kapitola.

2 ÚTOKY POSTRANNÍMI KANÁLY

Útoky postranními kanály označované zkratkou SCA (Side-Channel Attacks) na kryptografické systémy jsou v současnosti nejrozšířenější oblastí aplikované kryptoanalýzy. Kryptoanalýza postranními kanály nepracuje jen se samotným šifrovacím algoritmem, ale je zaměřena i na jeho konkrétní implementaci uvnitř kryptografického modulu. Útok prostřednictvím postranních kanálů bývá proto nazýván jako implementační.

Kryptografický modul si lze představit jako fyzické zařízení, které při vykonávání procesu šifrování (dešifrování) určitým způsobem interaguje s okolním prostředím. Sledováním těchto interakcí může potenciální útočník získat dostatek tzv. postranních informací k prolomení šifrovacího algoritmu a dešifrování tajných zpráv.

2.1 Historie útoků postranními kanály

V roce 2007 byl americkou vládou odtajněn materiál odkrývající část historie útoků postranními kanály [18]. Vrací se až do období druhé světové války. Americká armáda a námořnictvo tehdy používali pro zabezpečení komunikace šifrovací zařízení vyvinuté Bellovými laboratořemi pod označením 131-2B. Když jedno z těchto zařízení bylo v laboratořích podrobeno testu, výzkumník provádějící jeho kontrolu objevil, že po každém kroku šifrování se na vzdáleném osciloskopu objeví impulz. Osciloskop zachytával elektromagnetické pole vyzařované z šifrovacího zařízení. Bližším prozkoumáním zachyceného signálu bylo možné přečíst zprávy, které byly právě šifrovány. Tato událost dala vzniknout programu TEMPEST, jenž v dnešní době představuje standardy a doporučení pro elektronická zařízení vyzařující elektromagnetické pole.

Útok postranním kanálem za účelem získání tajných informací cizího státu byl poprvé využit v roce 1965 britskou tajnou službou MI5 [24]. Ta se neúspěšně pokoušela prolomit šifru používanou egyptskou ambasádou v Londýně. Jejich neúspěch vycházel z nedostatečného výpočetního výkonu tehdejších počítačů. Vědecký pracovník P. Wright navrhl umístit v blízkosti rotoru šifrovacího zařízení mikrofon s cílem detekovat počet cvaknutí. Odposlechem cvaknutí rotoru, při jeho každodenní inicializaci, se MI5 podařilo odhadnout pozici dvou nebo tří z rotorů. Tato informace umožnila snížit potřebný výpočetní výkon k prolomení šifry. MI5 mohla odposlouchávat tajné depeše egyptské ambasády celé roky.

2.2 Útoky na kryptografická zařízení

V průběhu posledních let bylo nalezeno mnoho typů útoků na kryptografická zařízení s cílem získat tajný klíč. Techniky využívané pro dosažení tohoto cíle lze rozdělit podle několika kritérií.

Pro útok na kryptografická zařízení a možné získání tajné informace jsou zejména potřebné finanční prostředky, důležitou úlohu hraje časová náročnost útoku, přístup k potřebnému vybavení a také odborné znalosti útočníka. Ve většině odborných textů zabývajících se útoky na kryptografická zařízení jsou zmiňována dvě základní kritéria dělení těchto útoků. První kritérium je, zda je útok pasivní či aktivní.

Pasivní útoky

Při pasivním útoku pracuje kryptografické zařízení podle daných specifikací a norem. Útok je zaměřen na pozorování fyzikálních projevů daného zařízení (tzn. čas potřebný k šifrování či dešifrování, proudový odběr z napájecího zdroje atd.)

Aktivní útoky

Při aktivním útoku je snahou útočníka ovlivnit vstupy kryptografického zařízení nebo prostředí, ve kterém se nachází. Tato manipulace způsobí netypické chování zařízení a vyvolá jeho chybový stav. Tajný klíč je poté možné odhalit využitím tohoto abnormálního chování.

Druhé kritérium se zaměřuje na dostupná rozhraní kryptografických zařízení. Každé kryptografické zařízení má několik fyzických a logických rozhraní. Podle přístupu k jednotlivým rozhraním, která jsou využívána k útoku, je možné rozlišit invazivní, semi-invazivní a neinvazivní útoky. Každý z těchto útoků může být buď pasivní, nebo aktivní.

Invazivní útoky

Invazivní útok patří mezi nejefektivnější druh útoku na kryptografická zařízení. K získání tajného klíče je možno využít veškeré dostupné prostředky.

Při invazivním útoku se nejprve odstraní vrstva chránící zařízení za účelem získat přímý přístup k jeho vnitřním komponentům. Pomocí měřicí sondy lze poté zachytit např. informace přenášené po datové sběrnici kryptografického zařízení. Tato část invazivního útoku je pasivní, pokud je sonda použita pouze k měření signálů na sběrnici. Lze však také přerušit vodivé cesty sběrnice a ovlivnit tak proces probíhající

uvnitř zařízení. Invazivní útok se poté stane aktivním. K tomuto záměru je možno využít laserový nůž či fokusovaný paprsek iontů.

Kryptografická zařízení s vyšší úrovní zabezpečení mohou obsahovat technologie, které se snaží invazivním útokům zabránit. Nejčastější technikou je detekce pokusu o narušení fyzické ochrany. Při zjištění pokusu o průnik k vnitřním částem zařízení se jeho paměť vynuluje, dále může přerušit svou činnost a informovat obsluhu.

Invazivní útoky jsou velice účinné. Pro jejich vykonání je však potřeba drahé vybavení. Často dochází také k úplnému zničení zařízení.

Semi-invazivní útoky

Při semi-invazivním útoku je potřebný přístup k vnitřním částem kryptografického zařízení, není však nutné vytvořit přímý kontakt s vodivými cestami uvnitř zařízení. Ochranná vrstva zůstává neporušená.

Semi-invazivní útok může být též pasivní či aktivní. Aktivním se stává pokud je útočníkem do kryptografického zařízení úmyslně zavedena chyba. To může být provedeno např. rentgenovými paprsky, světelnými paprsky nebo elektromagnetickým polem.

Tento typ útoku nevyžaduje tak drahé vybavení jako invazivní útok. Stále je však na provedení velice náročný a vyžaduje dostatek času a potřebné znalosti.

Neinvazivní útoky

Neinvazivní útok na kryptografické zařízení využívá pouze jeho přímo přístupných rozhraní. Není ovlivněna správná funkce zařízení a útočník nezanechá za sebou žádné stopy. Útok je tedy nedetekovatelný. Protože pro většinu neinvazivních útoků stačí relativně levné vybavení, představují tyto útoky obrovské riziko z hlediska bezpečnosti kryptografických zařízení.

V současné době se obrací pozornost zejména na pasivní neinvazivní útoky, tedy útoky postranními kanály. Mezi nejčastěji se vyskytující druhy patří časový postranní kanál, proudový postranní kanál a útok elektromagnetickým postranním kanálem. Tajný klíč z kryptografického zařízení může být získán např. měřením času potřebného pro vykonání daných operací, jeho následnou analýzou a porovnáním s procesy probíhajícími uvnitř zařízení. Je také možné měřit proudový odběr zařízení z napájecího zdroje nebo jeho elektromagnetické pole.

Kromě útoků postranními kanály existují i aktivní neinvazivní útoky. Mohou využívat změn napájecího napětí nebo změn teploty prostředí, ve kterém se zařízení nachází.

2.3 Druhy útoků postranními kanály

Jak bylo zmíněno výše, útoky postranními kanály patří do skupiny pasivních neinvazivních útoků na kryptografická zařízení. Jejich cílem je získat potřebné informace k odhalení tajného klíče. Tyto informace představují buď otevřený text, který má být zašifrován, nebo již zašifrovaný text.

Útoky postranními kanály se dostávají do popředí zájmu moderní kryptoanalýzy, neboť představují vážné riziko pro bezpečnost kryptografických zařízení. Některé typy útoků postranními kanály mohou být vykonány i s nízkými finančními prostředky, protože potřebná zařízení lze dnes pořídit do několika set dolarů. Nezbytný čas na útok a následnou analýzu naměřených dat bude záviset na typu útoku.

Tato práce se zaměřuje především na jednoduchou a diferenciální proudovou analýzu. Jsou zde však popsány další nejrozšířenější typy těchto útoků, mezi které patří časová analýza, elektromagnetická analýza a analýza chyb.

2.3.1 Časová analýza

Časová analýza je založena na měření času nutného pro provedení určité operace kryptografickým zařízením. Tato informace může vést až k odhalení tajného klíče. Útok prostřednictvím časového postranního kanálu představil poprvé odborné veřejnosti Paul C. Kocher [10]. Pokud je tímto útokem kryptografické zařízení zranitelné, pak zpravidla stačí znát jen výsledný zašifrovaný text. Samotný útok bývá výpočetně nenáročný.

Kryptografickým zařízením často trvá zpracování různých vstupních dat odlišnou dobu. Důvodem jsou výkonové optimalizace v implementaci šifrovacích algoritmů, větvení programu, přístupy do paměti, různá doba vykonávání instrukcí programu a další. Výkon zařízení většinou závisí jak na tajném klíči, tak na vstupních datech (v našem případě šifrovaný nebo nešifrovaný text). Mohlo by se zdát, že informace uniklé prostřednictvím časového postranního kanálu sdělují potenciálnímu útočníkovi jen malé množství znalostí o celém kryptosystému (např. Hammingovu váhu klíče). Nicméně, jak je popsáno v práci [10], útoky využívající měření přesné doby vykonávání šifrovacích operací umožňují nalézt celý tajný klíč kryptografického systému.

Naměřené hodnoty času vykonávání šifrovacích operací jsou vloženy do statistické funkce, která s určitou pravděpodobností odhadne tajný klíč na základě vztahů mezi jednotlivými měřeními. Počet měřených vzorků potřebných pro získání tajného klíče záleží na vlastnostech měřeného signálu a úrovni šumu. Čím větší množství šumu, tím je vyžadováno větší množství vzorků. V práci [10] jsou popsány některé

techniky umožňující snížit počet měřených vzorků, avšak za cenu zvýšení potřebného výpočetního výkonu.

V práci [6] jsou uvedeny příklady použití útoku časovým postranním kanálem na asymetrické šifrovací systémy. Autor nicméně dodává, že tento typ útoku je možné použít i na kryptografické systémy pracující se symetrickou šifrou. Dále zde uvádí možná opatření a techniky, které mají za úkol ztížit útočníkovi získání užitečné informace.

2.3.2 Útoky zavedením chyby

U kryptografických zařízení je kladen velký důraz na spolehlivost při vykonávání šifrovacích operací. Proto se nepředpokládá, že bezpečnost operací implementovaných uvnitř zařízení může být narušena např. selháním hardwarového vybavení nebo výskytem chyby v průběhu provádění operací. Opak je však pravdou. Takové chybové chování kryptografického systému poskytuje důležité postranní informace, které výrazně zvyšují zranitelnost šifry.

Útok zavedením chyby do kryptografické zařízení uveřejnili poprvé v roce 1997 Dan Boneh, Richard A. DeMillo a Richard J. Lipton [1]. Útočníkovi je poskytnuta spousta možností provedení tohoto útoku. Podle implementace šifrovacího algoritmu v systému existují odlišné postupy jak nesprávný výsledek využít. Proveditelnost útoku záleží na schopnostech útočníka a typu chyby, kterou dokáže vyvolat.

Nejpoužívanější techniky zavedení chyb do kryptografického systému jsou uvedeny níže [8].

- **Změny napájecího napětí** mohou způsobit, že procesor v průběhu vykonávání operací přeskočí určitou instrukci nebo vrátí nesprávný výsledek této instrukce. Tato metoda je nejčastěji zkoumána výrobci čipových karet.
- **Změny hodinového signálu** mohou být příčinou špatného přečtení hodnoty dat, kdy se procesor pokouší přečíst hodnotu z datové sběrnice předtím než je načtena z paměti.
- **Změnou okolní teploty** mimo rozsah hodnot stanovenými výrobcem, ve kterých zařízení pracuje správně.
- Pomocí **bílého světla**. Všechny elektrické obvody vykazují citlivost na světlo na základě fotoelektrického jevu. Proud v obvodu vytvořený fotony může vyvolat chybu, pokud je obvod vystaven krátkému intenzivnímu světelnému záření.
- **Laser** má stejný efekt jako bílé světlo. Umožňuje však zaměřit se pouze na malou část obvodu.
- **Rentgenové paprsky nebo svazky iontů** mohou být také použity jako zdroj chyb, aniž by bylo nutné odstraňovat pouzdro čipu.

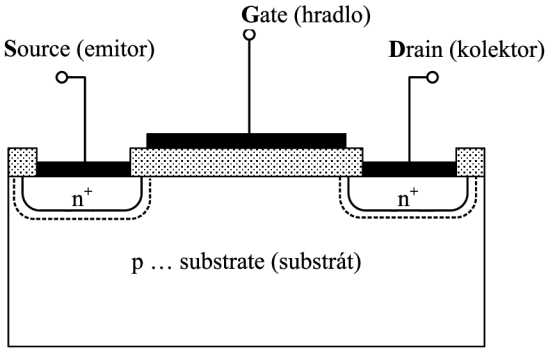
Kromě výše uvedených technik je možné do kryptografického zařízení poslat poškozená vstupní data. Zařízení na tuto nestandardní situaci obvykle zareaguje vysláním chybového hlášení uživateli, tedy útočníkovi. Hlášení obsahuje důvody o tom, proč byly právě probíhající operace zastaveny a může též neúmyslně obsahovat postranní informaci k odhalení tajného klíče.

Text práce [8] obsahuje podrobnosti, jak tento typ útoku aplikovat na konkrétní šifrovací algoritmy. V závěru jsou poté uvedeny některá protiopatření.

2.3.3 Proudová analýza

Proudový odběr kryptografického zařízení z napájecího zdroje není konstantní v čase, ale mění se v závislosti na aktuálně zpracovávaných datech a probíhajících operacích. Útok proudovým postranním kanálem je založen na analýze proudové spotřeby PA (Power Analysis) zařízení a jejím vztahem k právě vykonávaným operacím uvnitř zařízení.

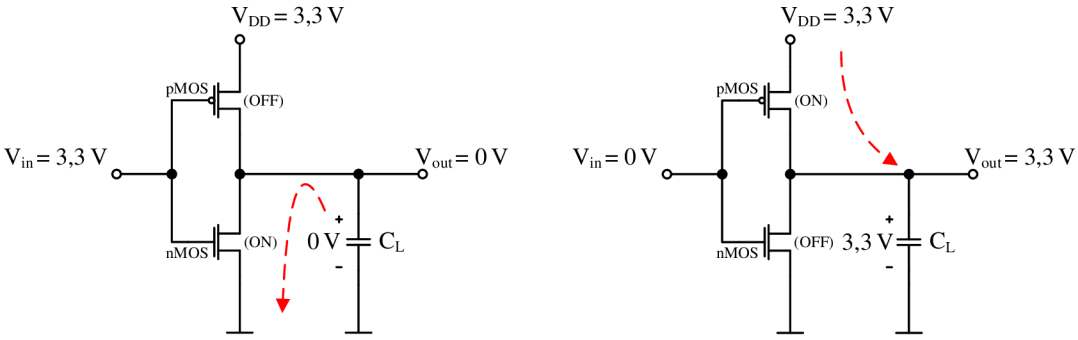
Integrované obvody uvnitř kryptografických zařízení jsou nejčastěji tvořeny z napěťově řízených tranzistorů (obr. 2.1) vyráběné technologií CMOS (Complementary Metal-Oxide Semiconductor).



Obr. 2.1: Struktura tranzistoru MOSFET s indukovaným vodivým kanálem.

Primárním stavebním prvkem logiky založené na technologii CMOS je invertující člen (obr. 2.2). Skládá se ze dvou tranzistorů pMOS a nMOS zapojených jako spínače řízené napětím. Pokud je na vstup prvního invertoru přivedena log. 1, pMOS tranzistor je uzavřen (OFF) a nMOS tranzistor otevřen (ON). Na výstupu prvního invertoru bude log. 0. Druhý invertor má na svém vstupu log. 0, v této situaci je pMOS tranzistor otevřen (ON) a nMOS tranzistor uzavřen (OFF). Na výstupu druhého invertoru bude log. 1. Celková proudová spotřeba invertoru může být rozdělena na dvě základní části [23]. První část tvoří statická proudová spotřeba, kdy invertor setrvává v ustáleném stavu. Její hodnota je velice malá. Druhá část je tvořena

dynamickou proudovou spotřebou, která nastává při změně stavů z log. 0 na log. 1 a obráceně. Dochází ke vzniku proudových špiček, které jsou způsobeny nabíjením a vybíjením parazitní kapacitní zátěže připojené na výstupy invertorů.



Obr. 2.2: Model CMOS invertoru a jeho princip činnosti.

Mikroprocesor uvnitř kryptografického zařízení využívá k provedení daných operací spínaní jednotlivých tranzistorů, tzn. mění aktuální odběr proudu z napájecího zdroje. Pouhým pozorováním proudového odběru je možné určit právě probíhající činnosti uvnitř mikroprocesorové jednotky. Tento typ útoku se nazývá jednoduchá proudová analýza SPA (Simple Power Analysis). Dále existuje komplikovanější diferenciální proudová analýza DPA (Differential Power Analysis) poskytující lepší interpretaci naměřených hodnot proudového odběru. Podrobněji jsou rozebrány v dalších kapitolách.

Jednoduchá proudová analýza SPA

Jednoduchá proudová analýza je postavena na přímém pozorování proudového odběru kryptografického zařízení z napájecího zdroje. Účelem tohoto pozorování je odhadnout, kterou instrukci mikroprocesor v daném čase provádí a s jakými hodnotami dat pracuje. Útočník musí k provedení tohoto útoku znát přesnou implementaci šifrovacího algoritmu.

Tento typ útoku může být použit k prolomení implementace šifrovacího algoritmu RSA (Rivest -Shamir -Adleman), u kterého lze pozorovat rozdíl ve spotřebě proudu mezi operacemi násobení a umocnění. Podobně pro většinu implementací šifrovacího algoritmu DES (Data Encryption Standard) je možné pozorovat rozdíl ve spotřebě proudu pro operace permutace a posunu [11].

Diferenciální proudová analýza DPA

Diferenciální proudová analýza je účinnější a efektivnější než výše zmíněná SPA. Při útoku prostřednictvím DPA nemusíme znát důkladně napadené kryptografické

zařízení. Obvykle postačuje znalost o tom, jaký šifrovací algoritmus dané zařízení obsahuje.

DPA vyžaduje velké množství naměřených průběhů proudové spotřeby kryptografického zařízení při šifrování či dešifrování vstupních dat. Ze zjištěných průběhů je možné získat tajný klíč. K tomu DPA využívá matematický aparát, zejména statistické analýzy a technik pro korekci chyb, které umožňují odhalit tajný klíč i z průběhů obsahujících velký šum.

Při provádění DPA útoku se postupuje podle následujících pěti kroků [13].

Krok 1: Volba vnitřní hodnoty vykonávaného šifrovacího algoritmu

V prvním kroku DPA útoku se zvolí vnitřní hodnota šifrovacího algoritmu, který je vykonáván kryptografickým zařízením. Tato vnitřní hodnota musí být funkcí $f(d, k)$, kde d jsou známá vstupní data (zpravidla otevřený či zašifrovaný text) a k představuje malou část použitého klíče, jenž lze odhadnout (např. první bajt).

Krok 2: Změření průběhů proudové spotřeby při šifrování

Druhým krokem DPA útoku je změření 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 vnitřní hodnoty určené v kroku 1. Hodnoty známých dat tvoří vektor $\mathbf{d} = (d_1, \ldots, d_D)'$, kde d_i označuje výsledek i-tého zpracovaného bloku vstupních dat.

Při vykonávání těchto operací je útočníkem zaznamenávána proudová spotřeba zařízení. Každému průběhu spotřeby $\mathbf{t}_i' = (t_{i,1}, \ldots, t_{i,T})$, kde T označuje dobu trvání průběhu, odpovídá jedna hodnota zpracovávaných dat d_i. Útočník měří proudovou spotřebu pro každý zpracovávaný blok dat D, a proto mohou být průběhy zapsány jako matice $\mathbf{T}$ o velikosti $D \times T$. Pro DPA útok je klíčové, aby měřené průběhy proudové spotřeby byly správně zarovnané. To znamená, že hodnoty proudové spotřeby v libovolném sloupci $\mathbf{t}_j$ matice $\mathbf{T}$ musí odpovídat stejné operaci. Toho lze dosáhnout správnou synchronizací použitého osciloskopu.

Krok 3: Sestavení matice hypotéz vnitřních hodnot

Dalším krokem útoku je pro všechny možné hodnoty klíče k určit hypotetické vnitřní hodnoty. Možné hodnoty klíče lze zapsat jako vektor $\mathbf{k} = (k_1, \ldots, k_K)$, kde K označuje celkový počet možných klíčů. Jednotlivým prvkům vektoru se říká hypotézy neboli odhady klíče. Z vektoru známých dat $\mathbf{d}$ a vektoru hypotéz všech klíčů je útočník schopen jednoduše vypočítat hypotetické vnitřní hodnoty $f = (d, k)$ pro

všechny šifrovací operace D a pro všechny hypotézy klíče K. Výsledkem bude matice $\mathbf{V}$ o velikosti $D \times K$.

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

Sloupec j matice $\mathbf{V}$ obsahuje vnitřní hodnoty, které byly vypočítány na základě příslušné hypotézy klíče k_j. Jeden sloupec matice $\mathbf{V}$ tedy obsahuje ty vnitřní hodnoty, které byly kryptografickým zařízením vypočítány během D operací šifrování a dešifrování. Hodnota klíče uvnitř zařízení je prvkem vektoru $\mathbf{k}$. Index tohoto prvku je označen ck. Klíč používaný zařízením poté odpovídá prvku k_{ck}. Cílem DPA útoku je nalézt, který sloupec matice $\mathbf{V}$ byl zpracováván během D operací šifrování a dešifrování a získat tak k_{ck}.

Krok 4: Určení závislosti proudové spotřeby na vnitřní hodnotě

Čtvrtým krokem DPA útoku je namapování matice $\mathbf{V}$ obsahující hypotézy vnitřních hodnot do matice $\mathbf{H}$ reprezentující hypotézy proudové spotřeby. V tomto kroku se využívá simulace proudové spotřeby kryptografického zařízení. Vytvořený model spotřeby přiřadí každé hypotetické vnitřní hodnotě $v_{i,j}$ hypotetickou hodnotu proudové spotřeby $h_{i,j}$.

Čím větší má útočník znalosti o analyzovaném zařízení, tím lepší simulaci spotřeby je schopen vytvořit a tím zefektivnit DPA útok. Mezi často využívané modely spotřeby patří model Hammingovy vzdálenosti a Hammingovy váhy.

Krok 5: Porovnání hypotetických hodnot proudové spotřeby se změřenými průběhy

V posledním kroku DPA útoku se porovnávají hypotetické hodnoty proudové spotřeby závislé na odhadu klíče (hodnoty ve sloupci $\mathbf{h}_i$ matice $\mathbf{H}$) se změřenými průběhy (hodnoty ve sloupci $\mathbf{t}_j$ matice $\mathbf{T}$). Výsledkem je matice $\mathbf{R}$ o velikosti $K \times T$. Každý prvek $r_{i,j}$ matice $\mathbf{R}$ je výsledkem porovnání mezi sloupci $\mathbf{h}_i$ a $\mathbf{t}_j$. Čím větší je hodnota prvku $r_{i,j}$, tím je míra lineární závislosti (korelace) mezi sloupci $\mathbf{h}_i$ a $\mathbf{t}_j$ větší. Porovnávání může být provedeno prostřednictvím různých metod. Na obr. 2.3 jsou graficky znázorněny kroky 3 až 5.

Naměřené průběhy vyjadřují proudovou spotřebu zařízení při vykonávání šifrovacího algoritmu pro různá vstupní data. Zvolená vnitřní hodnota z kroku 1 je součástí tohoto algoritmu. Zařízení tedy během každého procesu šifrování či dešifrování různých vstupních dat pracuje s vnitřními hodnotami $\mathbf{v}_{ck}$. Tzn., že naměřené průběhy jsou v určitých pozicích na těchto vnitřních hodnotách závislé. Tuto pozici lze označit jako ct a platí, že hodnoty proudové spotřeby ve sloupci $\mathbf{t}_{ct}$ závisí na vnitřních hodnotách $\mathbf{v}_{ck}$.

Na základě vnitřních hodnot $\mathbf{v}_{ck}$ byly útočníkem nasimulovány hypotetické hodnoty proudové spotřeby $\mathbf{h}_{ck}$. Proto platí, že sloupce $\mathbf{h}_{ck}$ a $\mathbf{t}_{ct}$ jsou na sobě silně závislé. Jejich korelací vznikne hodnota $r_{ck,ct}$ v matici $\mathbf{R}$, která bude nejvyšší v celé této matici. Protože ostatní sloupce matic $\mathbf{H}$ a $\mathbf{T}$ neprokazují takovou závislost, budou všechny ostatní hodnoty v matici $\mathbf{R}$ menší. Útočník je tedy schopen získat správný klíč k_{ck} pouhým nalezením nejvyšší hodnoty v matici $\mathbf{R}$.

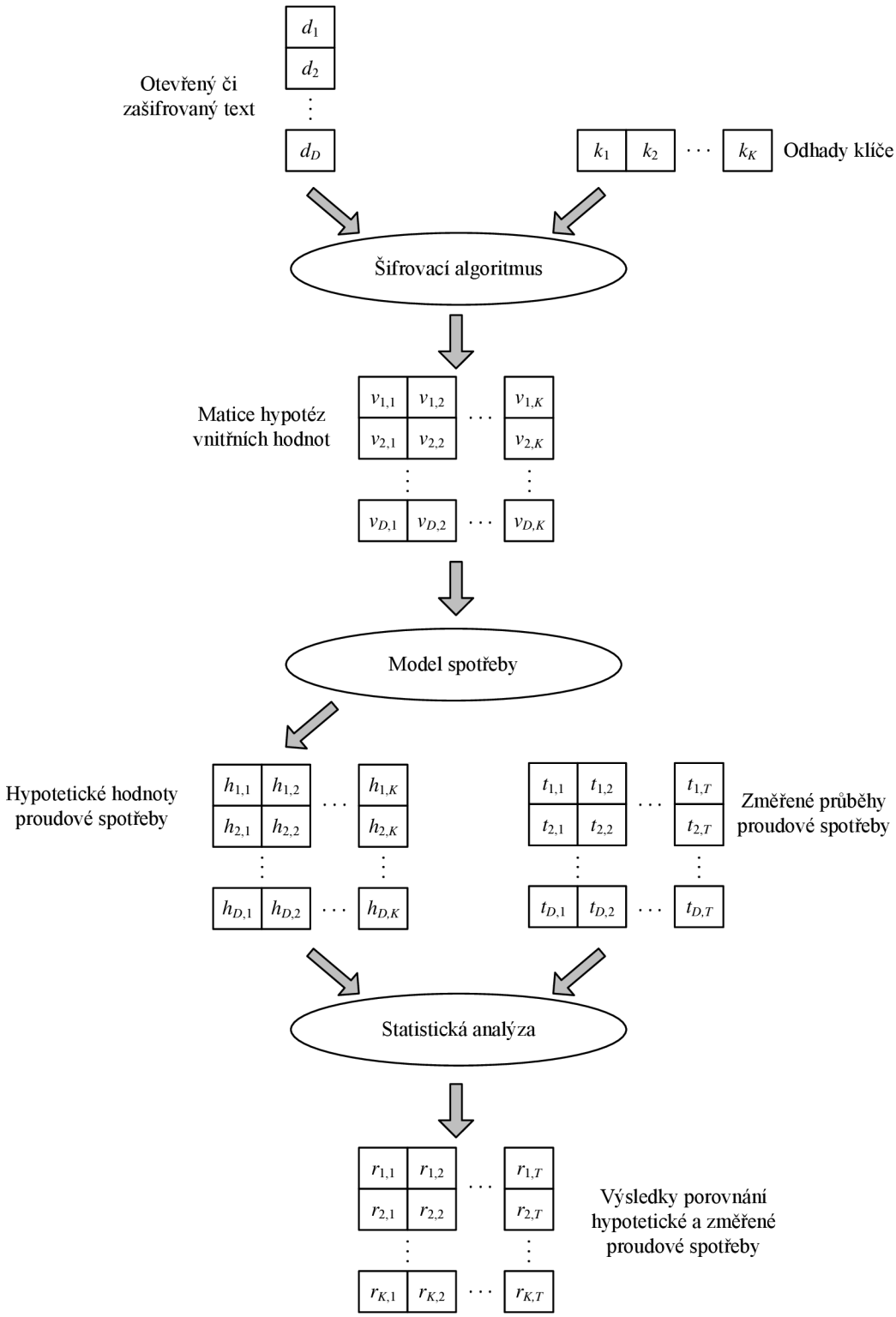
Při praktickém provedení DPA útoku se může stát, že hodnoty v matici $\mathbf{R}$ nabývají přibližně stejných hodnot. To je obvykle způsobeno nezměřením dostatečného množství průběhů proudové spotřeby ke stanovení závislosti mezi sloupci matic $\mathbf{H}$ a $\mathbf{T}$. Čím více průběhů bude naměřeno, tím budou sloupce matic $\mathbf{H}$ a $\mathbf{T}$ obsahovat více prvků a tím lze lépe charakterizovat vztah mezi sloupci.

2.3.4 Elektromagnetická analýza

Veškerá elektronická zařízení během své činnosti vytvářejí elektromagnetické záření. Pokud je vyzařované elektromagnetické pole dostatečně silné je možné jej zachytit a také analyzovat. Toto je však nežádoucí jev zejména pro kryptografická zařízení, u kterých by mohlo dojít k neúmyslnému úniku tajných informací prostřednictvím elektromagnetického postranního kanálu.

Elektromagnetický postranní kanál poprvé využil nizozemský vědec van Eck v roce 1985. Zjistil, že z elektromagnetického pole vyzařovaného počítačovým monitorem je schopen rekonstruovat informace, které jsou na monitoru zobrazeny.

Poslední výzkum v této oblasti ukázal, že útoky elektromagnetickým postranním kanálem na některá kryptografická zařízení umožňují získat více informací, jenž prostřednictvím proudového postranního kanálu lze získat jen velmi obtížně.



Obr. 2.3: Blokový diagram znázorňující kroky 3 až 5 DPA útoku [13].

3 TEORETICKÝ ÚVOD PRO MĚŘENÍ

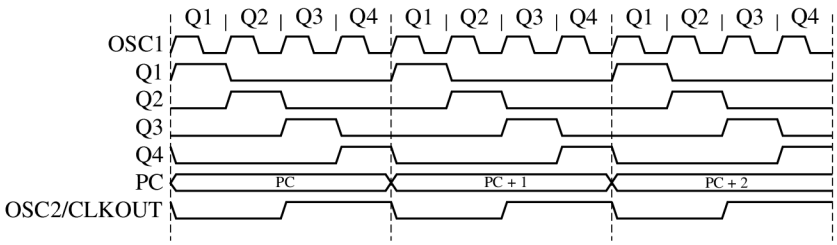
Tato kapitola vysvětluje základní princip fungování použitého mikrokontroléru MCU (Microcontroller) PIC16F84A a šifrovacího standardu AES (Advanced Encryption Standard). Získané znalosti budou uplatněny v praktické části, ve které je mikrokontrolér naprogramován pro vykonávání požadovaných instrukcí podle šifrovacího standardu AES.

3.1 Mikrokontroléry řady PIC16F8X

Protože problematika mikrokontrolérů netvoří hlavní náplň této práce, jsou zde uvedeny pouze nutné informace potřebné k pochopení, jak MCU vykonává jednotlivé instrukce programu.

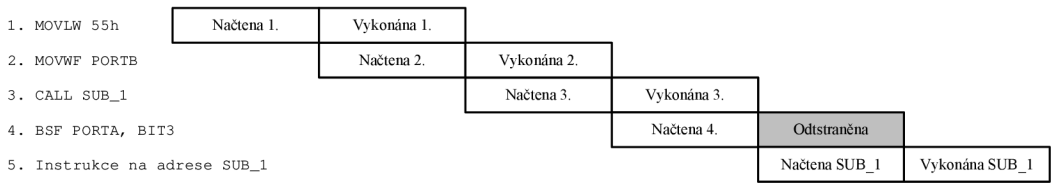
Mikrokontroléry PIC16F8X patří do rodiny osmibitových MCU založených na architektuře RISC (Reduced Instruction Set Computer), tzn. pracují pouze s omezenou sadou strojových instrukcí, ale zato vysokou rychlostí. Všechny MCU z řady PIC16F8X mají oddělenou instrukční a datovou sběrnici. Jsou tedy postaveny na Harvardské architektuře. Mezi další vlastnosti patří dvouúrovňové zřetězení instrukcí (tzv. pipelining), které umožňuje zpracování všech instrukcí v jednom cyklu. Tato vlastnost neplatí, pokud se v programu nachází instrukce větvení, na její vykonání jsou potřeba cykly dva. Instrukční sadu těchto MCU tvoří celkem 35 instrukcí, rozdělené do tří skupin – bajtově orientované, bitově orientované a řídící.

Jakým způsobem MCU vykonává jednotlivé instrukce programu je znázorněno na obr. 3.1. Hodinový signál z oscilátoru přivedený na vstup OSC1 je dělen čtyřmi. Tím vzniknou čtyři nepřekrývající se cykly Q1, Q2, Q3 a Q4, které tvoří celý instrukční cyklus. Programový čítač MCU při každém cyklu Q1 zvětší svoji hodnotu o 1. Instrukce je během cyklu Q1 načtena z paměti programu, při Q2 dojde k jejímu dekódování, v průběhu Q3 je vykonána a nakonec při cyklu Q4 je výsledek vykonané instrukce zapsán do registru.



Obr. 3.1: Instrukční cyklus mikrokontroléru PIC16F8X.

Mikrokontroléry řady PIC16F8X umožňují, jak bylo zmíněno výše, dvouúrovňové zřetězení po sobě jdoucích instrukcí. Tato funkce se nazývá pipelining a její princip znázorňuje obr. 3.2. Zřetězení probíhá tak, že nejprve je z paměti programu načtena první instrukce a v průběhu, kdy je vykonávána, dochází k načtení instrukce následující. Vykonaní každé instrukce tedy trvá jeden cyklus. To ovšem neplatí pro instrukce způsobující větvení programu. Na obr. 3.2 lze pozorovat, že při vykonávání instrukce `CALL_SUB1` (volání podprogramu) je načtena instrukce `BSF PORTA, BIT3`. V okamžiku, kdy je dokončeno vykonávání instrukce `CALL_SUB1`, MCU zapíše adresu instrukce `BSF PORTA, BIT3` do zásobníku (ukládá návratové adresy) a změní hodnotu programového čítače PC na adresu návěstí `SUB_1`. Načtená instrukce `BSF PORTA, BIT3` je tedy odstraněna (zahozena). Z toho vyplývá, že instrukce pro větvení programu jsou vykonávány ve dvou cyklech, neboť do jejich úplného vykonání nelze načíst další instrukci.



Obr. 3.2: Zřetězení instrukcí „pipelining“.

V praktické části této práce bude využit mikrokontrolér PIC16F84A. Jeho rozložení pinů v pouzdře je uvedeno v přiloženém katalogovém listu na CD. Podrobné informace o použitém MCU lze čerpat z literatury [15, 16].

3.2 Advanced Encryption Standard AES

V roce 1997 Americký úřad pro standardy a technologie NIST (National Institute of Standards and Technology) zahájil proces vytvoření nového šifrovacího standardu AES, který by byl schopný poskytnout dostatečné zabezpečení pro citlivé vládní informace a nahradil zastaralý standard DES [4]. Po zdlouhavém procesu byl na konci roku 2001 zvolen algoritmus Rijndael, pojmenovaný podle tvůrců Joana Daemena a Vincenta Rijmena, jako nový AES standard. Celé znění standardu AES je možné nalézt v literatuře [5].

Algoritmus AES umožňuje zašifrování vstupní bitové posloupnosti o délce 128 bitů do 128 bitové výstupní posloupnosti. Tyto vstupní a výstupní bitové posloupnosti jsou označovány jako bloky dat otevřeného a šifrovaného textu. Šifrovací klíče algoritmu AES mohou podle standardu nabývat délky 128, 192 či 256 bitů. Podle

délky šifrovacího klíče existují různé varianty AES, a to AES-128, AES-192 a AES-256.

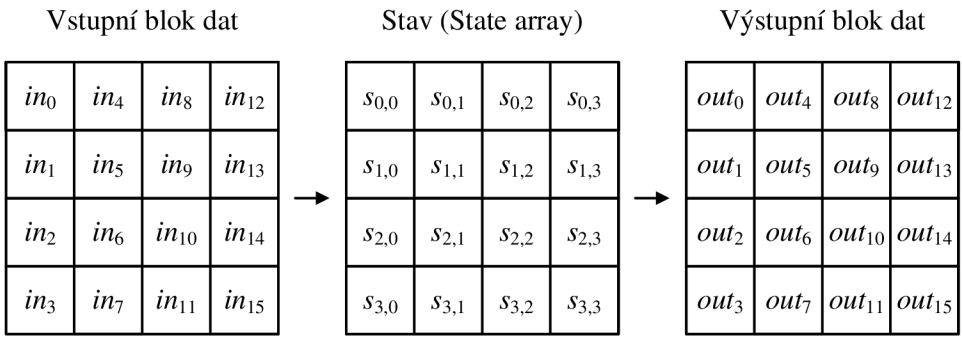
Celý proces šifrování a dešifrování vstupního bloku dat, jak znázorňuje obr. 3.8, probíhá v tzv. rundách (Rounds), které se skládají ze čtyř transformací. Pokud je vstupní blok dat šifrován, dochází k jeho modifikaci za pomoci těchto transformací: `SubBytes`, `ShiftRows`, `MixColumns` a `AddRoundKey`. Při dešifrování se pracuje s inverzními transformacemi, tedy `InvSubBytes`, `InvShiftRows`, `InvMixColumns` a `AddRoundKey`. Jak tyto transformace probíhají, je podrobněji popsáno v následující části. Počet rund, kterými vstupní blok dat musí opakovaně projít, závisí na délce použitého klíče (viz tab. 3.1).

Tab. 3.1: Počet rund pro různé varianty AES.

Varianta AES	Délka vstupního bloku	Délka klíče	Počet rund
AES-128	128 bitů	128 bitů	10 rund
AES-192	128 bitů	192 bitů	12 rund
AES-256	128 bitů	256 bitů	14 rund

3.2.1 Proces šifrování pomocí AES

Algoritmus AES provádí výše zmíněné transformace na dvojrozměrném poli bajtů velikosti 4×4 označovaném jako *Stav* (State array). Každý bajt v tomto poli je označen dvěma indexy, číslem řádku r a číslem sloupce c. Pozice jednotlivých bajtů $s_{r,c}$ jsou tedy jednoznačně určeny. Na začátku procesu šifrování či dešifrování je vstupní blok dat nejprve nakopírován do dvojrozměrného pole *Stavu* a po finální rundě nakopírován z pole *Stavu* do výstupního bloku dat (viz obr. 3.3).



Obr. 3.3: Dvojrozměrné pole bajtů (*Stav*).

Key Expansion

Algoritmus AES vytvoří z šifrovacího klíče jednotlivé rundovní klíče, podrobněji popsáno v literatuře [5].

Inicializační fáze

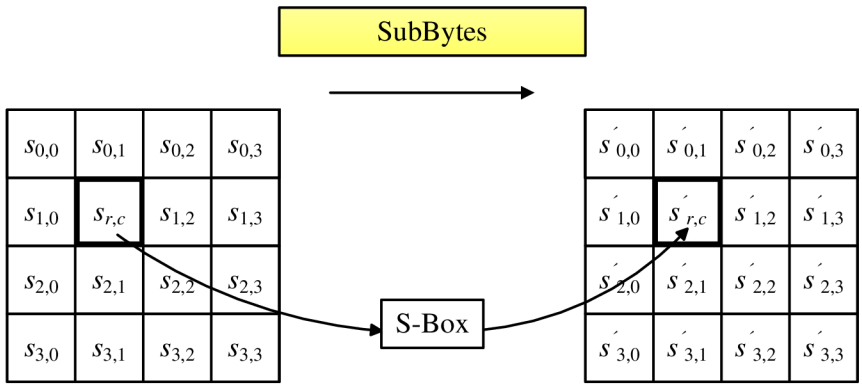
Každý bajt *Stavu* je kombinován s příslušným bajtem šifrovacího klíče prostřednictvím bitové funkce XOR (Exclusive disjunction), jejíž pravdivostní hodnoty jsou uvedeny v tab. 3.2. Tato transformace se nazývá `AddRoundKey`.

Tab. 3.2: Pravdivostní tabulka logické operace XOR.

B	A	A $\oplus$ B
0	0	0
0	1	1
1	0	1
1	1	0

`SubBytes` transformace

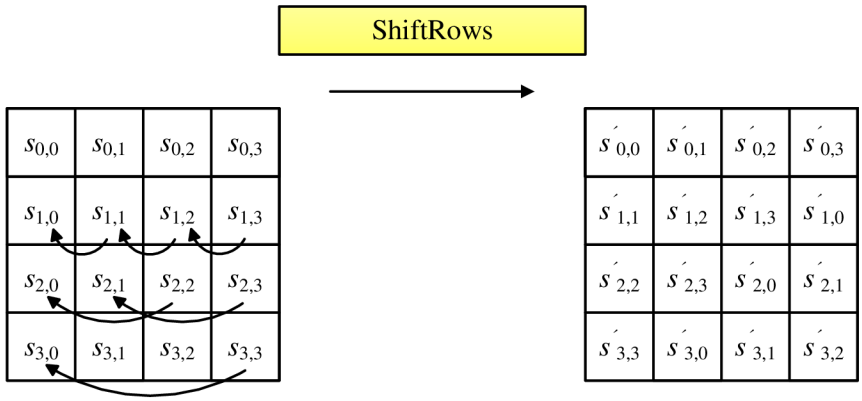
Tato nelineární transformace provede substituci (nahrazení) každého bajtu vytvořeného v inicializační fázi hodnotou v substituční tabulce, tzv. S-boxu (viz obr. 3.4).



Obr. 3.4: Transformace `SubBytes`.

`ShiftRows` transformace

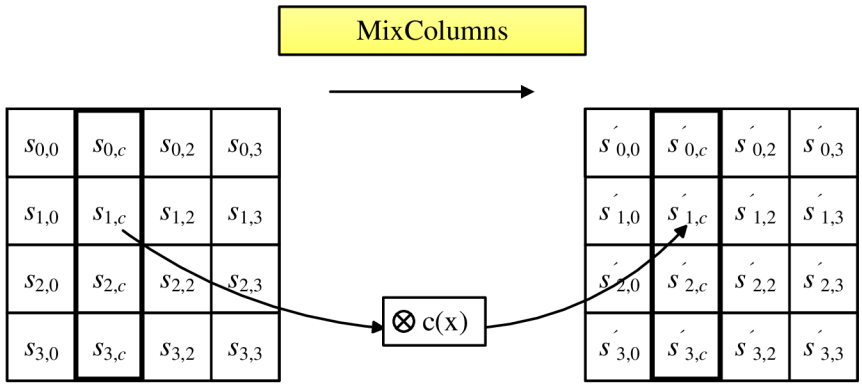
Bajty v posledních třech řádcích *Stavu* jsou cyklicky posunuty doleva o určitý počet kroků. Počet kroků, o které je bajt v řádku matice posunut, udává číslo řádku matice. První řádek se označuje jako nultý (viz obr. 3.5).



Obr. 3.5: Transformace `ShiftRows`.

`MixColumns` transformace

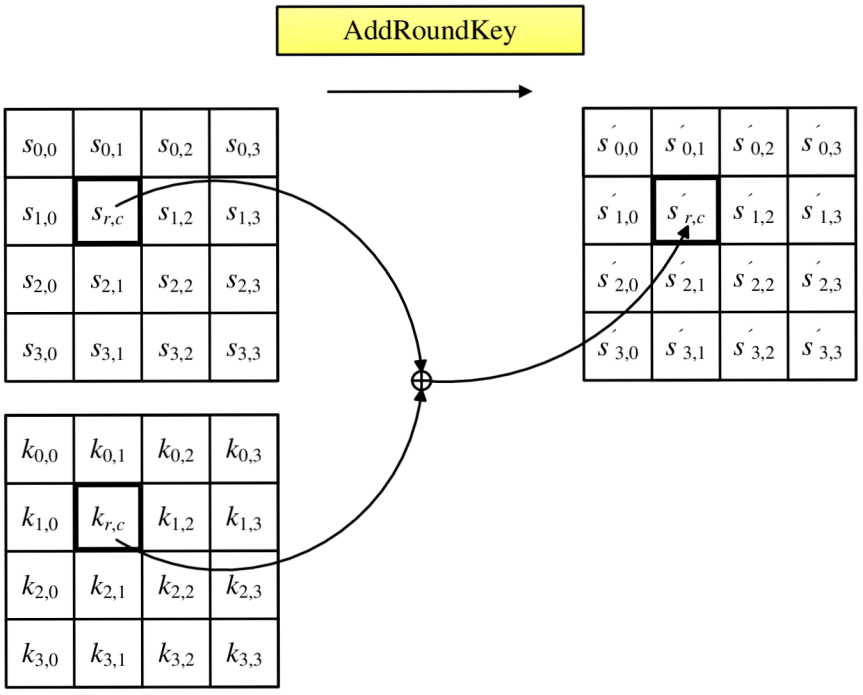
Při této transformaci je každý sloupec *Stavu* vynásoben pevně daným polynomem $c(x)$ (viz obr. 3.6).



Obr. 3.6: Transformace `MixColumns`.

`AddRoundKey` transformace

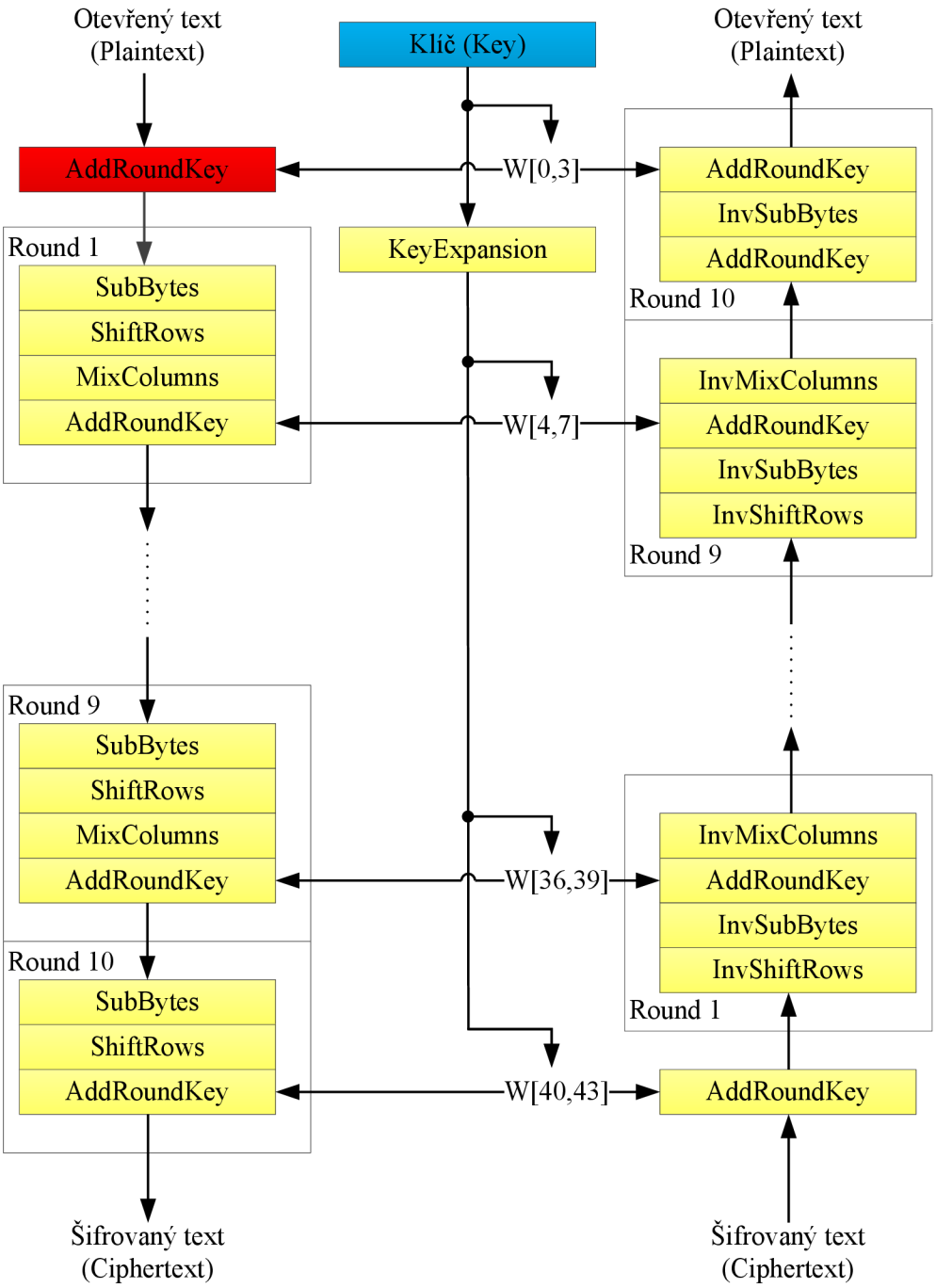
Každý bajt *Stavu* je kombinován s příslušným bajtem rundovního klíče prostřednictvím bitové funkce XOR. Tato transformace odpovídá inicializační fázi. Využívá se však rundovních klíčů odvozených z hlavního šifrovacího klíče (viz obr. 3.7).



Obr. 3.7: Transformace `AddRoundKey`.

Pruběh finální rundy

Finální runda je identická jako devět předchozích. Obsahuje však pouze transformace `SubBytes`, `ShiftRows`, a `AddRoundKey`.



Obr. 3.8: Princip šifrování (dešifrování) algoritmem AES-128 [2].

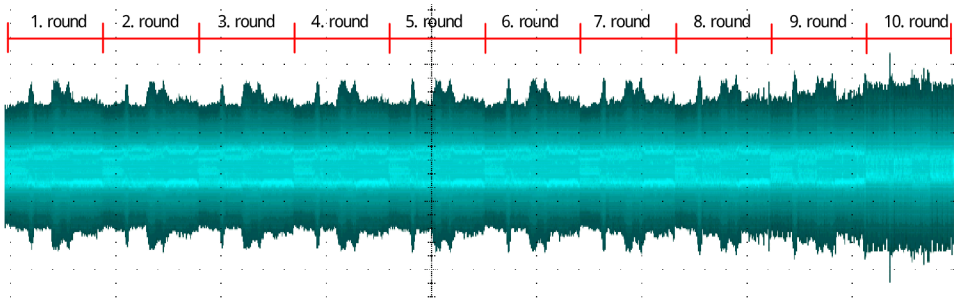
3.2.2 Provedení SPA/DPA algoritmu AES

V této části práce jsou prezentovány jednoduché příklady znázorňující SPA a DPA útok na šifrovací algoritmus AES nebo jeho část. Stejné či podobné postupy budou poté využity v praktické části pro konkrétní zadání.

Příklad SPA útoku

Šifrovací algoritmus v kryptografickém zařízení je vykonáván jako posloupnost různých operací. Tyto operace jsou přeloženy na instrukce, které zařízení podporuje.

V případě softwarové implementace algoritmu AES do mikrokontroléru jsou jednotlivé rundy implementovány jako sekvence instrukcí z používaného instrukčního souboru. Instrukční soubor obsahuje základní aritmetické a logické instrukce a také instrukce pro přesun dat a větvení programového kódu. Každá instrukce pracuje s různými hodnotami dat a různými částmi mikrokontroléru, které mají rozdílnou proudovou spotřebu. V měřeném průběhu proudové spotřeby zanechávají svůj specifický otisk. Na obr. 3.9 je znázorněn průběh spotřeby šifrovacího algoritmu AES, ve kterém lze rozeznat jeho jednotlivé rundy.



Obr. 3.9: Jednoduchá analýza šifrovacího algoritmu AES [19].

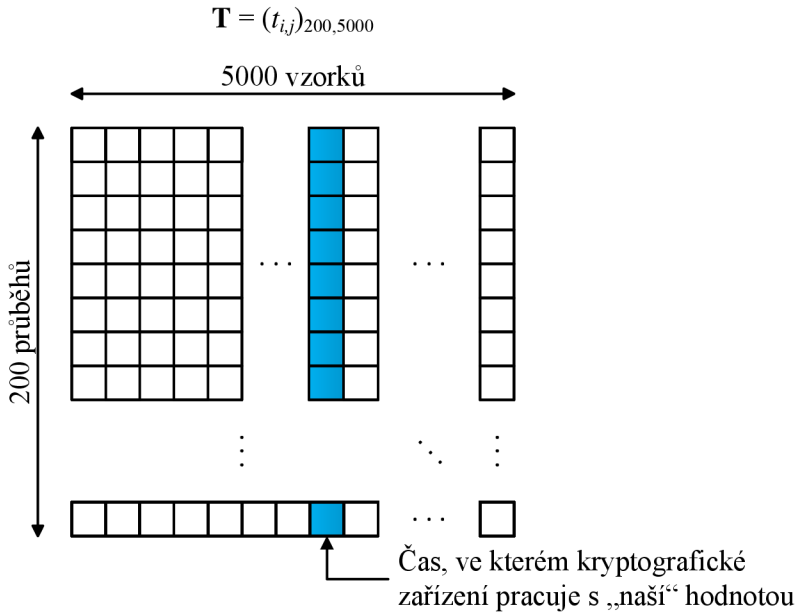
Příklad DPA útoku

V následujícím příkladě DPA útoku[1] je do mikrokontroléru implementována jen část algoritmu AES. AES vykonává pouze operaci `AddRoundKey` a operaci `SubBytes`. Postup útoku odpovídá obecnému popisu v kapitole 2.3.3.

V prvním kroku DPA útoku je nejprve zvolena vnitřní hodnota algoritmu AES. Tato hodnota závisí na známých datech a části klíče, jenž lze odhadnout. Pro konkrétní útok byl zvolen první výstupní bajt operace `SubBytes` v první rundě AES.

[1]Data potřebná pro demonstraci DPA útoku získána z http://www.cs.bris.ac.uk/home/eoswald/opensca.html

V dalším kroku jsou změřeny průběhy proudové spotřeby mikrokontroléru pro první rundu AES při šifrování 200 náhodných bloků otevřeného textu. Naměřené vzorky spotřeby vytvoří matici $\mathbf{T}$ (viz obr. 3.10).

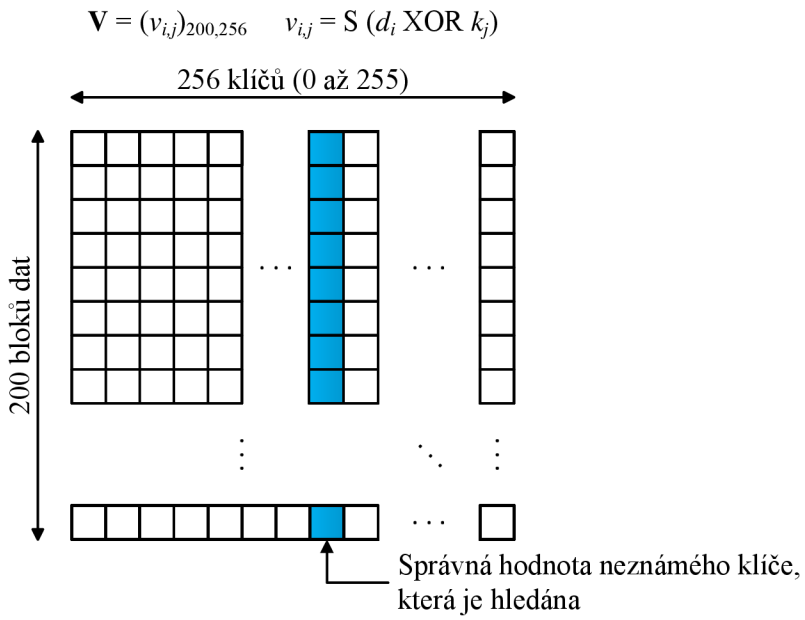


Obr. 3.10: Matice změřených průběhů proudové spotřeby.

Třetí krok DPA útoku spočívá ve stanovení hypotéz vnitřních hodnot algoritmu AES. Tyto hodnoty jsou určeny pro 200 bloků známého otevřeného textu. Výsledkem bude matice $\mathbf{V}$. Pro její prvky platí $v_{i,j} = S(d_i \oplus k_j)$, kde $d_1, \ldots, d_{200}$ je první bajt z každého bloku otevřeného textu a $k_j = j-1$ pro $j = 1, \ldots, 256$. Matice $\mathbf{V}$ obsahuje celkově 200×256 hypotéz vnitřních hodnot (viz obr. 3.11).

Ve čtvrtém kroku je každé hypotetické vnitřní hodnotě $v_{i,j}$ z matice $\mathbf{V}$ přiřazena hypotetická hodnota proudové spotřeby $h_{i,j}$. K tomu je nutné vytvořit simulaci proudové spotřeby kryptografického zařízení, tzv. model spotřeby. Zpravidla má útočník jen omezené množství informací o napadeném zařízení, a proto se snaží využít, co možná nejjednodušší model proudové spotřeby. Mezi nejběžnější patří model Hammingovy vzdálenosti a Hammingovy váhy.

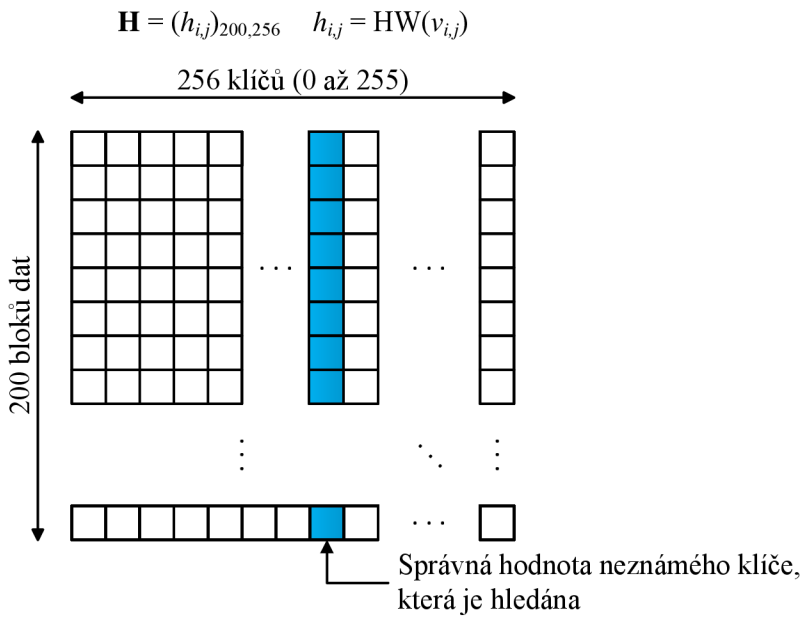
Hammingova vzdálenost dvou binárních hodnot v_0 a v_1 odpovídá Hammingově váze (HW) binární hodnoty získané výlučným součtem $v_0 \oplus v_1$. Hammingova váha je určena počtem bitů s logickou hodnotou 1. Platí tedy, že $HW(v_0 \oplus v_1)$ udává počet bitů, ve kterých se dvě binární hodnoty v_0 a v_1 liší. Model Hammingovy vzdálenosti lze uplatnit pro popis proudové spotřeby datové sběrnice mikrokontroléru, pokud na ní dochází ke změně hodnoty v_0 na hodnotu v_1. V případě modelu Hammingovy váhy se předpokládá, že proudová spotřeba kryptografického zařízení je úměrná počtu



Obr. 3.11: Matice hypotéz vnitřních hodnot.

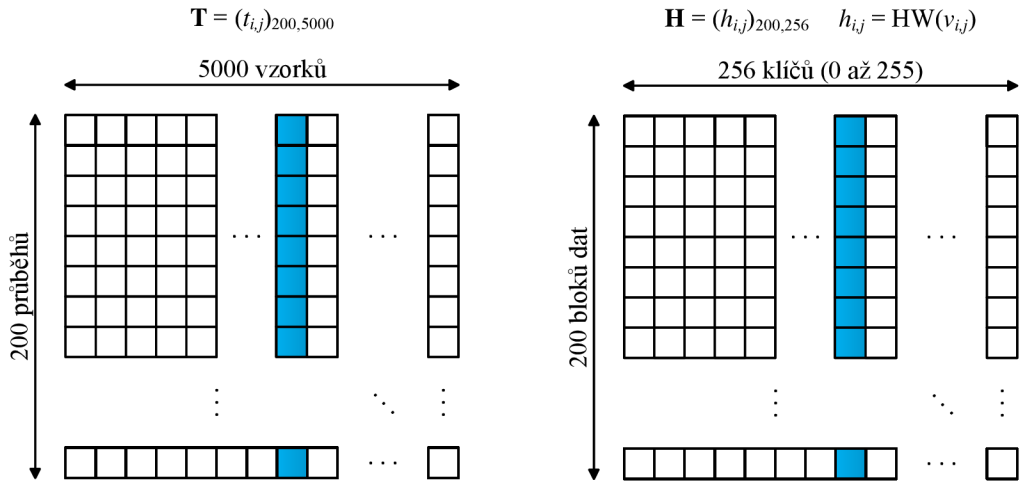
bitů právě zpracovávaných dat, které mají logickou hodnotu 1. Z toho vyplývá, že s rostoucí Hammingovou váhou dat roste proudová spotřeba zařízení.

V uvedeném příkladě je použit model Hammingovy váhy. Jeho aplikací na matici **V** hypotetických vnitřních hodnot vznikne matice **H** pro hypotézy proudové spotřeby (viz obr. 3.12).



Obr. 3.12: Matice hypotéz proudové spotřeby.

Poslední krok DPA útoku slouží k vyhodnocení míry lineární závislosti (korelace) hypotéz proudové spotřeby pro všechny odhady klíče (hodnoty ve sloupci $\mathbf{h}_i$ matice $\mathbf{H}$) a změřených průběhů (hodnoty ve sloupci $\mathbf{t}_j$ matice $\mathbf{T}$). Obě matice znázorňuje obr. 3.13.



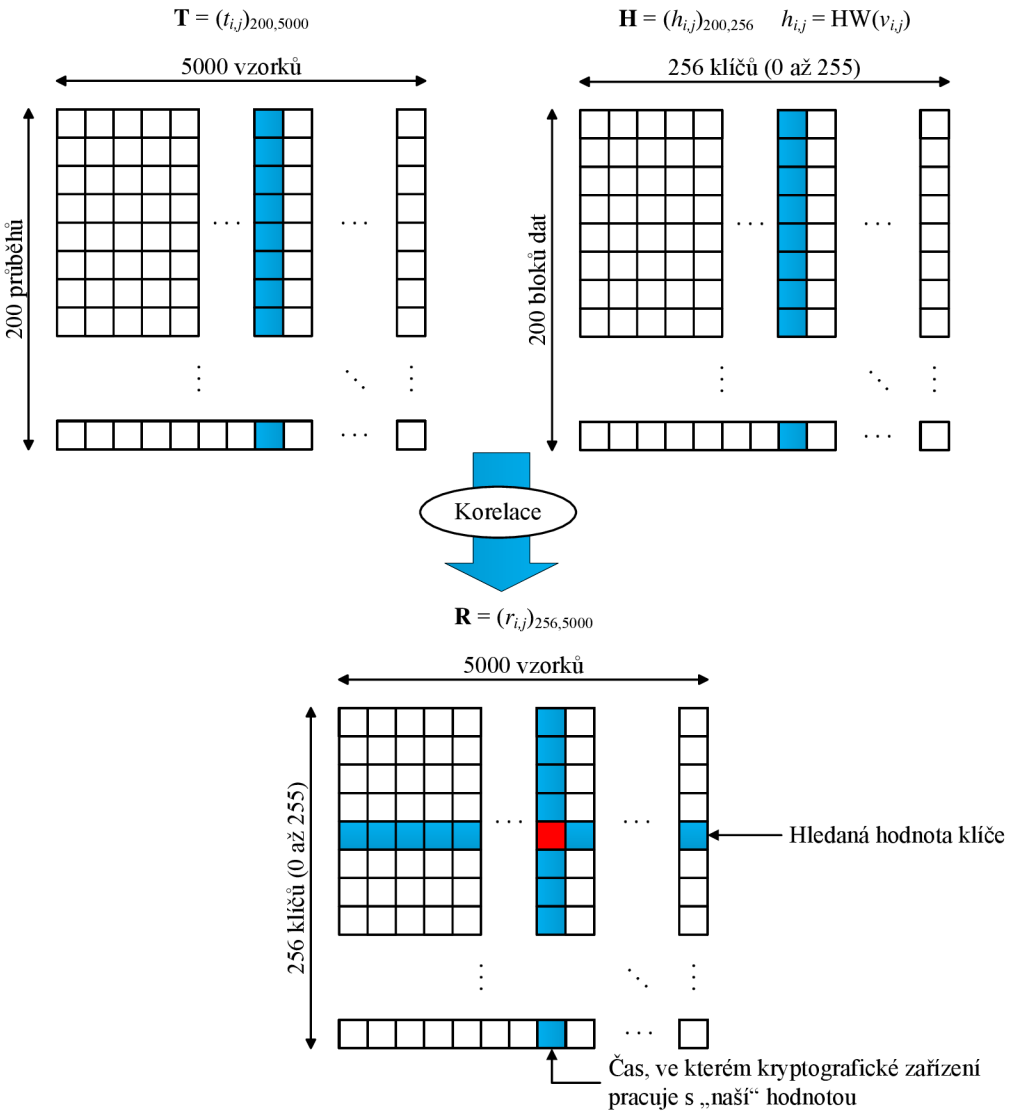
Obr. 3.13: Porovnání matice naměřených průběhů a hypotéz proudové spotřeby.

K vyhodnocení míry lineární závislosti mezi sloupci $\mathbf{h}_i$ a $\mathbf{t}_j$, kde $i = 1, \ldots, K$ a $j = 1, \ldots, T$, se využívá různých metod. Např. korelační koeficient, rozdíl průměrů, vzdálenost průměrů atd. Ze zmíněných metod je nejčastěji používán korelační koeficient. Výsledkem této metody je matice $\mathbf{R}$ korelačních koeficientů (viz obr. 3.14). Každá hodnota korelačního koeficientu $r_{i,j}$ je určena následovně [13]:

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

Hodnoty $\overline{h_i}$ a $\overline{t_j}$ označují průměrné hodnoty prvnků ve sloupcích $\mathbf{h}_i$ a $\mathbf{t}_j$. D udává počet těchto prvků.

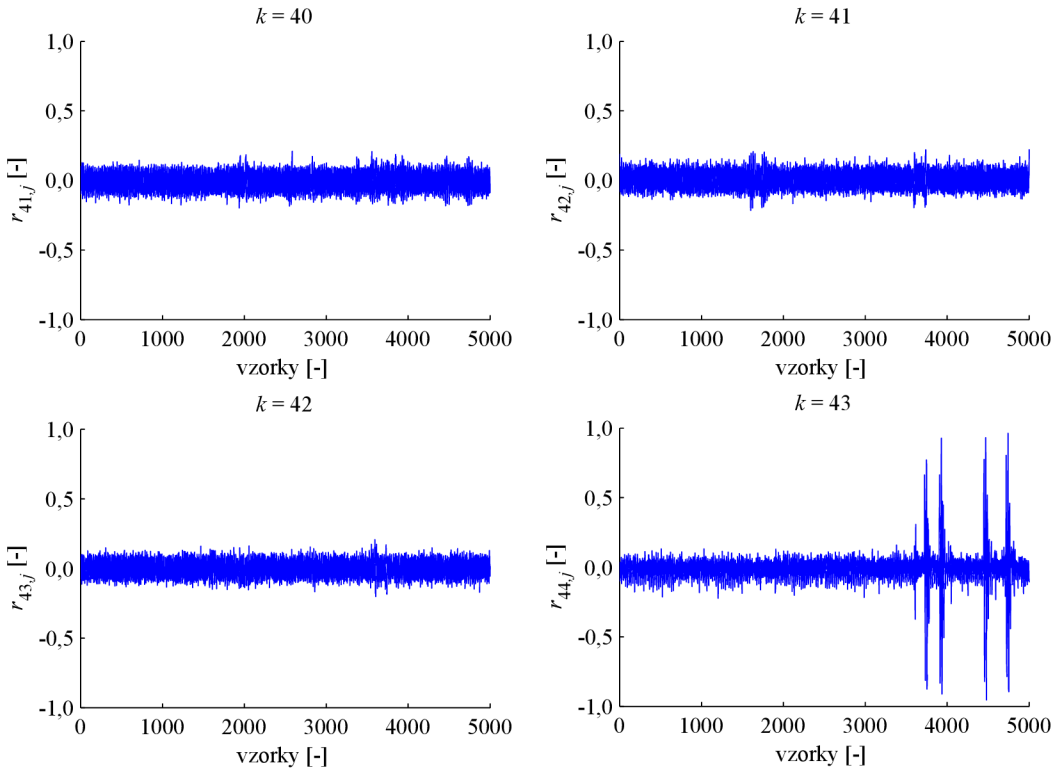
Matici $\mathbf{R}$ lze zobrazit jako množinu grafů. Každý graf znázorňuje jeden řádek matice $\mathbf{R}$, tedy jednu hypotézu (odhad) klíče. Na obr. 3.15 jsou zachyceny grafické průběhy pro hypotézy klíče 40 až 43 právě provedeného útoku. V průběhu pro hypotézu klíče 43 lze pozorovat velké špičky. Tyto špičky jsou ve skutečnosti nejvyšší v celé matici $\mathbf{R}$. Všechny ostatní hodnoty matice $\mathbf{R}$ jsou výrazně menší. Tato skutečnost poskytuje útočníkovi množství důležitých informací. Jedna z nejdůležitějších je, že první bajt tajného klíče má hodnotu 43. Z počtu špiček daného průběhu dále vyplývá, že mikrokontrolér s touto vnitřní hodnotou pracuje v několika instrukcích. To je zpravidla obvyklé pro softwarovou implementaci šifrovacího algoritmu, kdy



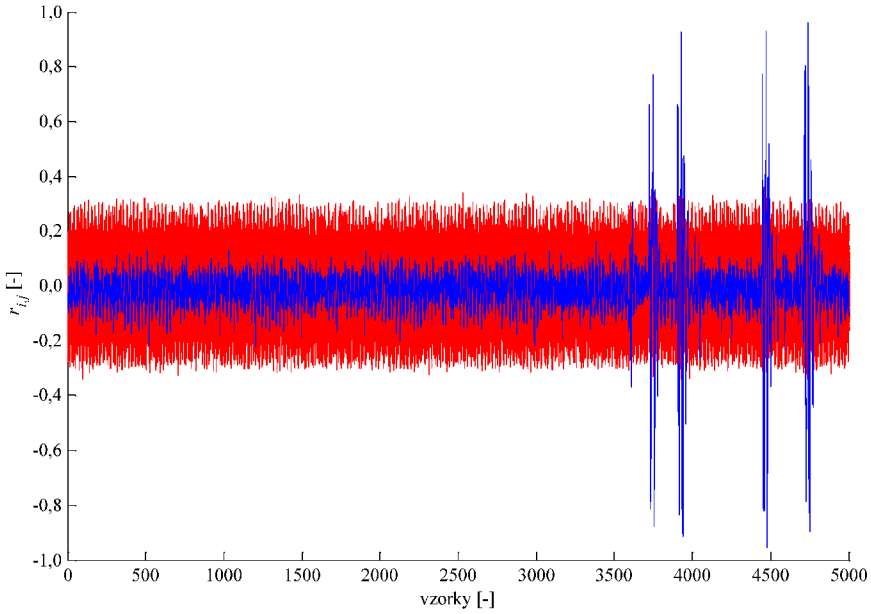
Obr. 3.14: Výpočet matice korelačních koeficientů.

při práci s hledanou vnitřní hodnotou dochází k přesunu této hodnoty mezi pamětí a registrem mikrokontroléru a obráceně.

Sloupce v matici **H** nejsou vzájemně všechny nezávislé. Pokud sloupec matice **H** vytvoří velkou hodnotu korelačního koeficientu, mohou i některé další sloupce vést k určité korelaci. Popsanou situaci lze pozorovat na obr. 3.15, ve kterém průběhy pro další hypotézy klíče také obsahují špičky. Ty jsou však výrazně menší a nezabrání odhalení klíče. Obr. 3.16 obsahuje průběhy pro všechny klíče. Průběh pro klíč 43 je modrý, zatímco pro ostatní klíče jsou průběhy červené. Významné špičky se nacházejí pouze v modrém průběhu.



Obr. 3.15: Řádky matice **R** pro hypotézy klíče 40 až 43.



Obr. 3.16: Všechny řádky matice **R** se zvýrazněnou hypotézou klíče 43.

4 NÁVRH MĚŘICÍHO PRACOVIŠTĚ

Pro měřicí účely byla navržena jednoduchá deska plošných spojů DPS s mikrokontrolérem PIC a potřebnými součástkami pro jeho správnou funkci. Realizovaná DPS představuje prostý kryptografický modul, na který bude aplikována jednoduchá proudová analýza. Pro diferenciální proudovou analýzu bude mikrokontrolér PIC přepojen do vývojové desky PICDEM 2 PLUS, která umožňuje komunikaci s počítačem přes sériové rozhraní RS-232. Této funkce bude využito pro kontrolu právě šifrovaných hodnot. V následující části je podrobněji popsáno zapojení obou vytvořených modulů a měřicí technika využitá při samotném měření.

4.1 Praktická realizace kryptografického modulu

Schéma zapojení DPS kryptografického modulu pro jednoduchou výkonovou analýzu je uvedeno v příloze B. Základ tvoří dvě patice (18 pinová a 40 pinová), které umožňují připojení dvou odlišných typů MCU. Hodinový signál pro MCU může být získán buď připojením krystalového oscilátoru do příslušné patice, nebo připojením externího generátoru signálu prostřednictvím BNC konektoru umístěným na desce. Volba zdroje hodinového signálu se provádí pomocí mechanické propojky na konektorové liště SV1. Proudová analýza kryptografického modulu je provedena proudovou sondou, která měří aktuální hodnotu proudu odebíraného modulem z napájecího zdroje. Technickým parametrům proudové sondy a jejímu správnému připojení do obvodu je věnována samostatná část. Na desce se také nachází konektorová lišta se čtyřmi vývody, z nichž tři jsou propojeny s příslušnými vstupy a výstupy MCU (RB0, RB1 a OSC1) a čtvrtý je uzemněn. Deska je v průběhu měření osazena pouze jedním MCU, lze tedy použít jen jednu konektorovou lištu. Na výstupu RB0 je generován obdélníkový signál, který slouží ke správné synchronizaci signálu měřeného proudovou sondou. Připojením napěťové sondy na výstup OSC1 lze na osciloskopu zobrazit hodinový signál krystalového oscilátoru nebo externího generátoru. Kromě výše uvedených se na desce nachází napájecí konektory pro připojení stejnosměrného napájecího zdroje.

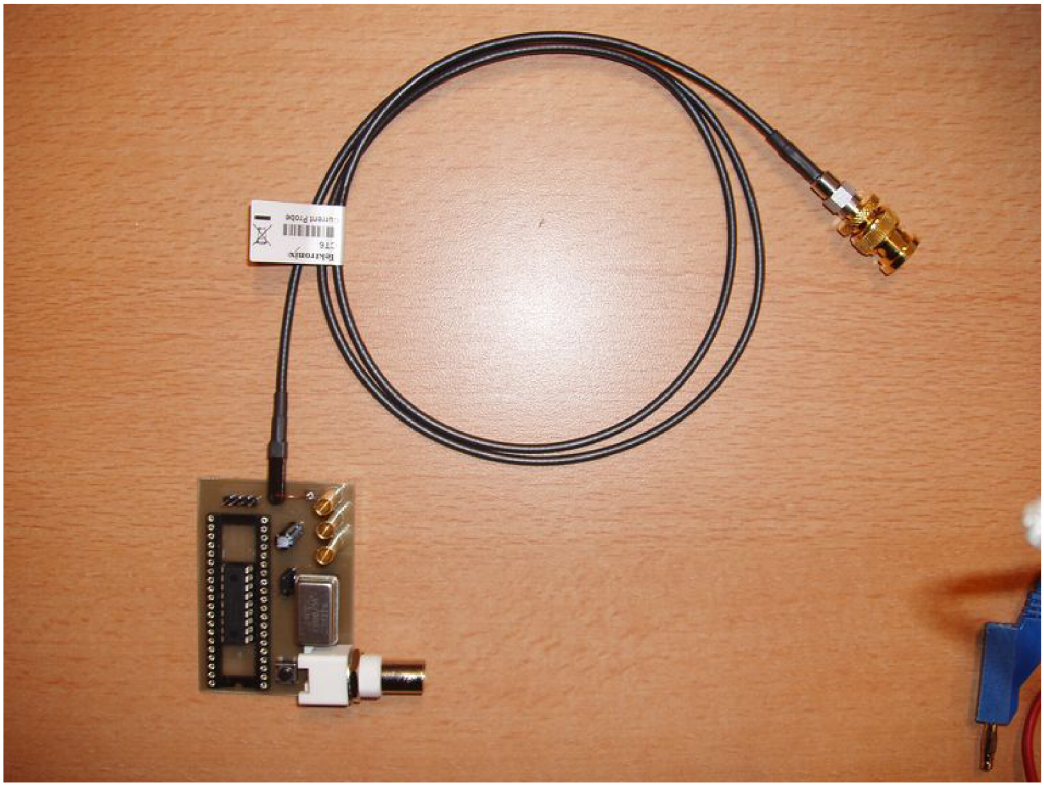
Pro diferenciální proudovou analýzu bude použit stejný typ MCU jako u jednoduché analýzy, avšak zapojen do vývojové desky PICDEM 2 PLUS od firmy Microchip. Výhoda desky spočívá v možnosti programového využití jejích hardwarových prvků. Zejména sériového rozhraní RS-232 pro komunikaci s počítačem a tlačítek pro změnu vstupních dat pro MCU. Podrobný popis všech prvků lze nalézt v uživatelském manuálu [17] a v elektronické příloze.

4.2 Technické parametry proudové sondy.

Proudová sonda CT-6 od firmy Tektronix je určena pro měření v nízkonapěťových, vysokofrekvenčních obvodech. Mezi její základní vlastnosti patří:

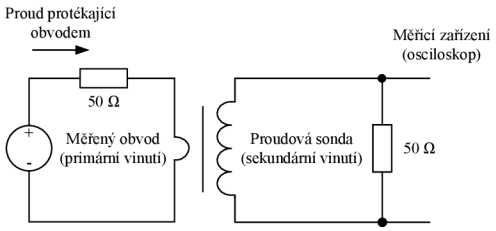
- šířka pásma 250 kHZ až 2 GHz,
- citlivost 5 mV/mA,
- nízká vstupní impedance,
- možnost měřit i injektovat signál.

Pro správné připojení proudové sondy do obvodu je nutné postupovat dle instrukcí uvedených v dodávaném manuálu [22]. Nejprve se sonda připojí k měřicímu zařízení (osciloskopu) pomocí SMA-BNC adaptéru. Měřený obvod se odpojí od napájecího zdroje. V tom místě obvodu, kde bude měřen protékající proud, se přeruší vodivá cesta a nahradí se drátovou propojkou (v našem případě dojde k přerušení cesty mezi zdrojem a napájecím vstupem MCU). Jako drátovou propojku je vhodné použít krátký vodič s malým průměrem, který je provlečen skrz sondu (viz obr. 4.1). Propojka se poté připájí na přerušené místo v obvodu. Je potřeba dodržet správnou polaritu podle polarizační tečky zobrazené na sondě. V posledním kroku se k obvodu připojí napájení a na osciloskopu se zobrazí průběh proudu protékající uvnitř obvodu.



Obr. 4.1: Připojení proudové sondy k měřenému obvodu.

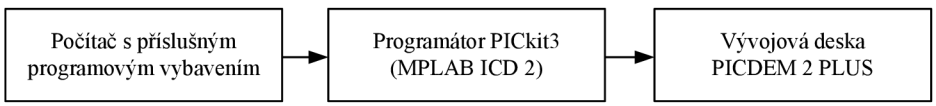
Proudová sonda se chová jako transformátor. Pokud je měřen proud protékající jedním vodičem, tak vodič představuje primární vinutí transformátoru a sonda tvoří sekundární vinutí (viz obr. 4.2).



Obr. 4.2: Princip měření proudu pomocí sondy.

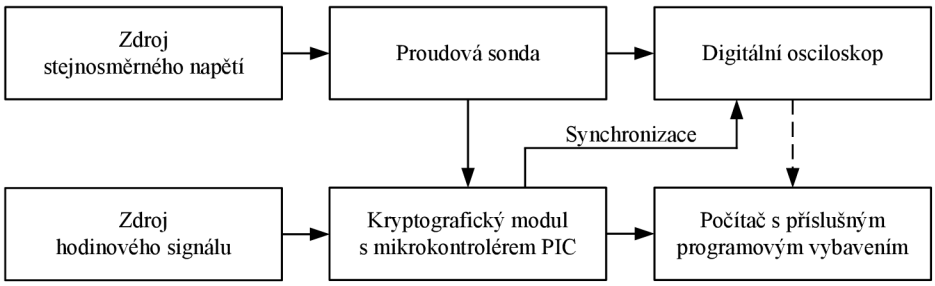
4.3 Měřicí pracoviště

Pracoviště, na kterém bude probíhat měření, se skládá ze dvou částí. První část (viz obr. 4.3) je tvořena počítačem s příslušným programovým vybavením a k němu připojeným programátorem s vývojovou deskou od firmy Microchip. Naprogramování MCU je provedeno pomocí vývojového prostředí MPLAB. Po úspěšném naprogramování je MCU z vývojové desky přepojen do patice sestaveného kryptografického modulu, na kterém bude probíhat měření.



Obr. 4.3: Blokové schéma pracoviště pro programování MCU.

Druhá část pracoviště (viz obr. 4.4) je tvořena stejnosměrným napájecím zdrojem pro napájení kryptografického modulu, zdrojem hodinového signálu, samotným modulem s naprogramovaným mikrokontrolérem PIC, digitálním osciloskopem a počítačem s vhodným programovým vybavením. Synchronizační signál je přiveden na první kanál osciloskopu pomocí napěťové sondy připojené na příslušný výstup modulu . Druhý kanál je použit pro připojení proudové sondy. Protože osciloskop i měřicí sondy jsou od stejného výrobce, lze v menu osciloskopu nastavit konkrétní typy připojených sond. Na základě zvoleného typu osciloskop automaticky provede nastavení parametrů zobrazovaných signálu.

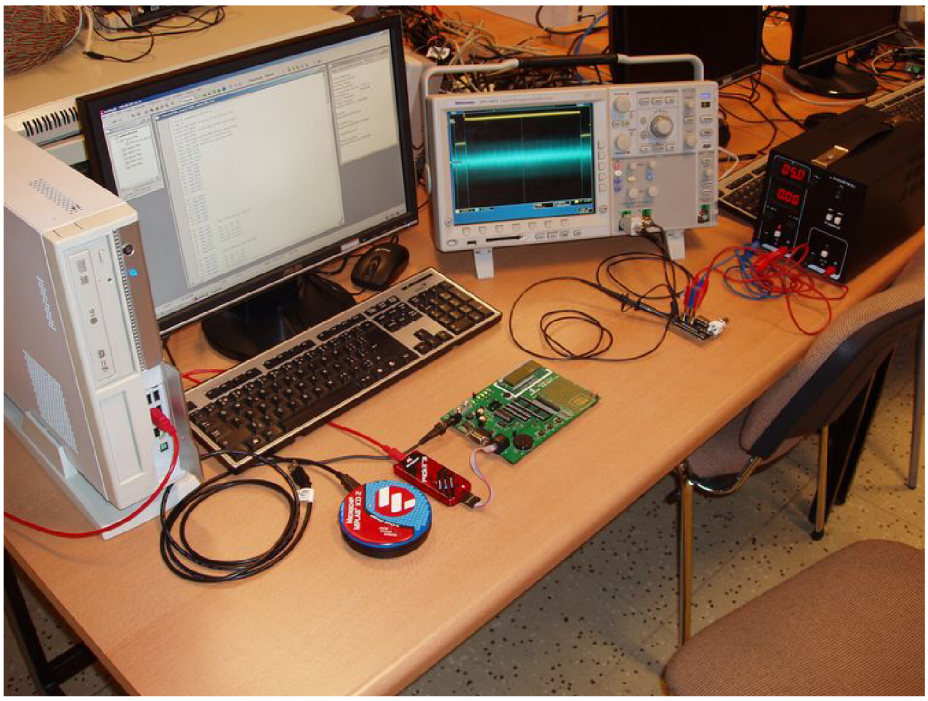


Obr. 4.4: Blokové schéma měřicího pracoviště.

Vybavení měřicího pracoviště

Měřicí pracoviště bylo sestaveno v laboratoři datových přenosů PA-339 (viz obr. 4.5). Jednotlivé komponenty jsou podrobněji popsány níže.

- **Počítač s příslušným programovým vybavením:** Počítač s operačním systémem Windows XP SP3 a nainstalovaným vývojovým prostředím MPLAB IDE v8.76 a programem na zpracování výsledků měření MATLAB v7.0.1.
- **Programátor PICkit 3 (MPLAB ICD 2):** Programátor slouží pro naprogramování mikrokontrolérů PIC a je ovládán pomocí vývojového prostředí MPLAB IDE v8.76.
- **Vývojová deska PICDEM 2 PLUS:** Vývojová deska umožňuje připojit a naprogramovat 18, 28 a 40 pinové mikrokontroléry řady PIC16X a PIC18X.
- **Napájecí zdroj Diametral P130R51D:** Laboratorní zdroj poskytuje na svém výstupu stejnosměrné regulovatelné napětí 30 V/4 A.
- **Digitální osciloskop Tektronix DPO-4032:** Dvoukanálový digitální osciloskop se vzorkovacím kmitočtem 2,5 GSa/s a šířkou pásma 350 MHz. Měřené průběhy ukládá na externí paměťové zařízení.
- **Kryptografický modul s mikrokontrolérem PIC16F84A:** Zařízení, na kterém je prováděna proudová analýza.
- **Proudová sonda Tektronix CT-6:** Proudová sonda pro měření průběhů proudu v kryptografickém modulu, podrobněji popsána výše v kapitole 4.2.
- **Napěťová sonda Tektronix P6139A:** Napěťová sonda pro přivedení synchronizačního signálu na první kanál osciloskopu.



Obr. 4.5: Sestavené měřicí pracoviště.

5 VÝSLEDKY MĚŘENÍ

Analýza proudového postranního kanálu sestaveného kryptografického modulu je provedena pomocí proudové sondy Tektronix CT-6. Sonda snímá aktuální proudový odběr modulu z napájecího zdroje. Naměřené hodnoty proudu jsou současně zobrazeny na osciloskopu a poté přeneseny do počítače k dalšímu zpracování. Cílem měření je provést jednoduchou a diferenciální proudovou analýzu mikrokontroléru PIC16F84A, který představuje jádro vytvořeného modulu. Ten cyklicky vykonává požadované operace šifrovacího algoritmu AES, na které jsou prováděné analýzy cíleny. Měření byla provedena na pracovišti popsané v kapitole 4.

5.1 Jednoduchá proudová analýza

Mikrokontrolér PIC16F84A byl pro jednoduchou proudovou analýzu naprogramován upravenou implementací šifrovacího algoritmu AES, která obsahovala pouze inicializační fázi `AddRoundKey`. Jak bylo vysvětleno v kapitole 3.2.1, tato funkce provádí bitovou operaci XOR mezi bajty vstupního bloku dat (otevřeného textu) a příslušnými bajty klíče. Analýza byla provedena pro různé hodnoty napájecího napětí a kmitočty hodinového signálu. Také je diskutován vliv nastavení snímacího módu osciloskopu.

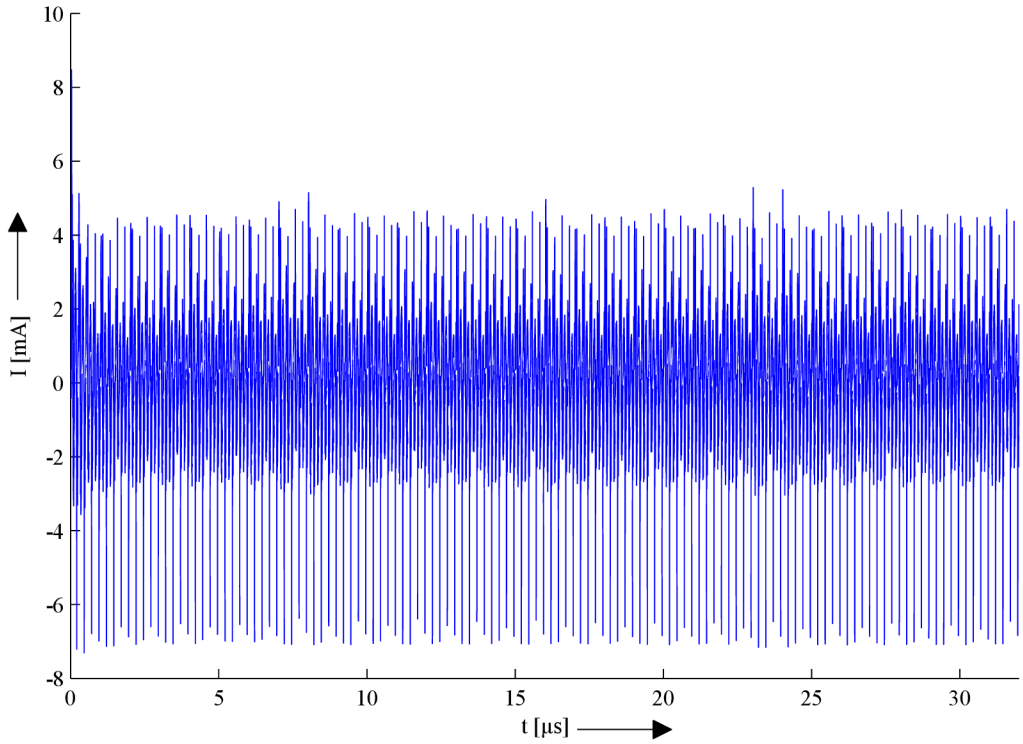
Měření proudového odběru kryptografického modulu proběhlo ve dvou fázích, přičemž byl využit model Hammingovy váhy klíče popsaný v kapitole 3.2.2.

V první fázi měření pracoval MCU s nulovou maticí otevřeného textu **M** a nulovou matici tajného klíče **K**. Znamená to tedy, že všechny bajty otevřeného textu i klíče nabývaly hodnoty logické 0. Pro lepší představu je uveden konkrétní hexadecimální zápis hodnot v maticové podobě a výsledek operace XOR, v našem případě matice **C** šifrovaného textu.

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

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

Při provádění operace XOR dojde ke změně takového počtu bitů matice **M**, kolik má bitů matice klíče **K** rovných hodnotě logická 1[1]. Operace XOR ovlivňuje počet sepnutých nebo rozepnutých tranzistorů uvnitř MCU, tedy i aktuální proudovou spotřebu obvodu. Protože použitý klíč má Hammingovu váhu 0, výsledkem operace XOR je nulová matice **C**. Naměřený proudový průběh pro první fázi měření zachycuje obr. 5.1.



Obr. 5.1: Proudový průběh první fáze měření.

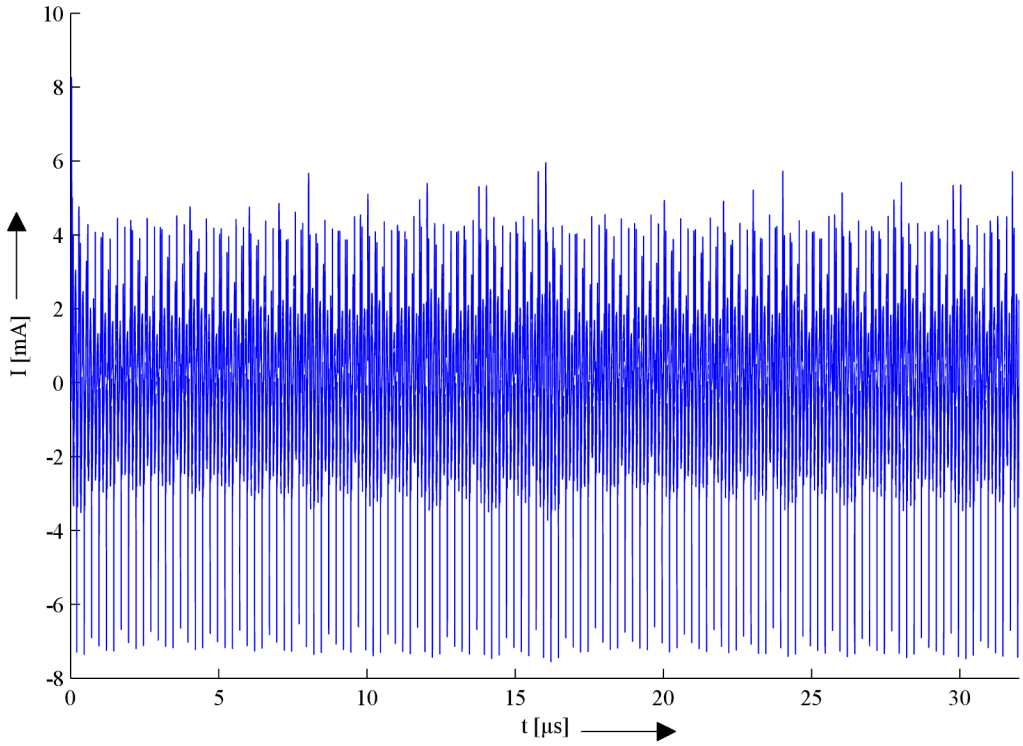
V druhé fázi měření byla matice otevřeného textu **M** opět nulová. Prvky matice tajného klíče **K** však postupně nabývali hodnot od 01h do FFh, tzn. Hammingova váha pro každý následující prvek byla zvětšena o 1. Konkrétní maticový zápis otevřeného textu, tajného klíče a výsledné operace XOR vypadá následovně:

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

[1]Stav, kdy bajty otevřeného textu mají hodnotu 0 nebo 1

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

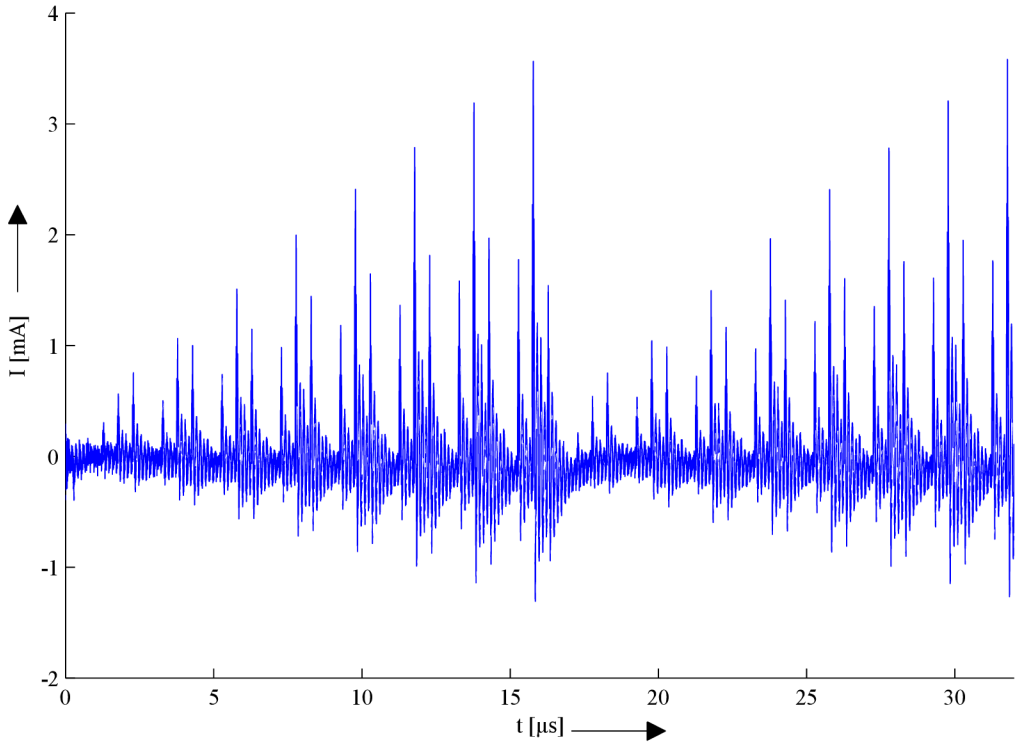
Naměřený proudový průběh pro druhou fázi měření je zachycen na obr. 5.2.



Obr. 5.2: Proudový průběh druhé fáze měření.

Zjištěné průběhy proudové spotřeby kryptografického modulu z předchozích dvou fází měření byly statisticky vyhodnoceny. Jejich odečtem vznikl diferenční průběh (viz obr. 5.3) znázorňující závislost proudové spotřeby modulu při vykonávání funkce `AddRoundKey` na Hammingově váze tajného klíče.

Z diferenčního průběhu na obr. 5.3 je zřejmé, že množství proudu odebíraného kryptografickým modulem je přímo úměrné počtu bitů tajného klíče, které nabývají hodnoty log. 1. Pokud útočník zná Hammingovu váhu klíče použitého při šifrování, výrazně klesá počet všech jeho možných variant. Útočník má tedy možnost prolomit zašifrovaný text pomocí útoku hrubou silou.



Obr. 5.3: Diferenční průběh funkce `AddRoundKey`.

5.1.1 Vliv napájecího napětí

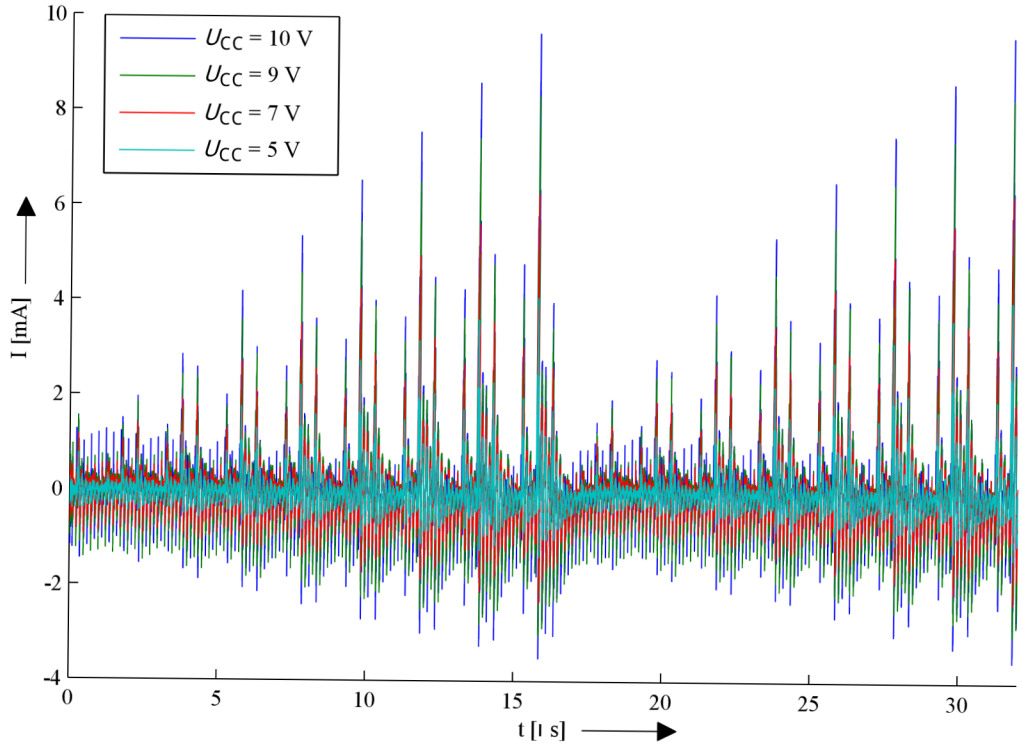
Obr. 5.4 znázorňuje závislost proudového odběru kryptografického modulu na hodnotě napájecího napětí zdroje U_{CC}. Je patrné, že s rostoucím napětím zdroje narůstá i hodnota proudového odběru mikrokontroléru při vykonávání funkce `AddRoundKey`.

Na obr. 5.5 je znázorněn detail průběhu proudového odběru modulu pro různé hodnoty napětí zdroje. Zachycené proudové špičky odpovídají operaci XOR mezi bajtem vstupních dat s hodnotou 00h a bajtem klíče hodnoty FFh. Pro $U_{\mathrm{CC}} = 10\,\mathrm{V}$ je velikost proudové špičky přibližně dvojnásobná.

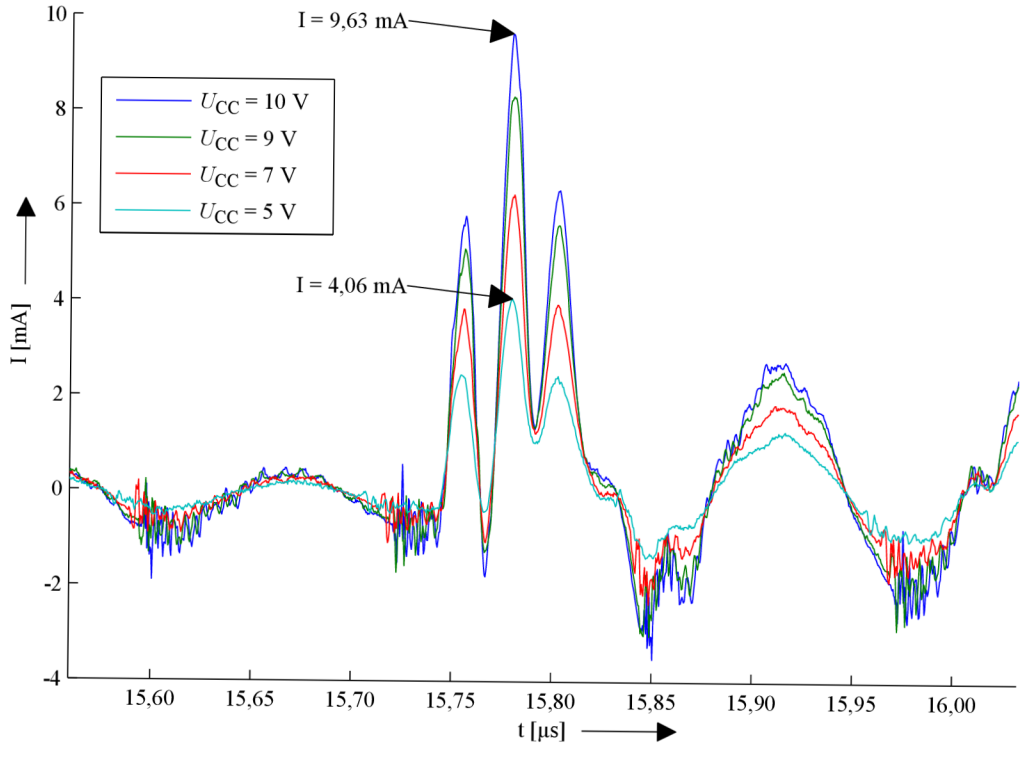
5.1.2 Vliv kmitočtu hodinového signálu

Kmitočet hodinového signálu má především vliv na úroveň šumu v měřeném průběhu proudového odběru kryptografického modulu. Zejména pak při vysokých kmitočtech. Tento jev znázorňuje obr. 5.6 a obr. 5.7.

Oba obrázky zachycují dva průběhy proudového odběru modulu během čtyř po sobě jdoucích hodinových cyklů pro napájecí napětí 5 a 10 V. Každý obrázek však pro jiný kmitočet hodinového signálu. V případě průběhů na obr. 5.6 byl kmitočet 4 MHz. Průběhy na obr. 5.7 byly měřeny pro kmitočet 8 MHz. Při zvýšení kmitočtu

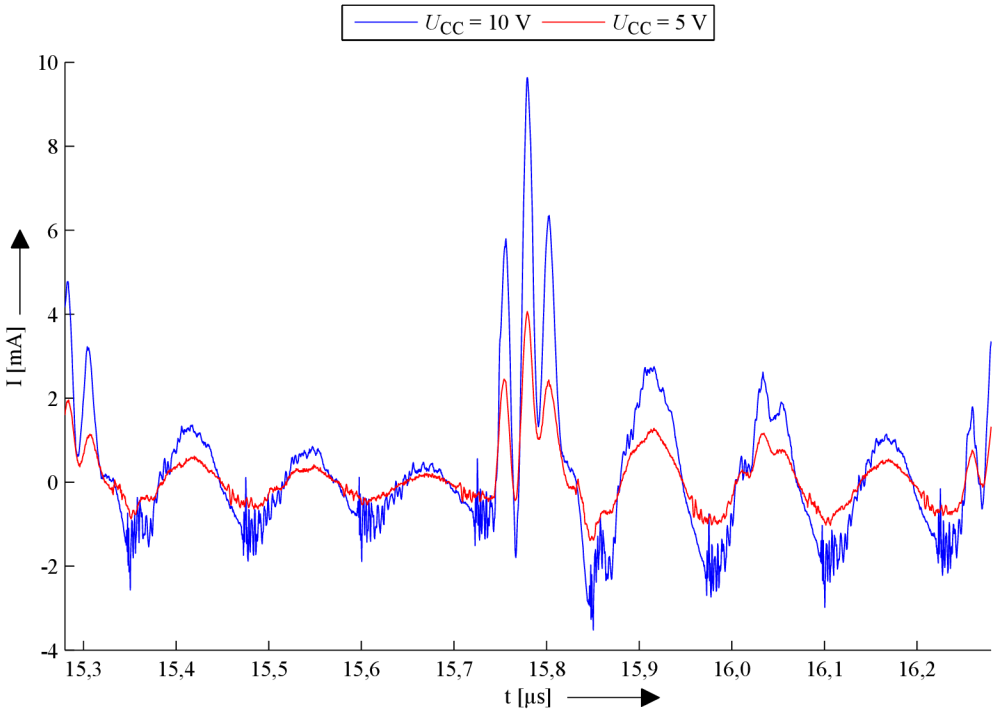


Obr. 5.4: Závislost proudového odběru modulu na napájecím napětí.

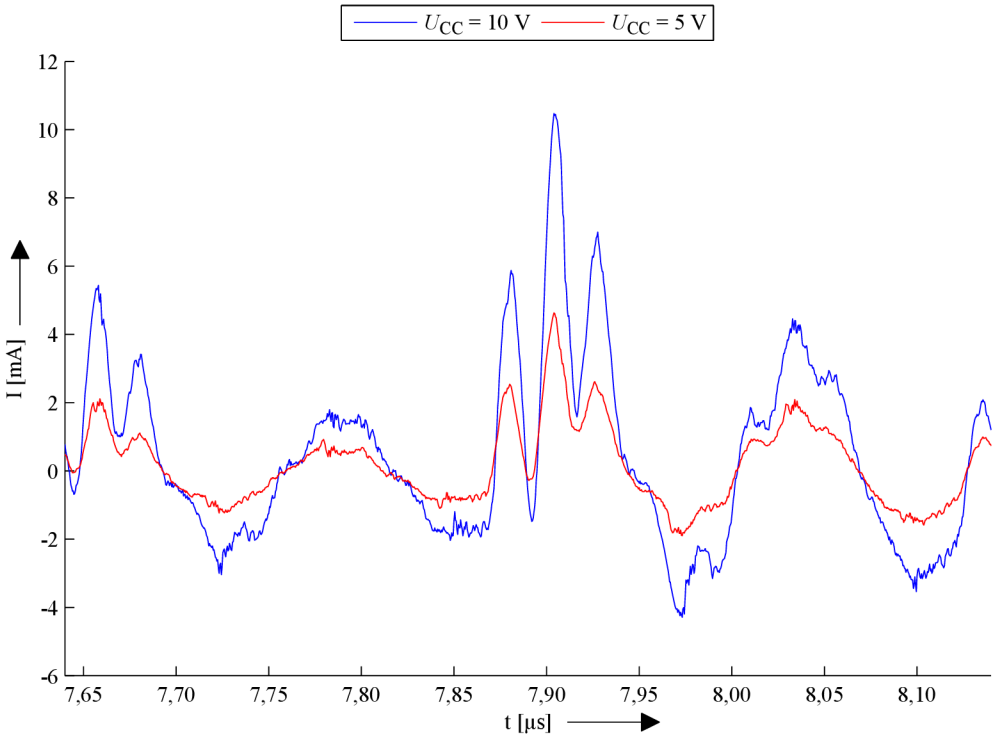


Obr. 5.5: Detailní průběh proudového odběru modulu pro různá napětí zdroje.

došlo k tomu, že špičky proudového odběru malé a velké úrovně, které při nižší frekvenci byly jednoznačně oddělené, se začaly překrývat. Při zvýšení kmitočtu by došlo k dalšímu výraznému překrytí.



Obr. 5.6: Průběhy proudu pro kmitočet hodinového signálu 4 MHz.

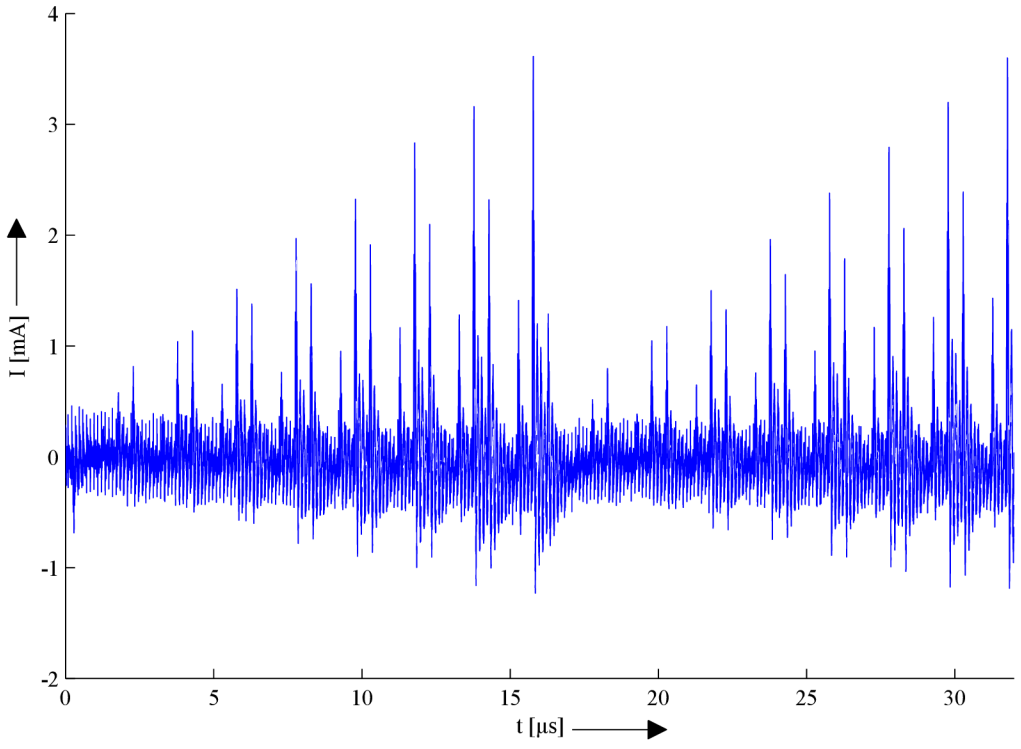


Obr. 5.7: Průběhy proudu pro kmitočet hodinového signálu 8 MHz.

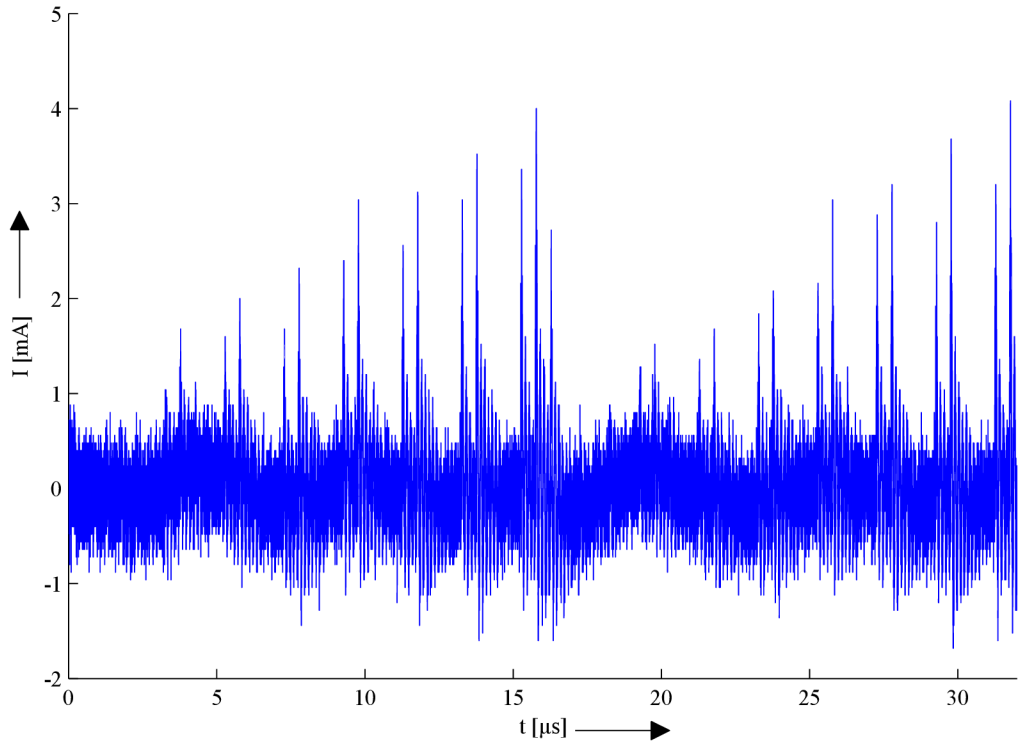
5.1.3 Vliv nastavení osciloskopu

Předtím než dojde k zobrazení měřeného signálu na obrazovce osciloskopu, musí být daný signál digitalizován. To se odehrává na daném vstupu, který je tvořen zesilovačem a obvodem pro vzorkování. Navzorkovaný signál ve formě digitálních dat se uloží do paměti, odkud jsou jednotlivé vzorky vybírány a původní signál je rekonstruován a zobrazen.

Použitý osciloskop umožňuje měření v různých snímacích módech, které mohou ovlivnit tvar naměřeného průběhu proudového odběru v předchozích bodech. V předchozích měřeních byl použit snímací mód s průměrováním (tzv. Average mode) nastavený na 64. Toto číslo udává, z kolika posledních vzorků na dané pozici bude vytvořena průměrná naměřená hodnota. Pro porovnání bylo vyzkoušeno měření průběhu pro snímací módy Average 16 (tzn. menší počet vzorků) a snímací mód Peak Detect, který pracuje pouze s nejvyšší a nejnižší hodnotou vzorku získanou ze dvou po sobě jdoucích snímaných intervalů. Získané průběhy jsou zachyceny na obr. 5.8 a obr. 5.9. Při použití módu Peak Detect lze pozorovat výrazné zvýšení úrovně šumu, při které dojde k částečnému překrytí užitečného signálu.



Obr. 5.8: Diferenční průběh pro snímací mód Average 16.



Obr. 5.9: Diferenční průběh pro snímací mód Peak Detect.

5.2 Diferenciální proudová analýza

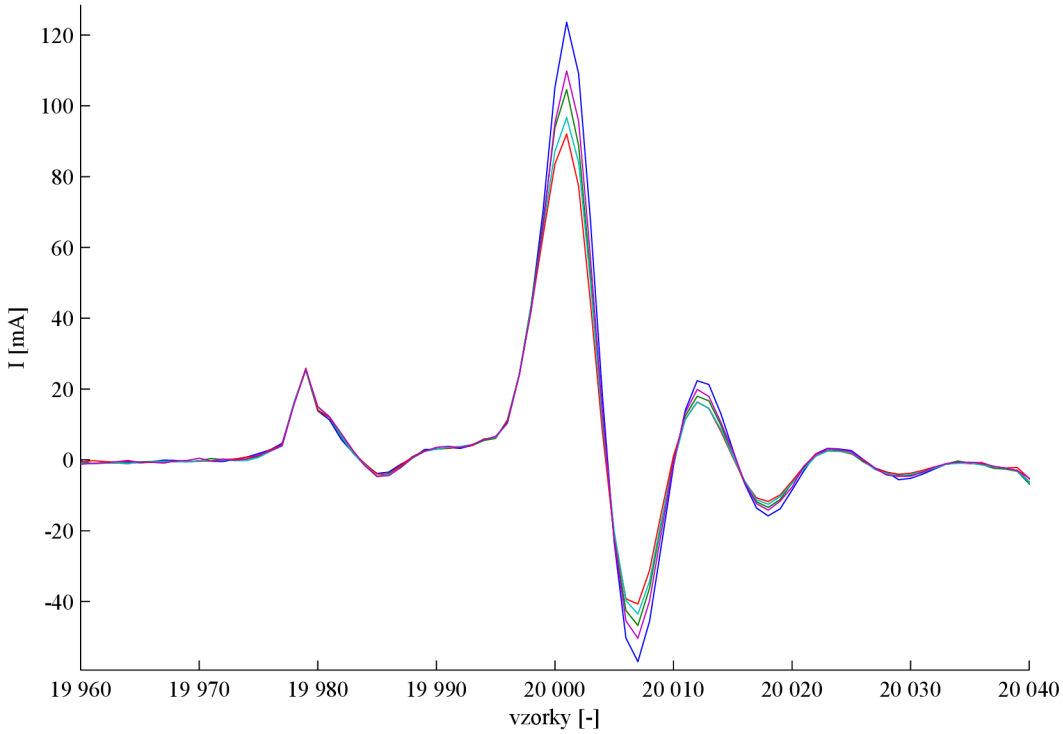
Mikrokontrolér PIC16F84A byl pro diferenciální proudovou analýzu opět naprogramován upravenou implementací šifrovacího algoritmu AES. Kromě inicializační fáze `AddRoundKey` vykonával i operaci `SubBytes`. Cílem analýzy je nalézt hodnotu prvního bajtu šifrovacího klíče.

Při diferenciální proudové analýze bylo postupováno podle obecných kroků uvedených v kapitole 2.3.3 a podle vzorového příkladu DPA útoku z kapitoly 3.2.2.

Na začátku DPA útoku byla nejprve zvolena vnitřní hodnota algoritmu AES, která závisí na známých vstupních datech a části klíče (v našem případě na jeho prvním bajtu).

Dále byly změřeny průběhy proudové spotřeby kryptografického modulu při procesu šifrování 256 náhodných bloků vstupních dat. Obr. 5.10 znázorňuje průběhy spotřeby modulu při šifrování 6 náhodných vstupních dat. Z průběhů plyne, že podmínka zarovnání měřených průběhů a tedy správné synchronizace osciloskopu je splněna.

V dalším kroku DPA útoku byla sestavena matice hypotéz vnitřních hodnot pro 256 bloků vstupních dat. Hledanému prvnímu bajtu klíče odpovídá první bajt každého bloku. Pro 256 možných klíčů, získáme 256×256 hypotéz vnitřních hodnot.



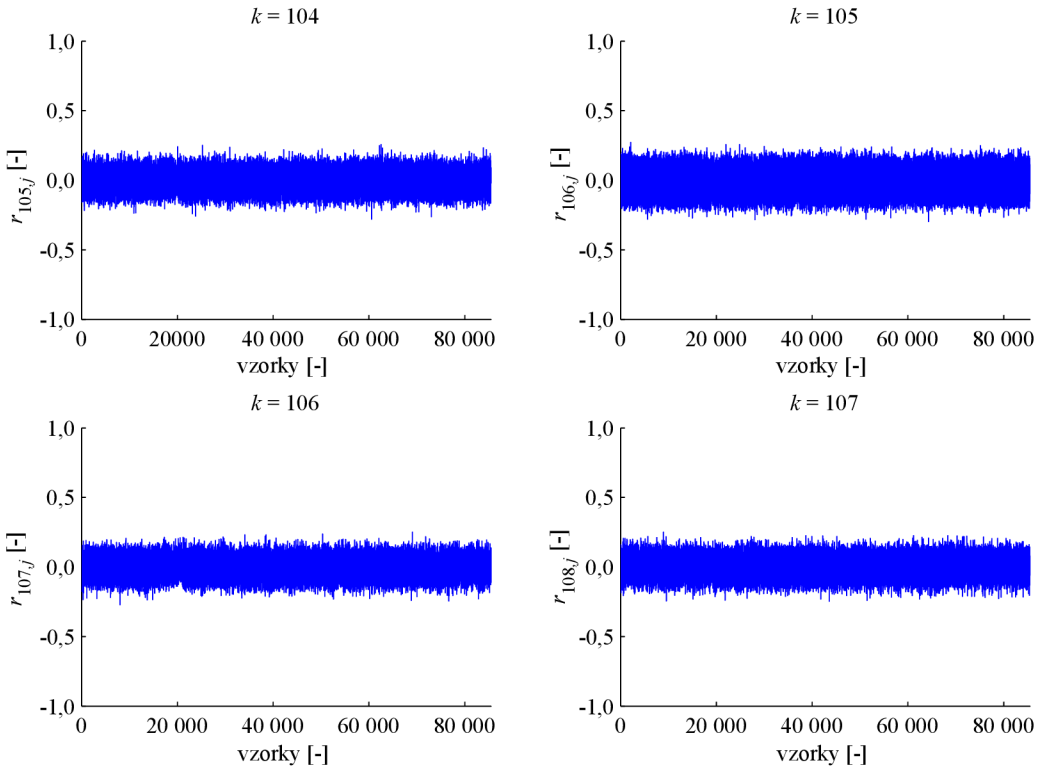
Obr. 5.10: Šifrování 5 náhodných vstupních dat.

Čtvrtý krok DPA útoku spočívá ve vytvoření simulace proudové spotřeby modulu. V našem případě byl zvolen model Hammingovy váhy, jehož aplikací na matici hypotéz vnitřních hodnot získáme matici hypotéz o spotřebě.

V posledním kroku došlo k vyhodnocení míry lineární závislosti naměřených průběhů a hypotéz proudové spotřeby pro všechna vstupní data a klíče. K tomu byl použit výpočet korelačního koeficientu. Z výsledné matice korelačních koeficientů jsou na obr. 5.11 zachyceny průběhy pro hypotézy klíče 104 až 107.

Klíč, který byl používán kryptografickým modulem při šifrování vstupních dat, měl první bajt manuálně nastaven na hodnotu 107. Podle teoretických předpokladů a očekávání by tedy v průběhu pro hypotézu klíče 107 měly být pozorovatelné špičky. V průběhu se však žádné špičky nevyskytují. Z toho vyplývá, že mezi hypotetickou spotřebou modulu pro daný klíč a naměřenými průběhy není žádná závislost. Klíč nelze odhalit.

Diferenciální proudová analýza nevedla k odhalení hodnoty klíče ani po provedení různých opatření. Byla provedena kontrola postupu u jednotlivých kroků analýzy podle kapitoly 2.3.3. Také bylo provedeno odkrokování programu pro mikrokontrolér PIC a skriptů pro zpracování naměřených dat v programu Matlab. Uvedená opatření nepřinesla požadovaný výsledek. Možná řešení jsou diskutována v závěru.



Obr. 5.11: Průběhy pro hypotézy klíče 104 až 107.

6 ZÁVĚR

Cílem bakalářské práce bylo prostudovat problematiku útoku proudovým postranním kanálem na kryptografický modul. Za tímto účelem byl navržen jednoduchý měřicí obvod tvořený mikrokontrolérem PIC16F84A a potřebnými součástkami pro správnou funkci tohoto obvodu. K analýze proudového postranního kanálu byla použita proudová sonda Tektronix CT-6.

Ke správnému sestavení měřicího pracoviště, k realizaci samotného útoku proudovým postranním kanálem a analýze výsledků měření posloužily teoretické základy proudové analýzy a studium principu fungování mikrokontrolérů PIC a šifrovacího standardu AES. Potřebné znalosti obsahuje teoretická část této práce.

Po sestavení a kontrole zapojení měřicího pracoviště byla provedena zadaná měření. Mikrokontrolér PIC16F84A byl nejprve naprogramován funkcí `AddRoundKey`, která tvoří část šifrovacího algoritmu AES. Na sestaveném kryptografickém modulu byla provedena jednoduchá proudová analýza. Při této analýze byl zkoumán vliv hodnoty napájecího napětí a kmitočtu hodinového signálu na průběhy proudové spotřeby modulu provádějícího funkci `AddRoundKey`. Také byl prozkoumán vliv nastavení snímacího módu osciloskopu.

S rostoucí hodnotou napětí napájecího zdroje modulu narůstá jeho proudový odběr. Při dvojnásobném zvětšení napájecího napětí došlo přibližně ke stejnému zvětšení úrovně proudových špiček. Nedošlo však téměř ke zvýšení úrovně šumu. Jednoduchá proudová analýza je tedy při vyšších hodnotách napájecího napětí mnohem účinnější.

Volba kmitočtu hodinového signálu má velký vliv na úroveň šumu v měřeném průběhu proudového odběru modulu. Pro omezení úrovně šumového pozadí v měřených průbězích je vhodné pracovat s nižšími hodnotami kmitočtů hodinového signálu, pokud jsou však tyto hodnoty modulem povoleny.

Také byl vyzkoušen vliv nastavení snímacího módu osciloskopu na diferenční průběh získaný jednoduchou proudovou analýzou. Výše popsaná měření byla provedena při snímacím módu Average 16, kdy došlo k lehkému nárůstu hodnoty šumu. Při snímacím módu Peak Detect vzrostla hodnota šumu natolik, že došlo k překrytí části užitečného signálu.

Při diferenciální proudové analýze byl kryptografický modul sestaven z mikrokontroléru PIC16F84A a vývojové desky od firmy Microchip, která nám umožnila komunikaci s počítačem přes sériové rozhraní. Mikrokontrolér byl naprogramován pro vykonávání funkce `AddRoundKey` a `SubBytes`. Diferenciální analýza měla za úkol odhalit hodnotu prvního bajtu šifrovacího klíče, tzn. byla cílena na první výstupní bajt šifrovaných dat operace `SubBytes`.

Přestože byla diferenciální proudová analýza provedena podle platných postupů,

nalezení hodnoty prvního bajtu šifrovacího klíče nebylo úspěšné. Výsledný průběh pro hypotézu klíče 107 (hledaná hodnota) neobsahoval žádné špičky. Tzn., že mezi naměřenými průběhy a hypotézami o spotřebě kryptografického modulu není žádná závislost.

Před opakovanými měřeními bylo provedeno několik opatření. Proběhla kontrola postupu analýzy včetně ověření správné funkce šifrovacího algoritmu AES implementovaného uvnitř mikrokontroléru PIC. Skripty vytvořené v programu Matlab pro statistické vyhodnocení DPA útoku byly ověřeny pomocí debug módu. Opakovaná měření však vedla ke stejnému výsledku.

Jako možné řešení se jeví vytvoření jiné simulace proudové spotřeby kryptografického modulu, tedy využití jiného modelu spotřeby. Také se zaměřit na konkrétní mikrokontrolér a ověřit jakým způsobem pracuje s vnitřními registry během operace `SubBytes`. Problémy může také způsobovat komunikace s počítačem po sériové lince, přes kterou jsou zasílány hodnoty vstupních dat.

LITERATURA

[1] BONEH, Dan; DEMILLO, Richard A.; LIPTON, Richard J. On the Importance of Eliminating Errors in Cryptographic Computations. In *Journal of Cryptology* [online]. New York: Springer, 2011 [cit. 2012-05-21]. Dostupné z WWW: <http://www.springerlink.com/content/cljfg7u5n4bw312a/>.

[2] BUČEK, Jiří. *Útok postranními kanály*. Praha: CryptoFest, 11. 6. 2011.

[3] DANĚČEK, Petr; BŘEZINA, Milan. Útok výkonovým postranním kanálem na hardwarový kryptografický modul. *Elektrorevue* [online]. 14. 8. 2006 [cit. 2012-05-21]. Dostupné z WWW: <http://www.elektrorevue.cz/clanky/06031/index.html>.

[4] FIPS PUB 46-3. *Data Encryption Standard (DES)* [online]. National Institute of Standards and Technology, 25. 10. 1999 [cit. 2012-05-21]. 26 s. Dostupné z WWW: <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>.

[5] FIPS PUB 197. *Advanced Encryption Standard (AES)* [online]. National Institute of Standards and Technology, 26. 11. 2001 [cit. 2012-05-21]. 51 s. Dostupné z WWW: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

[6] HAGAI, Bar-El. *Introduction to Side-Channel Attacks* [online]. 2003 [cit. 2012-05-21]. Dostupné z WWW: <http://www.hbarel.com/publications/Introduction_To_Side_Channel_Attacks.pdf>.

[7] HAGAI, Bar-El. *Known Attacks Against Smartcards* [online]. 2003 [cit. 2012-05-21]. Dostupné z WWW: <http://www.hbarel.com/publications/Known_Attacks_Against_Smartcards.pdf>.

[8] HAGAI, Bar-El. *The Sorcerer's Apprentice Guide to Fault Attacks* [online]. 2004 [cit. 2012-05-21]. Dostupné z WWW: <http://www.hbarel.com/publications/Sorcerers_Apprentice_Guide.pdf>.

[9] KOC, Cetin Kaya. *Cryptographic Engineering*. New York: Springer, 2009. 522 s. ISBN 978-0-387-71816-3.

[10] KOCHER, Paul C. *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems* [online]. 1996 [cit. 2012-05-21]. Dostupné z WWW: <http://www.cryptography.com/public/pdf/TimingAttacks.pdf>.

[11] KOCHER, Paul C.; JAFFE, Joshua; JUN, Benjamin. *Introduction to Differential Power Analysis and Related Attacks* [online]. 1998 [cit. 2012-05-21]. Dostupné z WWW: <http://www.cryptography.com/public/pdf/DPATechInfo.pdf>.

[12] KOCHER, Paul C.; JAFFE, Joshua; JUN, Benjamin. *Differential Power Analysis* [online]. 1998 [cit. 2012-05-21]. Dostupné z WWW: <http://www.cryptography.com/public/pdf/DPA.pdf>.

[13] MANGARD, Stefan; OSWALD, Elisabeth; POPP, Thomas. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. New York: Springer, 2007. 338 s. ISBN 978-0-387-30857-9.

[14] MENEZES, Alfred J.; OORSCHOT, Paul C. van.; VANSTONE, Scott A. *Handbook of Applied Cryptography*. CRC Press, 1996. 816 s. ISBN 0-8493-8523-7.

[15] Microchip Technology. *PIC16F8X, 18-pin Flash/EEPROM 8-bit MCU* [online datasheet]. Poslední aktualizace 4. 3. 2002 [cit. 2012-05-21]. Dostupné z WWW: <http://ww1.microchip.com/downloads/en/devicedoc/30430c.pdf>.

[16] Microchip Technology. *PIC16F84A* [online datasheet]. Poslední aktualizace 11. 11. 2002 [cit. 2012-05-21]. Dostupné z WWW: <http://ww1.microchip.com/downloads/en/devicedoc/35007b.pdf>.

[17] Microchip Technology. *PICDEM 2 Plus Demonstration Board User´s Guide* [online]. Poslední aktualizace 30. 9. 2011 [cit. 2012-05-21]. Dostupné z WWW: <http://ww1.microchip.com/downloads/en/DeviceDoc/41584B.pdf>.

[18] National Security Agency. *TEMPEST: A Signal Problem* [online]. 27. 9. 2007 [cit. 2012-05-21]. Dostupné z WWW: <http://www.nsa.gov/public_info/_files/cryptologic_spectrum/tempest.pdf>.

[19] NEČAS, Ondrej. *Útok elektromagnetickým postranním kanálem*: diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2011. 84 s. Vedoucí práce byl Ing. Peter Stančík.

[20] 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.

[21] Tektronix. *DPO4000 Series Digital Phosphor Oscilloscopes: User manual*. 12. 1. 2006 [cit. 2011-11-21].

[22] Tektronix. *CT-6 High Frequency AC Current Probe: Instruction manual*. [cit. 2012-05-21].

[23] WESTE, Neil H. E.; HARRIS, David. *CMOS VLSI Design: A Circuits and System Perspective*. Boston: Addison Wesley, 2005. 838 s. ISBN 0-321-26977-2.

[24] ZHOU, Yong Bin; FENG, Deng Guo. *Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing* [online]. 2005 [cit. 2012-05-21]. Dostupné z WWW: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.100.8856&rep=rep1&type=pdf>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

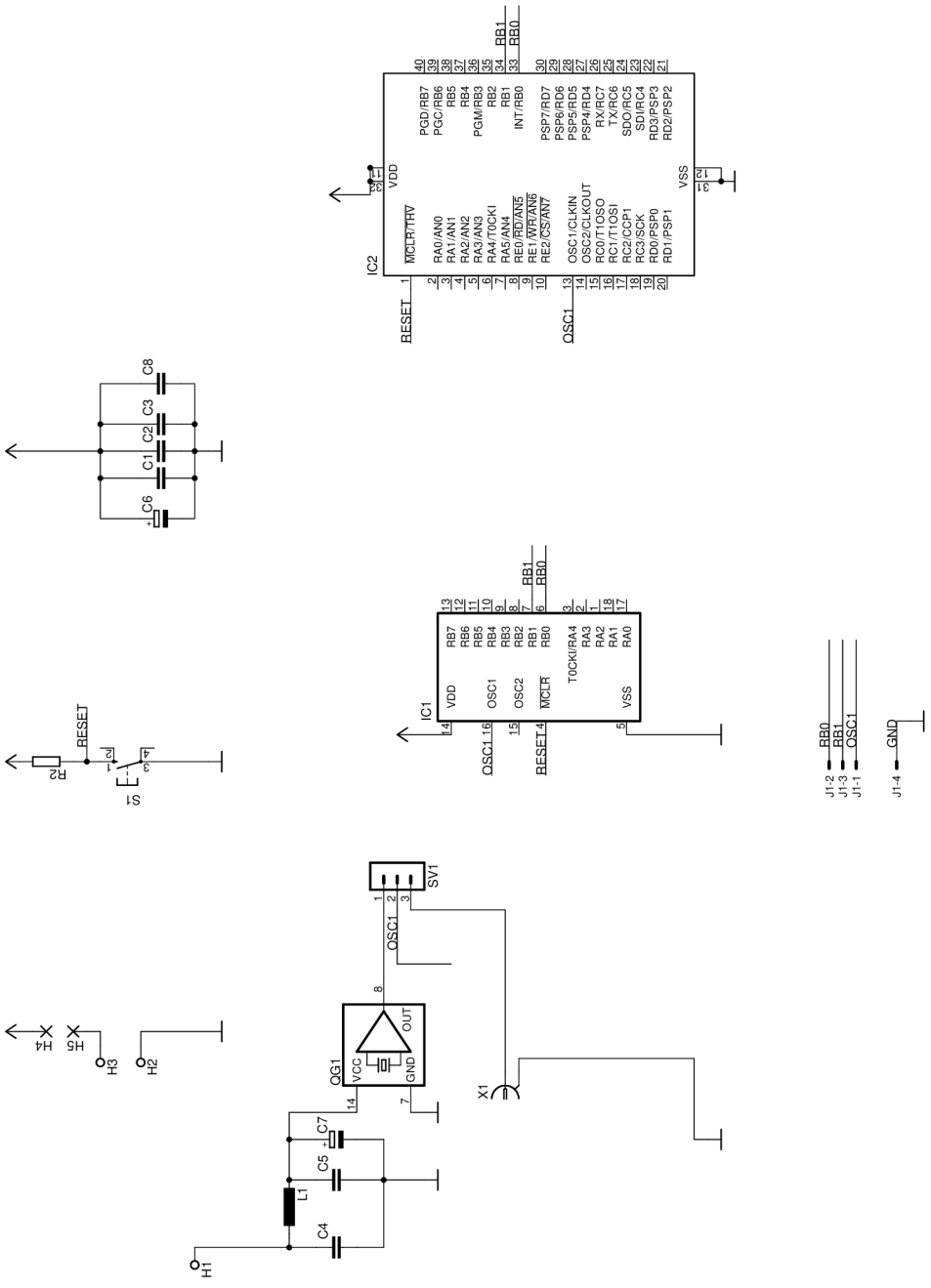
AES	Pokročilý standard pro šifrování dat – Advanced Encryption Standard
CLK	Hodinový signál – Clock
CMOS	Technologie pro výrobu integrovaných obvodů – Complementary Metal-Oxide Semiconductor
DES	Standard pro šifrování dat – Data Encryption Standard
DPA	Diferenciální proudová analýza – Differential Power Analysis
DPS	Deska plošných spojů
LSB	Nejméně významný bit – Least Significant Bit
MCU	Mikrokontrolér – Microcontroller
NIST	Americký úřad pro standardy a technologie – National Institute of Standards and Technology
PA	Proudová analýza – Power Analysis
RISC	Procesor s redukovanou instrukční sadou – Reduced Instruction Set Computer
RSA	Asymetrický šifrovací algoritmus – Rivest -Shamir -Adleman
SCA	Útok postranním kanálem – Side-Channel Attack
SPA	Jednoduchá proudová analýza – Simple Power Analysis
TEMPEST	Standardy a doporučení pro elektronická zařízení vyzařující elektromagnetické pole – Transient Electromagnetic Pulse Emanation Standard
XOR	Exkluzivní disjunkce – Exclusive disjunction

SEZNAM PŘÍLOH

A OBSAH PŘILOŽENÉHO CD

- Elektronická verze semestrální práce.
- Schéma zapojení a návrh DPS kryptografického modulu s mikrokontrolérem PIC16F84A (vytvořeno v editoru Eagle 5.11.0).
- Katalogový list mikrokontroléru PIC16F84A.
- Uživatelský manuál k vývojové desce PICDEM2 Plus.
- Program v jazyce Assembler implementující funkci AddRoundKey (spustitelný ve vývojovém prostředí MPLAB 8.76).
- Program v jazyce Assembler implementující funkci AddRoundKey a SubBytes (spustitelný ve vývojovém prostředí MPLAB 8.76).
- Veškerá data potřebná pro diferenciální proudovou analýzu ve formě matic s příponou *.mat (spustitelné ve vývojovém prostředí Matlab 7.11.0).
- Skripty použité pro zpracování naměřených proudových průběhů při diferenciální proudové analýze (spustitelné ve vývojovém prostředí Matlab 7.11.0).

B SCHÉMA DPS SESTAVENÉHO MODULU



Obr. B.1: Schéma DPS kryptografického modulu.