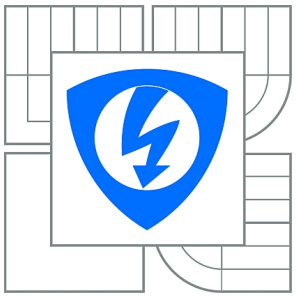
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

ELEKTROMAGNETICKÁ ANALÝZA

ELECTROMAGNETIC ANALYSIS

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

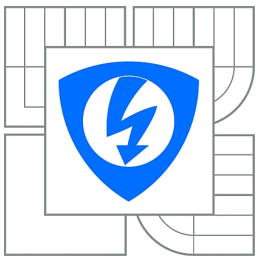
AUTOR PRÁCE — Bc. JOSEF KOLOFÍK

AUTHOR

VEDOUCÍ PRÁCE — Ing. ZDENĚK MARTINÁSEK

SUPERVISOR

BRNO 2012



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student: Bc. Josef Kolofík ***ID:*** 112050
Ročník: 2 ***Akademický rok:*** 2011/2012

NÁZEV TÉMATU:

Elektromagnetická analýza

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte útok elektromagnetickým postranním kanálem na kryptografický modul. Seznamte se s experimentálním pracovištěm v laboratoři a pomocí něj realizujte analýzu elektromagnetického postranního kanálu mikroprocesoru PIC16F84. Procesor bude pracovat s algoritmem AES. Analýzu zaměřte nejprve na implementaci funkce AddRoundKey. Prostudujte vliv pozice nenulového bitu v šifrovacím klíči na elektromagnetický průběh. Vytvořte a natrénujte neuronovou síť pomocí získaných znalostí a proveďte analýzu prvního bajtu tajného klíče algoritmu AES.

DOPORUČENÁ LITERATURA:

[1] Agrawal, D., Archambeault, B., Rao, J., Rohatgi, P.: The EM SideChannel(s). pp. 29-45 (2003). DOI, URL http://dx.doi.org/10.1007

[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:*** 24.5.2012

Vedoucí práce: Ing. Zdeněk Martinásek
Konzultanti diplomové práce:

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

UPOZORNĚNÍ:

SIX research centre
sensor, information and communication systems

Faculty of Electrical Engineering
and Communication

Brno University of Technology
Purkynova 118, CZ-61200 Brno, Czechia

http://www.six.feec.vutbr.cz

Výzkum popsaný v této diplomové práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007–13
OP Výzkum a vývoj pro inovace

ABSTRAKT

Tato práce se zabývá problematikou elektromagnetické analýzy a aplikací elektromagnetického postranního kanálu. První a druhá část práce popisují základy kryptografie, funkci kryptografického modulu a útoky vedené postranními kanály. Třetí část práce rozebírá možnosti elektromagnetické analýzy, konstrukci sondy, popis laboratorního pracoviště, elektromagnetickou emisi PIC16F84A, algoritmus AES a přípravu na laboratorní měření. Čtvrtá část práce popisuje konkrétní laboratorní měření a extrakci užitečného signálu. V páté části práce jsou uvedeny výsledky zpracování naměřených hodnot, výstupy vytvořených skriptů a zjištěné souvislosti mezi naměřenými průběhy a šifrovacím klíčem algoritmu AES. V šesté části práce jsou rozebrány základní možnosti obrany proti útoku postranním kanálem.

KLÍČOVÁ SLOVA

elektromagnetická, analýza, postranní, kanál, aes, pic16f84a, kryptografie, neuronová síť

ABSTRACT

This thesis deals with electromagnetic analysis and applications of electromagnetic side channel. The first and second part describes the basics of cryptography, function of cryptographic module and side-channel attacks. The third part discusses the electromagnetic analysis, construction of probe, a description of the laboratory workplace, the electromagnetic emission of PIC16F84A, AES and preparation for laboratory measurements. The fourth part describes specific laboratory measurements and extracting the useful signal. In the fifth part of the thesis presents the results of processing the measured values, the outputs generated by scripts and found the link between measured curves and AES encryption key. In the sixth part of the thesis are analyzed the basics of defense against side channel attack.

KEYWORDS

electromagnetic, analysis, side, channel, aes, pic16f84a, cryptography, neural network

KOLOFÍK, Josef *Elektromagnetická analýza*: diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2012. 56 s. Vedoucí práce byl Ing. Zdeněk Martinásek

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Elektromagnetická analýza“ 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

Rád bych poděkoval vedoucímu diplomové práce panu Ing. Zdeňku Martináskovi za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Cílem práce je prostudování útoku elektromagnetickým postranním kanálem a jeho následná aplikace na laboratorním pracovišti Ústavu telekomunikací FEKT VUT v Brně, dále jen laboratorní pracoviště elektromagnetické analýzy. V úvodu práce budou ve dvou kapitolách zpracovány základní informace o kryptografickém modulu a požadavcích na zabezpečení dat. Následně budou rozebrány možné útoky na kryptografický modul s využitím běžných útoků i útoků postranními kanály.

Dílčím cílem práce je podrobnější prostudování útoku využitím elektromagnetického postranního kanálu. Tímto se bude zabývat 3. kapitola práce, jejímž cílem je zjištění možností elektromagnetické analýzy, prostudování základních pojmů a důvodů vzniku elektromagnetického pole. Dalším dílčím cílem kapitoly je seznámení se s pracovištěm elektromagnetické analýzy, kde budou prováděny laboratorní měření na základě získaných teoretických znalostí. Tato část práce bude zahrnovat také prostudování vlastností mikrokontroléru PIC16F84A a jeho uvedení do funkce kryptografického modulu, resp. simulátoru části algoritmu AES, která je vhodná k provedení útoku elektromagnetickým postranním kanálem. Dále budou uvedeny výsledky simulací činnosti logického invertoru, který je hlavním stavebním prvkem uvedeného mikrokontroléru.

Ve čtvrté části práce budou provedena laboratorní měření na připraveném mikrokontroléru PIC16F84A, které jsou hlavním cílem práce a jejichž výstupem by mělo být zjištění konkrétních souvislostí mezi naměřenými průběhy a šifrovacím klíčem. Konkrétní cíl práce spočívá ve zjištění závislosti průběhu elektromagnetické analýzy na poloze nenulového bitu v jednom z bajtů šifrovacího klíče algoritmu AES při vykonávání operace AddRoundKey. Dále budou provedena měření pro celý rozsah hodnot klíče v jednom bajtu.

Pátá část práce se bude zabývat zpracováním naměřených hodnot, experimentálním zjišťováním souvislostí mezi naměřenými průběhy a šifrovacím klíčem. Výstupem této části práce budou skripty pro prostředí Matlab demonstrující možné využití zjištěných souvislostí pro útok elektromagnetickým postranním kanálem.

Obsahem šesté části práce bude kapitola pojednávající o možnostech ochranných opatření proti útoku elektromagnetickým postranním kanálem.

Přínos práce spočívá v navázání na předchozí práce využívající laboratorní pracoviště elektromagnetické analýzy, prohloubení doposud získaných informací a rozšíření informací o možnostech využití útoku elektromagnetickým postranním kanálem.

1 ÚVOD DO KRYPTOGRAFIE

V dnešní době jsou ve většině možných případů využívány možnosti elektronické komunikace. Zařízení pro elektronickou komunikaci proto nacházíme téměř všude, hlavními důvody jsou vysoká technická úroveň těchto zařízení a vyspělost výrobních procesů, které umožňují tato zařízení vyrábět za ceny dostupné pro většinu populace. Společně s technickým rozvojem elektronických komunikací přišel také rozvoj nasazení těchto technologií do široké škály oborů lidské činnosti.

Oblast nasazení elektronických komunikačních technologií zahrnuje v současné době prakticky všechny obory, tedy i ty obory, u kterých se pracuje s daty, jež je možno souhrnně označit jako tzv. „citlivá data“. Jedná se zejména o data, jejichž únik nebo změny během komunikace by mohly znamenat bezpečnostní riziko různého charakteru. Z tohoto důvodu se na elektronickou komunikaci začalo pohlížet jako na systémy určené ke zpracování a výměně dat s definovanými požadavky na jednotlivé části systému a na spoje mezi těmito částmi. Poté bylo možné jasně definovat, které části a které spoje jsou stěžejní pro bezpečnost a přiřadit jim kryptografické bezpečnostní prvky dle požadované úrovně zabezpečení.

1.1 Požadavky na kryptograficky zabezpečený systém

Příkladem oborů s požadavky na kryptograficky zabezpečené komunikační systémy mohou být následující čtyři odvětví:

- bankovnictví,
- obchod,
- armáda,
- informační technologie.

U všech uvedených odvětví a obecně u všech zabezpečených prvků komunikačních systémů byly definovány základní požadavky, které stanovují základní principy, jenž musí být dodrženy, aby systém mohl být označen jako kryptograficky zabezpečený. Kryptograficky zabezpečený systém má za úkol zajistit, aby tzv. „citlivá data“ nebylo možné zachytit a změnit během komunikace. K vysvětlení důvodů poslouží dále uvedené příklady z praxe.

Armádní komunikační systémy kladou jako jeden ze základních požadavků zajištění skutečnosti, že přenášeným datům porozumí pouze jejich adresát. Předpokládá se tak, že veškerá komunikace bude zcela důvěrná a kromě odesilatele a adresáta nesmí mít nikdo jiný k uvedeným datům přístup.

V bankovním sektoru je požadováno, aby bylo možné zcela jednoznačně určit spojitost mezi daty a jejich autorem, musí být zajištěna autentičnost dat. Například při elektronické platbě tak musí být zcela jistě určeno, že příkaz k platbě pochází od majitele bankovního účtu a musí být možné tuto informaci ověřit.

Oblast informačních technologií, kterou využívají obě výše uvedená odvětví a je prakticky nepostradatelná i pro další odvětví, klade ještě jeden základní požadavek, který úzce souvisí s oběma výše zmíněnými příklady. Pokud je nutné zajistit důvěrnost mezi odesilatelem a adresátem a zamezit úniku informací, případně pokud je nutné zajistit spojitost mezi daty a jejich autorem, je pak nutné také zajistit, aby data nebyla při přenosu zaměněna, změněna, nebo aby s daty bylo jakkoliv jinak manipulováno za účelem porušení důvěrnosti nebo autentičnosti. Třetím základním požadavkem na kryptograficky zabezpečený systém je integrita dat, která zajišťuje, že při přenosu dat je ověřitelné, že s daty nebylo nijak manipulováno a že stav při příjmu odpovídá stavu při odeslání. Jako velmi jednoduchý praktický příklad může být zmíněn například kontrolní součet, který je běžně používán [1].

Z uvedených příkladů jsou zřejmé tři základní požadavky, které jsou kladeny na kryptograficky zabezpečené systémy a tyto systémy je musí v základu splňovat na předem definované úrovni. Úroveň zajištění základních požadavků pak určuje celkovou úroveň systému. V souhrnu lze tedy definovat požadavky:

- důvěrnosti – přenášeným datům smí porozumět pouze jejich adresát, nikdo jiný,
- autentičnosti – musí být jednoznačně prokazatelná spojitost mezi daty a jejich autorem,
- integrity dat – musí být prokazatelné a ověřitelné, že data nebyla při přenosu nijak změněna.

1.2 Kryptografický bezpečnostní modul

Kryptografické bezpečnostní moduly jsou nasazovány tam, kde je zapotřebí zajistit určitou úroveň bezpečnosti komunikačního systému a splnit tak základní požadavky na zabezpečený systém. Kryptografický bezpečnostní modul je obecně prvek poskytující služby k zabezpečení komunikace. Vyskytovat se může ve formě softwarové nebo hardwarové. Princip činnosti tohoto prvku je založen na aplikaci kryptografických protokolů a kryptografických algoritmů, pomocí nichž jsou data zabezpečena [1], [2].

1.3 Kryptografický algoritmus

Kryptografický algoritmus je souhrnem operací, které jsou prováděny s daty při jejich přesunu ze vstupu kryptografického bezpečnostního modulu na jeho výstup. Účelem prováděných operací je zabezpečení dat. Celý cyklus lze obecně nazvat jako šifrování.

Z praktického hlediska se jedná o matematické operace, při nichž je dle pravidel daného algoritmu vytvořen výstupní proud dat, která není možné uvést do původní podoby bez znalosti šifrovacího klíče. Matematicky se tedy jedná o funkci, která na základě šifrovacího klíče transformuje vstupní data do jejich výstupní zabezpečené podoby. U kryptografických algoritmů není hlavním cílem utajit samotný algoritmus, nýbrž utajit šifrovací klíč. Z hlediska využití šifrovacího klíče jsou rozlišovány dva druhy šifrovacích algoritmů:

- symetrický algoritmus,
- asymetrický algoritmus,

kde symetrický algoritmus využívá pro operace šifrování i dešifrování shodný šifrovací klíč. Asymetrický algoritmus využívá pro operaci šifrování klíč, který je odlišný od klíče využívaného při operaci dešifrování, obecně známé označení je soukromý a veřejný klíč [1].

1.4 Kryptografický protokol

Kryptografický protokol je označení souhrnu pravidel pro implementaci kryptografických algoritmů. Definovány jsou způsoby komunikace mezi jednotlivými prvky řetězce systému, komunikace s řídícími prvky systému a další parametry implementace.

Zejména u hardwarových implementací není možné zcela přesně definovat všechny parametry implementace, tím pak dochází k nezávislosti protokolu na hardwaru. Rozdíly vzniklé tímto způsobem tak často nebývají zcela ošetřeny a je možné je s výhodou využít k útoku na kryptografický modul [1], [2].

2 ÚTOKY NA KRYPTOGRAFICKÝ MODUL

2.1 Funkce kryptografického modulu

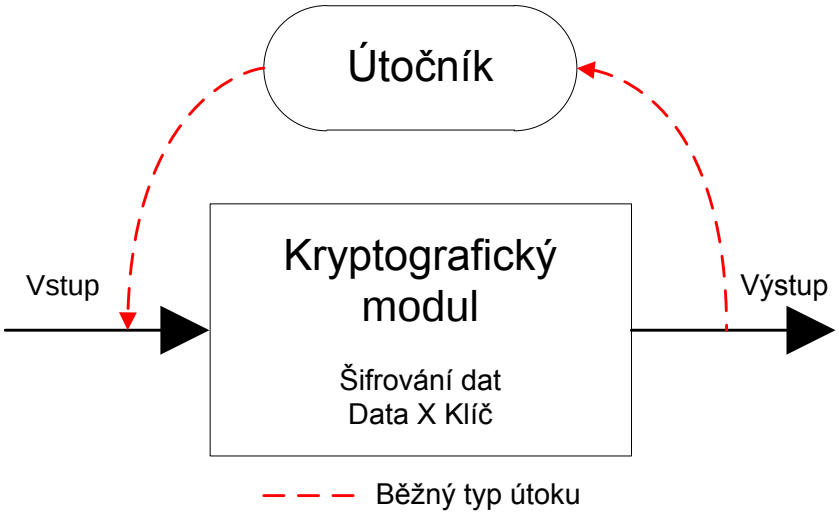
Kryptografický bezpečnostní modul lze znázornit jako systém se dvěma primárními kanály, vstupním a výstupním, pomocí nichž komunikuje s ostatními prvky kryptografického řetězce a zprostředkovává jim služby zpravidla šifrování a dešifrování. Grafický model znázorňuje obrázek 2.1.

Obr. 2.1: Model kryptografického bezpečnostního modulu.

Na vstup kryptografického bezpečnostního modulu jsou přiváděna data nešifrovaná nebo šifrovaná. Modul poté na data aplikuje kryptografický algoritmus využívající šifrovací klíč. Výstupem jsou data šifrovaná nebo dešifrovaná dle toho, zda prováděnou operací bylo šifrování nebo dešifrování. Data v požadovaném formátu jsou pak předávána na výstup modulu, odkud jsou odesílána dalším prvkům kryptografického řetězce [2].

2.2 Běžné útoky na kryptografický modul

Dříve byly útoky na kryptografický bezpečnostní modul prováděny přímým využitím primárních kanálů. Útok vycházel z jednoduchého principu, kdy útočník zavedl na vstup vlastní datovou posloupnost a následně analyzoval výstupní datovou posloupnost modulu. Ze vztahu mezi vstupními a výstupními daty, pak bylo možné určit kryptografický algoritmus a následně i šifrovací klíč. Toto však bylo možné pouze u velmi jednoduchých kryptografických algoritmů, s postupně se zvyšující úrovní kryptografických algoritmů však tyto typy útoků postupně ztrácí na svém významu. Na obrázku 2.2 je graficky znázorněn princip běžných útoků na kryptografický modul.



Obr. 2.2: Princip běžného útoku na kryptografický bezpečnostní modul.

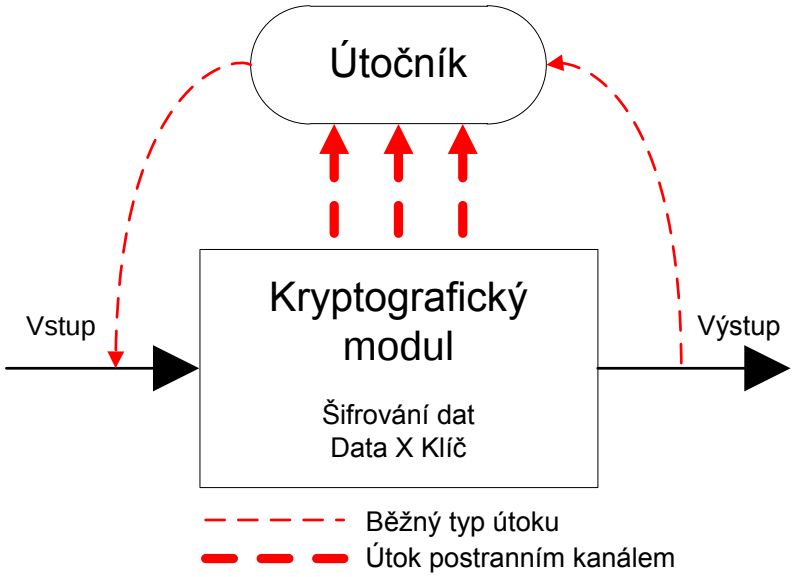
2.3 Útoky postranními kanály

Kryptografický bezpečnostní modul při své činnosti emituje do svého bezprostředního okolí elektromagnetické pole a teplo vzniklé důsledkem průchodu napájecího proudu, dále zvuk a světlo, které mohou být produkovány činností kontrolních prvků modulu nebo jako důsledek činnosti jednotlivých součástek modulu. Jedná se o fyzikální projevy spojené s celkovou činností modulu.

Na základě souvislostí mezi prováděnými operacemi modulu a fyzikálními projevy při jeho činnosti je možné usuzovat na konkrétní operace prováděné modulem. Stejně tak lze zohlednit např. dobu vykonávání šifrování, chybová hlášení nebo spotřebu energie. Ze souvislostí mezi těmito skutečnostmi a prací modulu lze opět usuzovat na konkrétní operace prováděné modulem, vznikají tak informační kanály, které v mnoha případech nejsou nijak ošetřeny, jejich využitím pak dochází k tzv. útokům postranními kanály. Na obrázku 2.3 je znázorněn princip všech útoků na kryptografický modul [2], [3].

2.4 Typy útoků dle přístupu ke kryptografickému modulu

Z dříve uvedených typů útoků je zřejmé, že jednotlivé typy se budou lišit dle toho, jaký přístup musí mít útočník k zařízení. U běžných typů útoků zpravidla postačovalo, aby se útočník dostal do blízkosti spojovacího vedení. Útoky postranními kanály již ale v některých případech vyžadují mnohem bližší přístup, mnohdy i



Obr. 2.3: Princip všech útoků na kryptografický bezpečnostní modul.

s nutností destrukce některých částí zařízení. Útoky na kryptografický modul je proto možné dále dělit na základě přístupu k zařízení a fyzických následků útoku na:

- útoky invazivní, kdy dochází k destrukci částí zařízení,
- útoky semi-invazivní, kdy nedochází k destrukci částí zařízení, ale je zapotřebí dostat se do těsné blízkosti zařízení,
- útoky neinvazivní, kdy útok nezasáhne do chodu zařízení a využívá zejména postranní kanály.

2.5 Přehled využívaných postranních kanálů

2.5.1 Časový postranní kanál

Časový postranní kanál využívá časových souvislostí v kryptografickém algoritmu. Operace prováděné kryptografickým modulem trvají ve většině případů přesně určitelnou dobu, která je závislá na zpracovávaných datech. Přesným měřením doby provádění jednotlivých operací je pak možné více či méně přesně určit zpracovávaná data. Tato metoda byla využívána zejména u jednodušších matematických šifrovacích algoritmů, které byly založeny například na násobení dat šifrovacím klíčem, pak bylo možné z doby zpoždění mezi vstupem a výstupem určit délku klíče nebo přímo klíč [4].

2.5.2 Chybový postranní kanál

Chybový postranní kanál využívá spojitost mezi chybami a jim příslušným chybovým hlášením modulu. Umělým zavedením chyby na vstup kryptografického modulu je vyvoláno chybové hlášení modulu. Analýzou vztahů mezi chybami a hlášením je možné získat informace vedoucí k získání šifrovacího klíče.

2.5.3 Akustický postranní kanál

Akustický postranní kanál je založen na analýze akustických projevů kryptografického modulu resp. jeho vstupních zařízení. Analýzou akustického spektra při zadávání údajů na klávesnici (PC, bankomat, telefon, vstupní terminál aj.) lze získat přímo tajný klíč nebo přístupové heslo. Další možností využití akustického postranního kanálu je monitorování akustického spektra v blízkosti součástek kryptografického modulu, které z principu své konstrukce mohou do svého okolí šířit akustický signál o vysoké frekvenci. Mohou to být cívky nebo kondenzátory [5].

2.5.4 Optický postranní kanál

Optický postranní kanál využívá velmi jednoduchého principu, který je založen na fyzikálních vlastnostech tranzistorů, z nichž se skládají paměťové moduly. Změnou stavu paměťové buňky dochází ke změnám stavů tranzistorů, z nichž je daná buňka složena. Tranzistor při každé změně svého stavu emituje velmi malé množství fotonů. Správným odkrytováním pouzdra paměťového modulu a využitím fotonásobiče je možné tyto fotony zachytit a vytvořit tak obraz činnosti paměti, ze kterého pak lze poměrně jednoduše přečíst požadované informace včetně šifrovacího klíče. Nevýhodou této metody je invazivní přístup a velmi vysoké náklady na její provedení [6], [7].

2.5.5 Výkonový postranní kanál

Výkonový postranní kanál je založen na analýze proudového odběru kryptografického modulu. Analyzováním vztahu mezi proudovým odběrem modulu a zpracovávanými daty je možné určit informace vedoucí k získání šifrovacího klíče [3], [8].

2.5.6 Elektromagnetický postranní kanál

Elektromagnetický postranní kanál je založen na analýze elektromagnetického pole v okolí kryptografického modulu. Elektromagnetické pole vznikající v důsledku průchodu elektrického proudu jednotlivými součástkami kryptografického modulu přímo souvisí s operacemi vykonávaného kryptografického algoritmu. Jelikož spolu velmi

úzce souvisí velikost vyzařovaného elektromagnetického pole a výkonový odběr kryptografického modulu, bývají oba typy těchto postranních kanálů využívány současně pro upřesnění získaných dat. Vhodnou analýzou elektromagnetického pole v okolí kryptografického modulu je možné získat informace vedoucí k získání šifrovacího klíče. Podrobněji se elektromagnetickým postranním kanálem budou zabývat následující kapitoly [9], [10], [11].

3 ELEKTROMAGNETICKÁ ANALÝZA

3.1 Elektromagnetické pole

Elektromagnetické pole je složeno z magnetického a elektrického pole, která jsou vzájemně fyzikálně propojena. Složky obou polí jsou na sebe vzájemně kolmé, současně jsou kolmé i na směr šíření energie. Teoreticky je elektromagnetické pole svým dosahem nekonečné, v praxi se ovšem omezuje pouze na tu oblast, která ovlivňuje tělesa v jeho okolí. K přesnému popisu elektrického a magnetického pole je využíváno Maxwellových rovnic.

Z pohledu kvantové fyziky je elektromagnetické pole základním přírodním projevem, neboť elektromagnetická interakce vzniká vzájemnou interakcí elementárních částic v důsledku interakce jejich vlastních elektromagnetických polí [9].

3.2 Elektromagnetické záření

Elektromagnetické záření je kombinací postupného příčného vlnění elektrického a magnetického pole, z výše uvedeného vyplývá, že se tedy jedná o pole elektromagnetické. Každý pohybující se elektrický náboj s nenulovým zrychlením vyzařuje do svého okolí elektromagnetické vlnění, jehož částicí je foton s energií:

$$E = hf, \tag{3.1}$$

kde h je Planckova konstanta a f frekvence. Průchodem elektrického proudu, pohybem nábojů, vodičem vzniká v okolí vodiče elektromagnetické pole. Tento princip platí i opačně, působením elektromagnetického pole na vodič se ve vodiči indukuje elektrické napětí. Elektromagnetické záření se vyskytuje v různých podobách, nejznámější je prosté světlo, dále rádiové vlny, rentgenové záření a další [9].

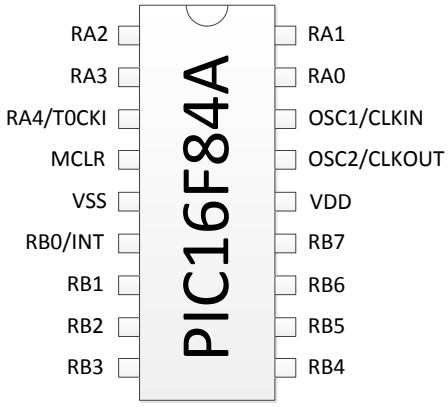
3.3 Vlastnosti mikrokontroléru PIC16F84A

Pro účely analýzy bude využíván mikrokontrolér PIC16F84A firmy Microchip. Jedná se o 8 bitový mikrokontrolér s univerzálním využitím, který je vyroben technologií CMOS. Disponuje 64 bajty programové paměti typu EEPROM a 68 bajty datové paměti typu RAM, konstrukce mikrokontroléru je tedy harvardského typu. Instrukční sada je typu RISC (redukovaná instrukční sada) a obsahuje celkem 35 různých jednoslovných instrukcí. Maximální taktovací kmitočet je 20MHz [12].

Mikrokontrolér má celkem 18 vývodů, z nichž 13 je použitelných jako vstupně/výstupní porty. Dále mikrokontrolér umožňuje využití časovačů a přerušení. Důležitou

vlastností pro samotné měření je technologie In-Circuit Serial Programming™, která umožňuje programování již osazeného a v obvodu zapojeného mikrokontroléru pomocí 2 pinů. Tato skutečnost bude při měření velkým přínosem, neboť bude možné dle potřeby rychle měnit zdrojové kódy bez nutnosti dalších manipulací s mikrokontrolérem.

Mikrokontrolér PIC16F84A bude na laboratorním pracovišti osazen na zkušební desce PICDEM™ 2 PLUS, která zajistí napájení a připojení taktovacího oscilátoru pro funkci obvodu. Zkušební deska zároveň poskytne snadný přístup k výstupním portům, jejichž pomocí bude měření synchronizováno a zároveň jimi bude mikrokontrolér programován. Zapojení vývodů PIC16F84A je uvedeno na obrázku 3.1.



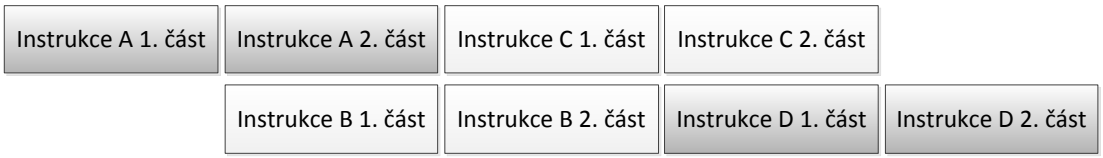
Obr. 3.1: Zapojení vývodů PIC16F84A.

3.3.1 Parametry PIC16F84A důležité pro analýzu

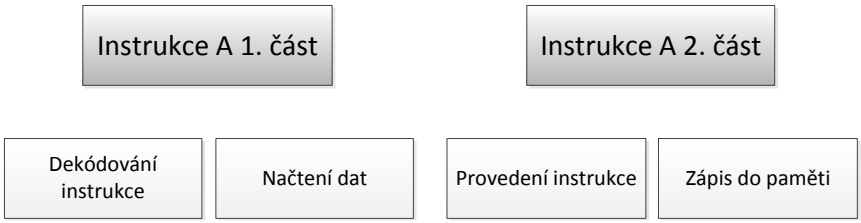
Nejdůležitějším faktem ovlivňujícím veškeré zpracování naměřených hodnot je u tohoto typu mikrokontroléru zřetězování instrukcí. Téměř každou instrukci je možné rozdělit na dvě části, v první části dochází k načtení hodnot prováděné instrukce do paměti, ve druhé pak samotné zpracování a zápis výsledných hodnot do paměti.

Velmi jednoduše je pak možné celé zpracování instrukcí pojmout jako dvě linie současného zpracování instrukcí s posunem o jednu část instrukce. Vždy tak probíhá současně zpracování aktuální instrukce a načítání hodnot instrukce následující. Princip řetězení instrukcí uvádí obrázek 3.2.

Výše uvedený princip je možné dále upřesnit, ve skutečnosti je totiž celá instrukce dělena na 4 části, pak tedy části A i B jsou složeny vždy ze dvou částí. V části A je nejprve instrukce dekódována a následně jsou načteny její hodnoty z paměti. V části B pak dojde k provedení samotné instrukce a následně pak k uložení výsledných hodnot do paměti. Dělení obou částí znázorňuje obrázek 3.3.



Obr. 3.2: Princip řetězení instrukcí.



Obr. 3.3: Dělení instrukce.

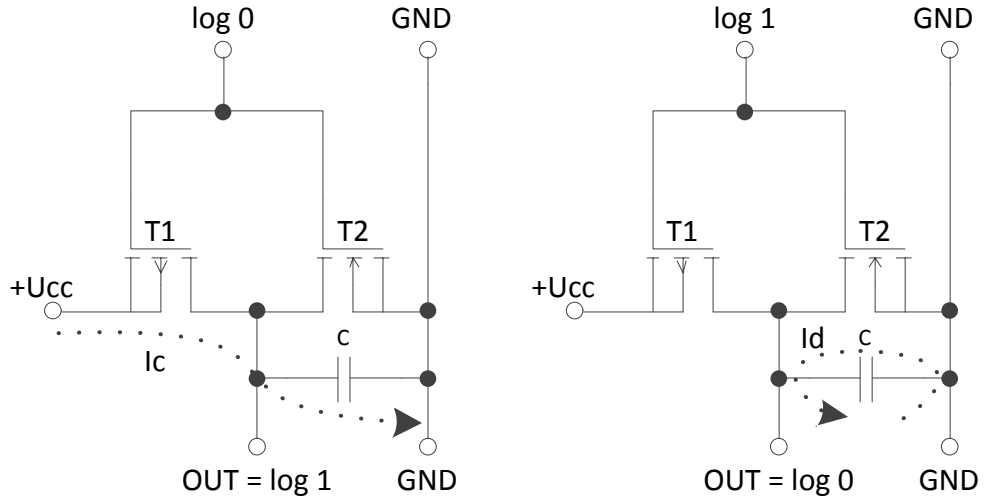
Toto dělení instrukcí je odvozeno od taktovacího kmitočtu mikrokontroléru, kdy kmitočet oscilátoru je interně dělen 4, doba trvání jedné elementární části instrukce tak trvá jednu čtvrtinu taktu. Dělení instrukcí ovlivňuje měření ve smyslu zpoždění výstupu, které pak není dáno pouze celkovým zpožděním zpracování, ale navíc právě uvedeným rozdělením instrukce na 4 části, a ve smyslu vzájemného překrývání instrukcí [12].

3.3.2 Elektromagnetická emise PIC16F84A

Uvedený mikrokontrolér je vyroben technologií CMOS, jejímž základním prvkem je logický invertor. Princip zapojení logického invertoru je uveden na obrázku 3.4.

Logický invertor je složen ze dvou MOS-FET tranzistorů ve funkci napětím řízených spínačů. Princip činnosti logického invertoru je velmi jednoduchý. Logická úroveň 0 na vstupu uzavře tranzistor T2, přes otevřený tranzistor T1 pak prochází proud Ic, který nabíjí kondenzátor C. Na výstupu je pak vstupní napětí, které odpovídá úrovni log. 1. Logická 1 na vstupu způsobí uzavření tranzistoru T1 a otevření tranzistoru T2, přes který se pak vybíjí kondenzátor C. Přes tranzistor T2 prochází vybíjecí proud Id a na výstupu je nulové napětí odpovídající log 0.

Během změny stavu dochází na velmi krátký časový úsek ke stavu, kdy jsou oba tranzistory otevřeny zároveň. V tomto okamžiku vzniká velmi krátká odběrová špička, která však nemá na elektromagnetickou emisi zásadní vliv. Hlavním zdrojem elektromagnetické emise je v tomto případě nabíjení a vybíjení kondenzátoru C, což je z časového hlediska delší děj, než samotná odběrová špička při přechodu



Obr. 3.4: Princip zapojení logického invertoru.

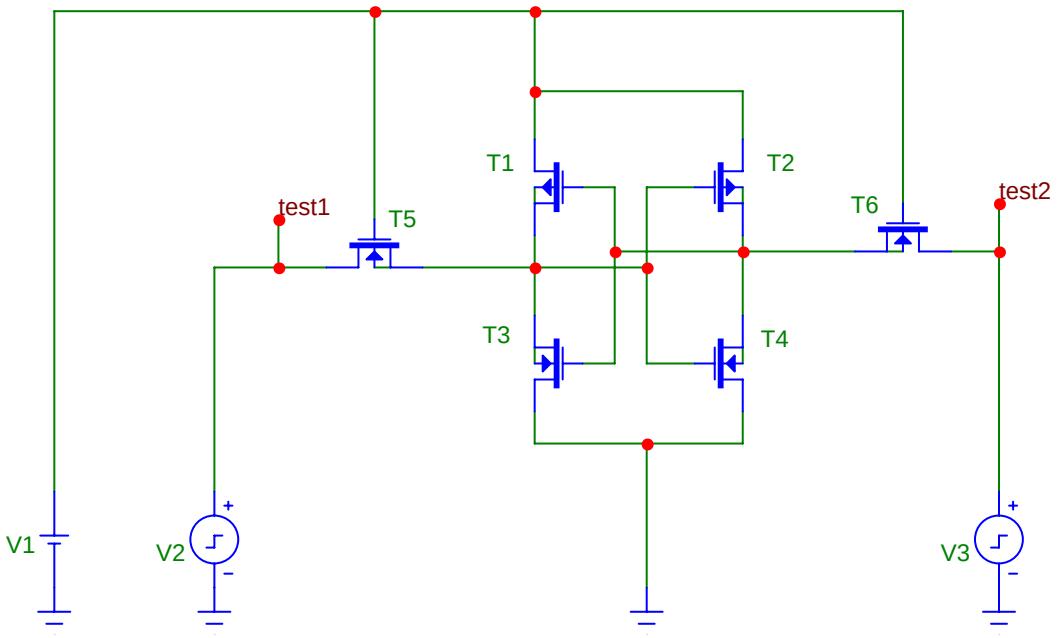
tranzistorů z jednoho do druhého stavu. Velikost vzniklého elektromagnetického pole je přímo úměrná počtu tranzistorů přecházejících mezi stavy.

3.3.3 Simulace chování logického invertoru

Před samotným měřením byly provedeny simulace chování logického invertoru v prostředí MicroCap. Simulace byla zaměřena zejména na vznik proudových špiček při změně stavu paměťové buňky založené na principu logického invertoru.

Paměťová buňka je v reálných obvodech složena ze 6 a více tranzistorů, z nichž 4 tranzistory tvoří samotný logický invertor a ostatní tranzistory slouží k výběru buňky v poli, do kterých jsou buňky zapojovány. Pro účely simulace byla vytvořena typická 6 tranzistorová buňka, jako zdroje změny logických hodnot byly použity dva pulzní zdroje s obdélníkovým průběhem. Oba zdroje jsou v protifázi, tím je docíleno chování běžně používaného invertoru na vstupu, ovšem s tím rozdílem, že v tomto případě je možné zcela přesně ovlivnit náběžné a sestupné hrany signálů. Zapojení je znázorněno na obrázku 3.5.

Jak již bylo uvedeno v kapitole 3.3.2, při změnách stavů paměťových buněk dochází k proudovým špičkám. Ty jsou způsobeny nabíjením a vybíjením kapacit přechodů tranzistorů T3 a T4, v modelu v kapitole 3.3.2 byly oba tranzistory pro zjednodušení nahrazeny kondenzátorem. Výstupní průběhy simulované paměťové buňky jsou uvedeny na obr. 15, na kterém jsou patrné proudové špičky při přechodech mezi oběma logickými stavy. Doba přechodu byla záměrně nastavena na dobu 20 ms, aby proudové špičky byly jasně patrné. Souvislost mezi dobou přechodu a velikostí proudové špičky je úměrná, se zkracující se dobou přechodu se proudová

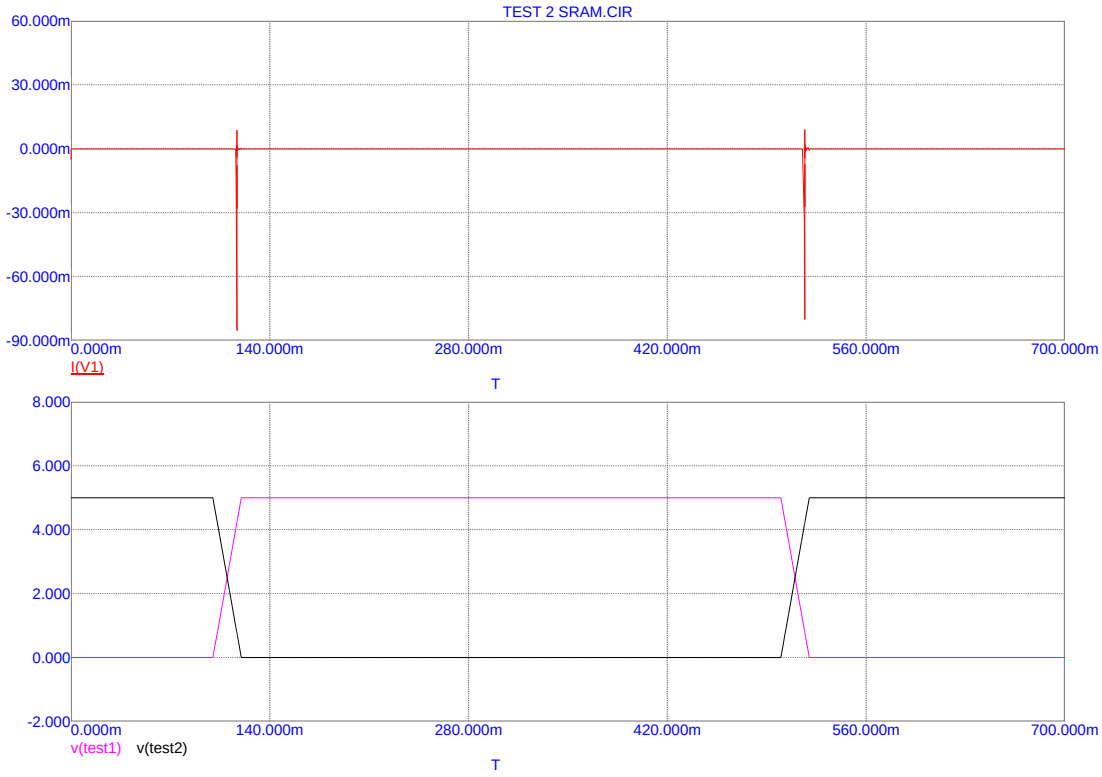


Obr. 3.5: Zapojení paměťové buňky pro simulaci.

špička zmenšuje. Výstupní průběhy simulace zachycuje obrázek 3.6.

Simulována byla i statická hodnota proudového odběru paměti složené ze 40 jednotlivých paměťových buněk. Jelikož ale není možné zcela přesně realizovat simulace celé paměti, byla realizována pouze simulace vlivu samotných paměťových buněk. Propojení mezi buňkami bylo provedeno jako ideální spoj, odpor vedení k jednotlivým buňkám tedy nebyl zohledněn. Výsledkem simulace je rozdíl mezi první a poslední buňkou nastavenou na log. 1 zhruba 9 nA, což je hodnota zanedbatelná. Pokud by ovšem byly zohledněny všechny parazitní vlastnosti, včetně zmíněných odporů spojů a pokud by bylo zohledněno i chování obvodu zajišťujícího výběr konkrétní buňky (multiplexery pro výběr řádku a sloupce matice buněk), pak by zřejmě výsledná hodnota rozdílu statického proudového odběru byla výrazně vyšší.

Pomocí simulace chování paměťové buňky složené z logického invertoru v prostředí MicroCap byly zjištěny souvislosti pro vznik elektromagnetického pole v okolí paměťové buňky. Ze simulovaných hodnot je možné odvodit souvislost mezi délkou změny logických stavů paměťové buňky a velikostí vzniklého elektromagnetického pole. Pomocí hodnot získaných simulacemi bylo možné velmi zhruba odvodit velikost indukovaného magneto-motorického napětí sondy. Po dosazení řádů jednotlivých hodnot do vztahu 3.2 a následně do vztahu 3.3 byla zjištěna předpokládaná hodnota indukovaného napětí v okolí hodnoty 1,1 mV, která odpovídá reálně naměřeným hodnotám.



Obr. 3.6: Výstupní průběhy simulace paměťové buňky.

3.4 Měření elektromagnetického pole

Měření elektromagnetického pole jsou realizována pomocí elektrických nebo magnetických sond v tzv. blízké oblasti zdroje elektromagnetického pole. Blízké pole je definováno vzdáleností sondy od zdroje, která nesmí být delší než délka jedné vlny. Pro tuto oblast pak lze definovat Biot-Savartův zákon magnetické indukce pole $\vec{B}$:

$$d\vec{B} = \frac{\mu I \ \vec{dl} \times \hat{r}}{4\pi \left|\hat{r}\right|^2}, \tag{3.2}$$

kde μ značí permeabilitu prostředí, I značí proud, $\vec{dl}$ značí vektor délky diferenčního elementu, jež zároveň určuje směr konvenčního proudu a $\hat{r}$ označuje vzdálenost mezi zdrojem elektromagnetického záření a místem měření. Pro $\hat{r}$ platí vztah $\hat{r} = \frac{\hat{r}}{|\hat{r}|}$. Jako sonda pro měření magnetického pole je využíván vodič navinutý do tvaru solenoidu. V blízké oblasti zdroje elektromagnetického pole je pak pomocí této sondy možné měřit magnetickou složku elektromagnetického pole. Velikost magneto-motorického napětí indukovaného v sondě lze vyjádřit pomocí Faradayova zákona:

$$U_{emf} = -N\frac{d\Phi}{dt}, \tag{3.3}$$

kde N je počet závitů vodiče sondy, $d\Phi$ vyjadřuje změnu magnetického toku za dobu dt [9], [14].

3.4.1 Sonda pro měření magnetické složky elektromagnetického pole

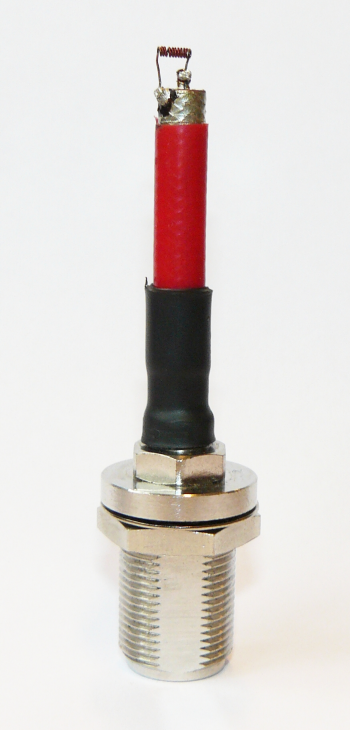
Jako sonda magnetické složky elektromagnetického pole je využíván vodič navinutý do tvaru solenoidu, jak již bylo zmíněno v předchozí kapitole. Ze vztahu 3.3 je zřejmé, že počet závitů N je přímo úměrný velikosti indukovaného magneto-motorického napětí, což znamená, že indukované napětí bude tím větší, čím větší bude počet závitů sondy. Pro konkrétní měření malých zdrojů elektromagnetického pole, typicky právě částí kryptografických modulů jako jsou například procesor, paměti a datové sběrnice, je však nutné, aby sonda měla malé rozměry a snímala pouze vybranou část zařízení. Pro takto konkrétní měření je pak nutné zvážit a laboratorně otestovat rozměrovou konstrukci sondy a počet závitů volit vhodně tak, aby velikost indukovaného napětí byla dostatečně velká a rozměry dostatečně malé pro daný typ měření. Při větších rozměrech by docházelo k měření elektromagnetických polí více zdrojů, což by znehodnotilo nebo negativně ovlivnilo prováděná měření.

3.4.2 Konkrétní konstrukce sondy

Na pracovišti elektromagnetické analýzy na Ústavu telekomunikací Vysokého učení technického v Brně již byla realizována laboratorní měření, při kterých byly navrženy a odzkoušeny různé konstrukce sond magnetické složky elektromagnetického pole. Pro laboratorní pracoviště pak byla vybrána konkrétní sonda navinutá měděným vodičem o průměru 0,3 mm s počtem 11 závitů. Touto sondou bylo realizováno několik měření, kterými bylo zjištěno, že pro aplikace tohoto pracoviště je velikost indukovaného magneto-motorického napětí dostatečně velká a není ovlivňována jinými částmi měřených zařízení. Mechanickou konstrukci sondy zachycuje obrázek 3.7. Další možné konstrukce uvádí pramen [9].

3.5 Pracoviště elektromagnetické analýzy

Ústav telekomunikací Vysokého učení technického v Brně disponuje pracovištěm, kde byla vyrobena a odzkoušena sonda uvedená v kapitole 3.4.1. Pracoviště sestává z osobního počítače s nainstalovaným softwarem MPLAB IDE v8.63, který zajišťuje možnost tvorby zdrojových kódů částí šifrovacích algoritmů pro následnou implementaci v mikrokontroléru PIC16F84A osazeného na zkušební desce Microchip PICDEM^{TM} 2 PLUS, [13]. S uvedenou deskou je počítač propojen přes programátor



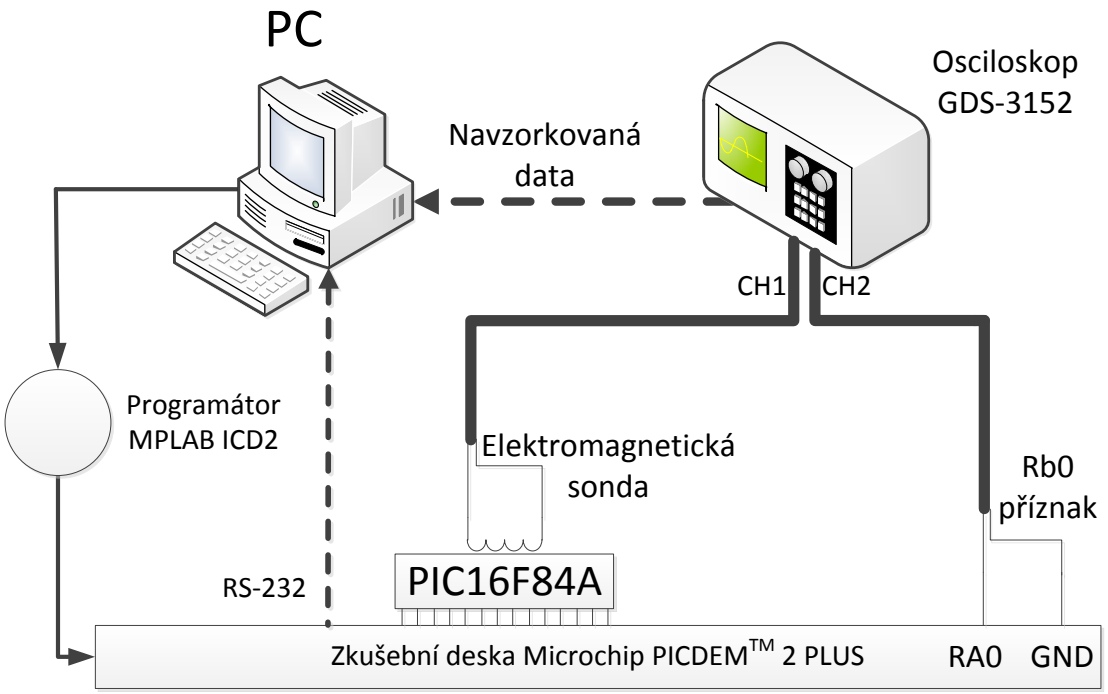
Obr. 3.7: Sonda pro měření magnetické složky elektromagnetického pole.

MPLAB ICD2 a přes standardní sériový kabel. Dále je na PC nainstalován software Matlab, kterým jsou zpracovávána naměřená data z připojeného osciloskopu GDS–3152, později byl nahrazen přístrojem Tektronix DPO4032. K osciloskopu je připojena sonda magnetické složky elektromagnetického pole a výstupní port mikrokontroléru, který slouží k synchronizaci měřeného průběhu. Schéma zapojení pracoviště je uvedeno na obrázku 3.8.

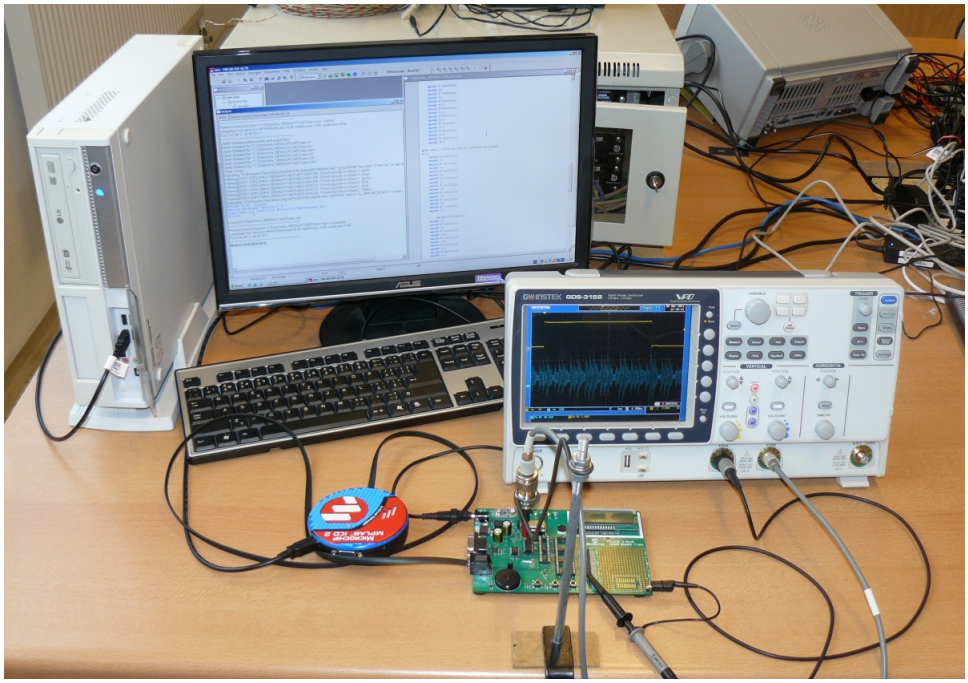
Celé pracoviště je zachyceno na fotografii 3.9, dále je na fotografii 3.10 zachycen detail umístění sondy nad mikrokontrolérem PIC16F84A, který má částečně upravenou horní stranu pouzdra tak, aby sonda mohla být umístěna co nejblíže ke zdroji elektromagnetického pole a aby byla dodržena podmínka aplikace Biot–Savartova zákona, tedy umístění sondy v tzv. blízké oblasti.

3.6 Šifrovací algoritmus AES

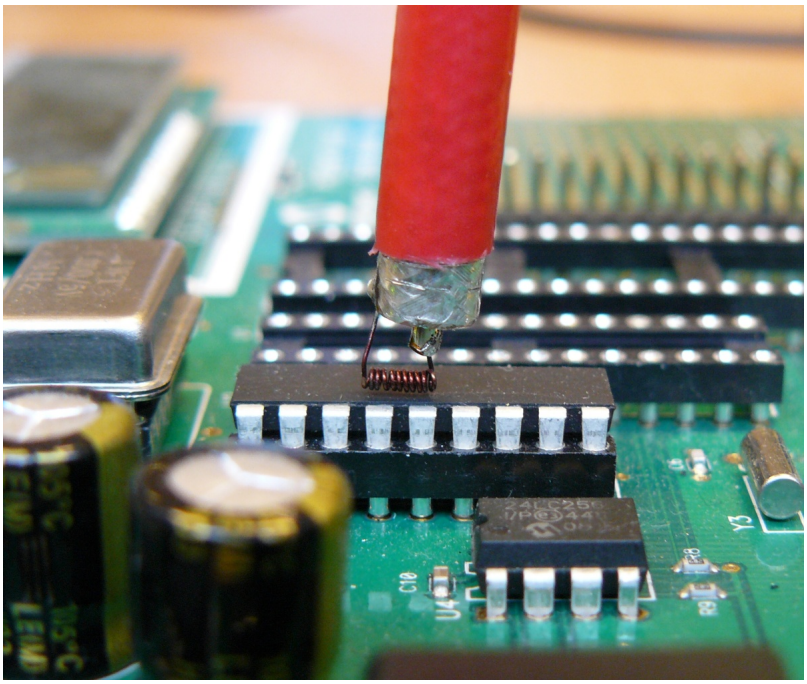
Šifrovací algoritmus AES je symetrický šifrovací algoritmus, využívá pro šifrování i dešifrování shodný klíč. Vstupní data jsou rovnoměrně dělena na bloky o délce 128 bitů a následně šifrována pomocí klíče o délce 128, 192 nebo 256 bitů. Jednotlivé bloky dat postupně prochází algoritmem v tzv. rundách (opakováních), při kterých jsou prováděny 4 různé operace: AddRoundKey, SubBytes, ShiftRows, MixColumns.



Obr. 3.8: Schematické zapojení měřicího pracoviště.



Obr. 3.9: Fotografie pracoviště.



Obr. 3.10: Detail umístění sondy.

Počet rund Nr závisí na délce klíče, závislost uvádí tabulka 3.1. Pro laboratorní měření bude použit algoritmus AES s délkou klíče 128 bitů.

Tab. 3.1: Závislost počtu rund na délce šifrovacího klíče

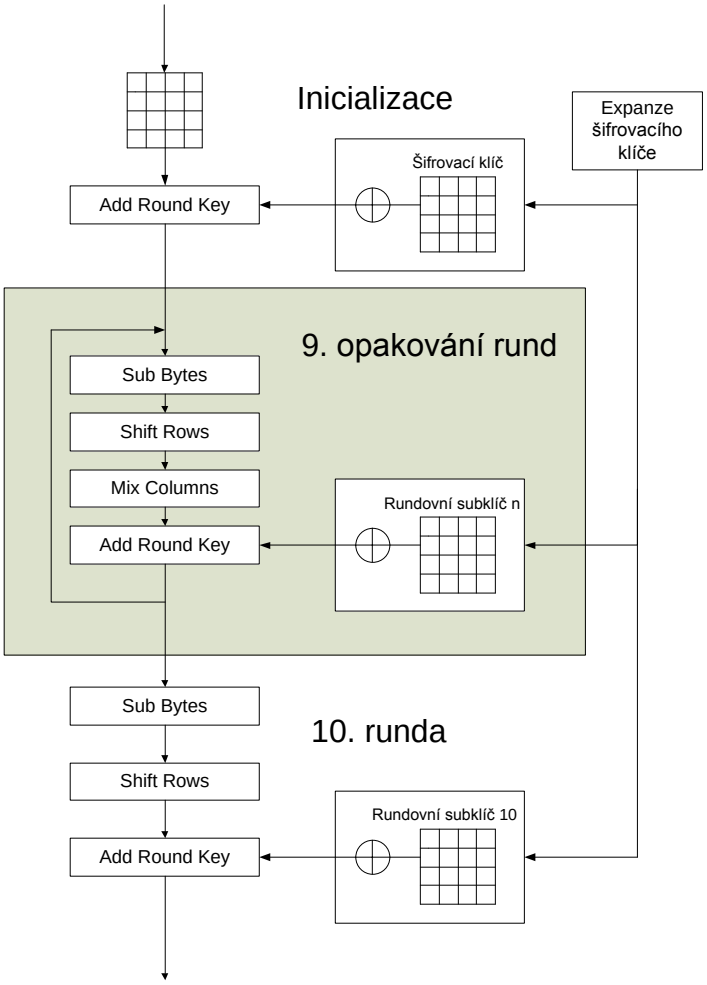
-	Klíč 128 bitů	Klíč 192 bitů	Klíč 256 bitů
N_r	10	12	14

Během provádění algoritmu dochází postupně k odvozování nového šifrovacího klíče (subklíče) pro každou rundu, tato operace je nazývána expanze šifrovacího klíče. Jednotlivé fáze algoritmu AES jsou následující:

1. Na začátku algoritmu probíhá operace AddRoundKey, při které dochází k exkluzivnímu součtu (XOR) vstupních stavových dat a šifrovacího klíče.
2. Následuje 10 rund, kdy dochází k operaci SubBytes, což je substituce dle substituční tabulky S-BOX, dále k operaci ShiftRows, která posouvá řádky datové matice o určitý počet míst, následně dojde k operaci MixColumns, která každý sloupec datové matice vynásobí maticí (tato matice je shodná pro všechny rundy). V závěru každé rundy je provedena operace AddRoundKey, která provede exkluzivní součet upravené datové matice s odvozeným šifrovacím klíčem (subklíčem).

3. V poslední rundě je vynechána operace MixColumns, ostatní operace probíhají standardně.

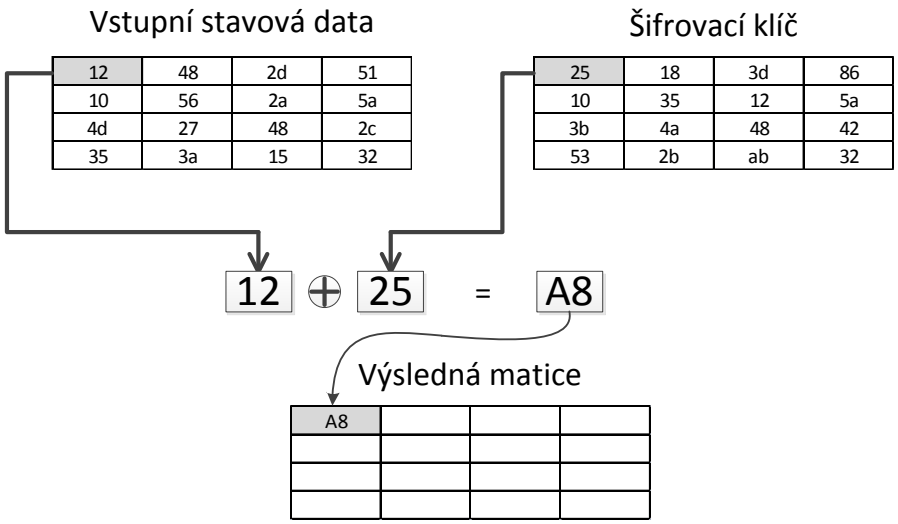
Celý průběh algoritmu AES s použitím 128 bitového klíče zachycuje obrázek 3.11.



Obr. 3.11: Schéma činnosti šifrovacího algoritmu AES.

Pro účely měření je nejdůležitější inicializační fáze celého algoritmu, zejména první operace AddRoundKey, kdy dochází k exkluzivnímu součtu vstupní stavové matice s šifrovacím klíčem. Tato část je jedinou fází v algoritmu, kdy se pracuje s nezměněným původním šifrovacím klíčem, je tedy ideální fází k útoku postranním kanálem. Princip operace AddRoundKey je uveden na obrázku 3.12.

Jelikož měření bude zaměřeno právě na operaci AddRoundKey, nejsou ostatní operace prováděné algoritmem AES pro měření podstatné, jejich podrobný popis proto nebude uveden [15], [16].



Obr. 3.12: Princip operace AddRoundKey.

3.7 Příprava zdrojového kódu pro měření

Zdrojový kód pro měření obsahuje pouze část algoritmu AES a to již zmíněnou operaci AddRoundKey v programovacím jazyce Assembler. Program tedy obsahuje pouze vstupní stavová data a šifrovací klíč, který je rozdělen dle zadání práce po bajtech. Mezi daty a klíčem probíhá operace XOR v nekonečném cyklu. Pro každou operaci XOR je vzhledem k použitému mikrokontroléru nutné provést vždy načtení hodnoty klíče a stavu (vstupní hodnoty dat) do pracovních registrů, mezi nimiž je pak možné operaci XOR provést. Ukázka instrukcí pro operaci XOR:

- `movf k0,w`,
- `xorwf s0,f`.

Zdrojový kód umožňuje změnu klíče za chodu programu bez nutnosti přeprogramování programové paměti. Pro kontrolu nastavených hodnot klíče program obsahuje implementaci komunikace po sériové lince, mikrokontrolér odesílá do PC údaj s aktuálně nastavenou hodnotou klíče. Kompletní výpis zdrojového kódu je uveden v elektronické příloze.

4 LABORATORNÍ MĚŘENÍ

Laboratorní měření probíhalo na pracovišti elektromagnetické analýzy Ústavu telekomunikací Vysokého učení technického v Brně, bližší popis pracoviště je uveden v kapitolách 3.4.2 a 3.5. Pro měření byl využit mikrokontrolér PIC16F84A ve funkci simulátoru kryptografického modulu, v němž byl implementován program dle zdrojového kódu uvedeného v kapitole 3.7.

4.1 Úvodní měření

Dílčím cílem úvodního měření bylo nastavení optimálního zobrazení použitých měřicích přístrojů a polohy sondy s ohledem na velikost signálu a obsah šumu. Hlavním cílem tohoto měření bylo následné určení oblasti měřeného signálu, ve které lze pozorovat vliv změny průběhu elektromagnetického pole v závislosti na použitém šifrovacím klíči. Parametry zobrazování pro oba osciloskopy uvádí tabulka 4.1 a tabulka 4.2.

Tab. 4.1: Nastavení parametrů osciloskopu GW Instek GDS-3152 pro měření

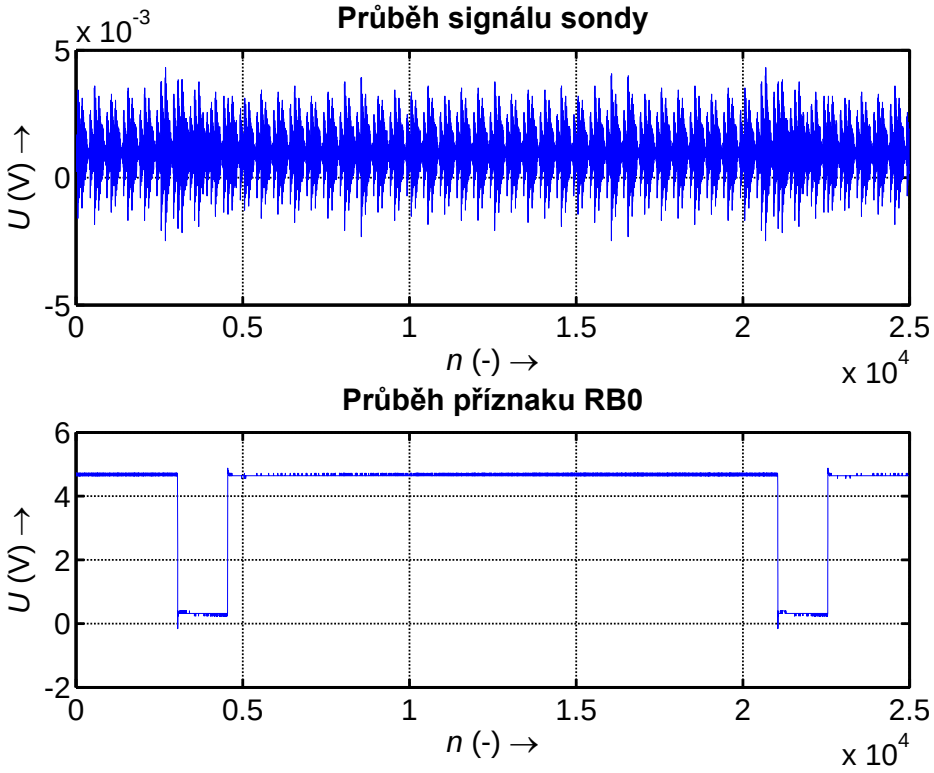
Kanál 1	Příznak na RB0
Kanál 2	Signál ze sondy
Snímací mód	Průměrování ze 32 vzorků
Synchronizace	Nástupná hrana 1. kanálu
Coupling	DC
Sampling rate	Max. 2,5 GSa/s

Tab. 4.2: Nastavení parametrů osciloskopu Tektronix DPO4032 pro měření

Kanál 1	Signál ze sondy
Kanál 2	Příznak na RA0
Snímací mód	Průměrování ze 16 vzorků
Synchronizace	Nástupná hrana 2. kanálu
Coupling	DC
Sampling rate	Max. 2,5 GSa/s

Zachycené výstupní signály uvádí obrázek 4.1. Zdrojový kód obsahuje nekonečnou smyčku, v níž se operace AddRoundKey provede celá vždy dvakrát. Na začátku

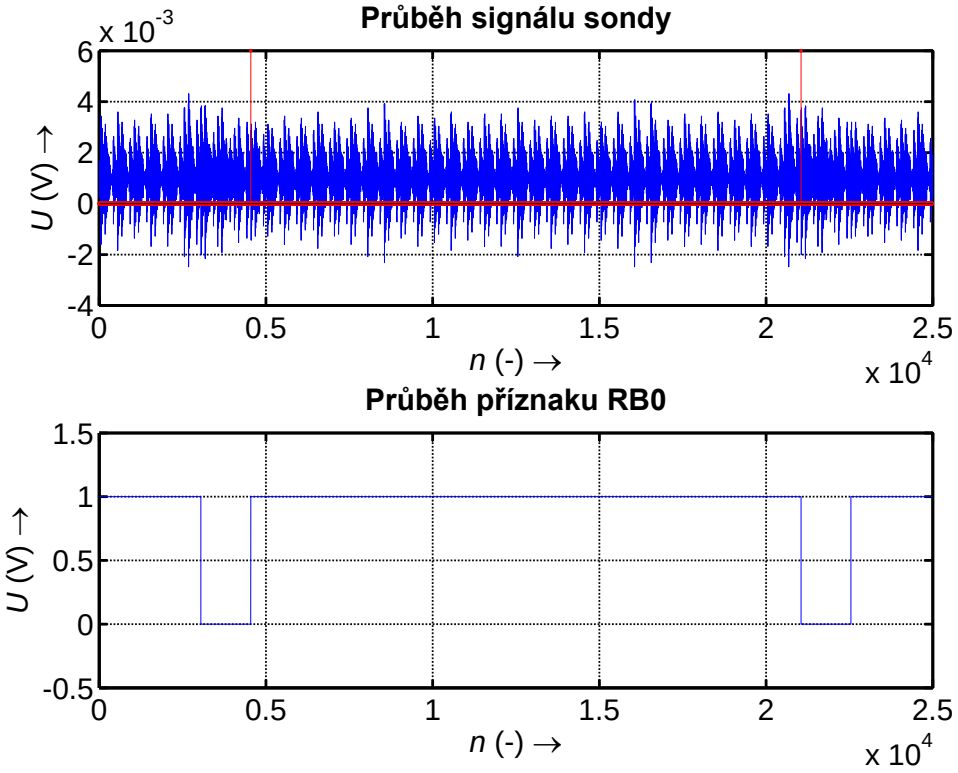
celého cyklu je nastaven příznakový bit RB0 na hodnotu log. 1, při skončení druhého opakování cyklu je bit RB0 nastaven na hodnotu log. 0. Během celého sledovaného cyklu proběhne celkem 32 period, z čehož 16 period náleží vždy každé celé operaci AddRoundKey. Z naměřených hodnot je možné velmi dobře těchto 32 jednotlivých bloků, které odpovídají jednotlivým operacím načítání hodnot a exkluzivního součtu, odečíst. Po úpravě synchronizačního signálu RB0 je možné s jeho pomocí detekovat hrany a označit tak v průběhu signálu ze sondy pouze požadovanou část průběhu. Označení této části průběhu zachycuje obrázek 4.2.



Obr. 4.1: Výstupní průběhy po nastavení osciloskopu.

4.1.1 Extrakce užitečného signálu

Původní signál byl upraven do podoby, kdy podle příznaku RB0 byly odstraněny přebytečné hodnoty. Výsledný signál zobrazuje obrázek 4.3. Na obrázku je patrné, že první a poslední pulzy nejsou kompletní, jedná se o chybu způsobenou přepínáním stavu bitu RB0, každá operace je dělena na 4 části (viz kapitola 3.3.1), k fyzické změně stavu tedy nedochází okamžitě v místě zápisu instrukce, ale až po jejím úvodním zpracování, čemuž odpovídají průběhy prvního a poslední pulzu.

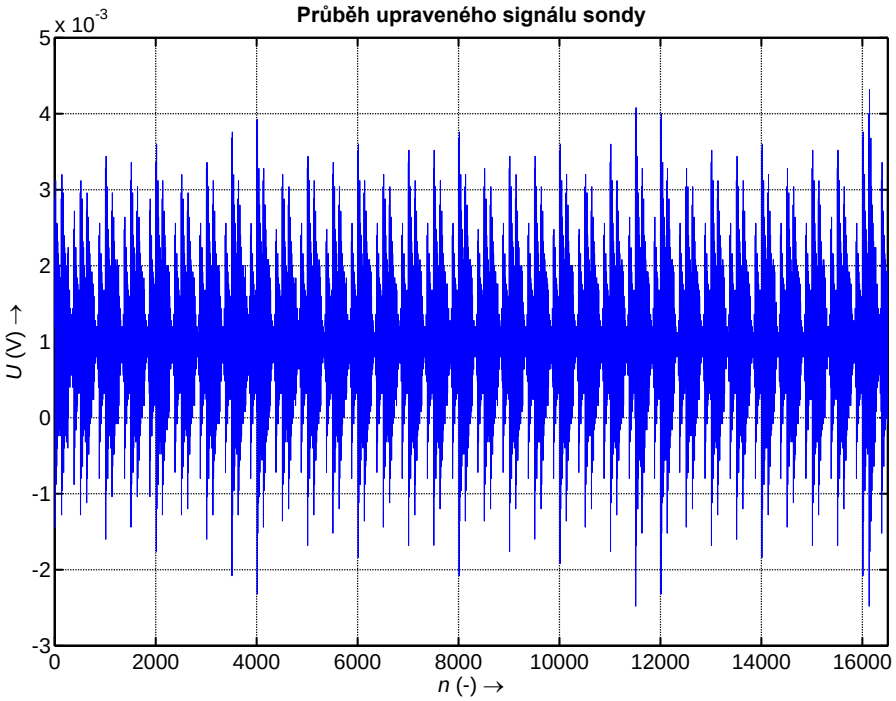


Obr. 4.2: Označení požadované části pomocí signálu RB0.

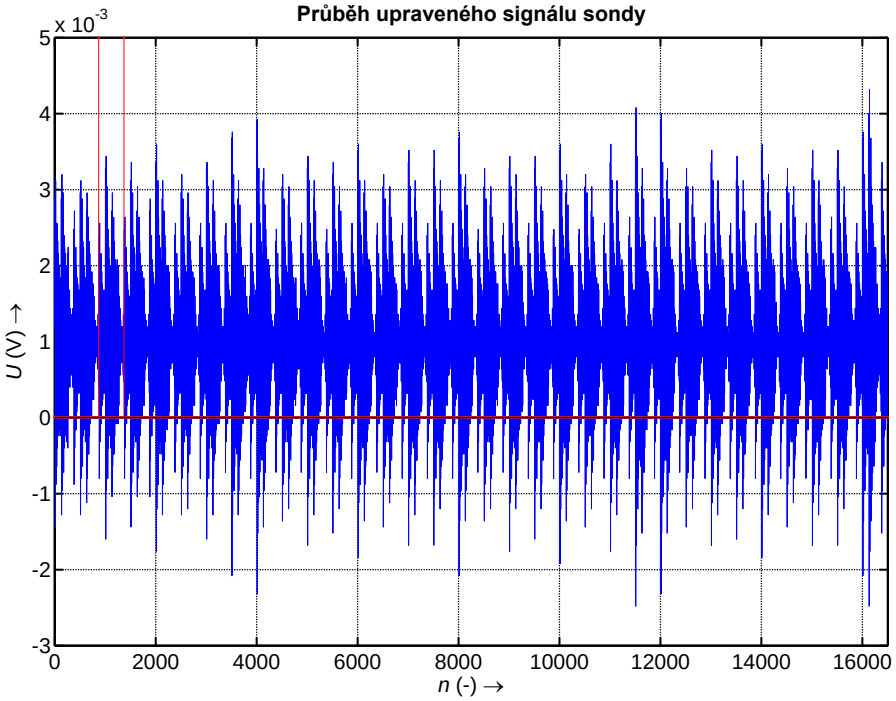
Cílem práce je analýza průběhu pro jeden bajt klíče. Z upraveného signálu byl tedy s ohledem na zadání práce vybrán pouze průběh pro bajt k2. Bajt k2 byl vybrán náhodně, z výběru byly vyřazeny pouze průběhy prvního a posledního bajtu vzhledem k tomu, že by mohly být zmíněným překrýváním instrukcí ovlivněny předchozí nebo další instrukcí. Lokace průběhu bajtu k2 v celém průběhu je zachycena na obrázku 4.4.

4.1.2 Měření průběhu signálu pro bajt k2

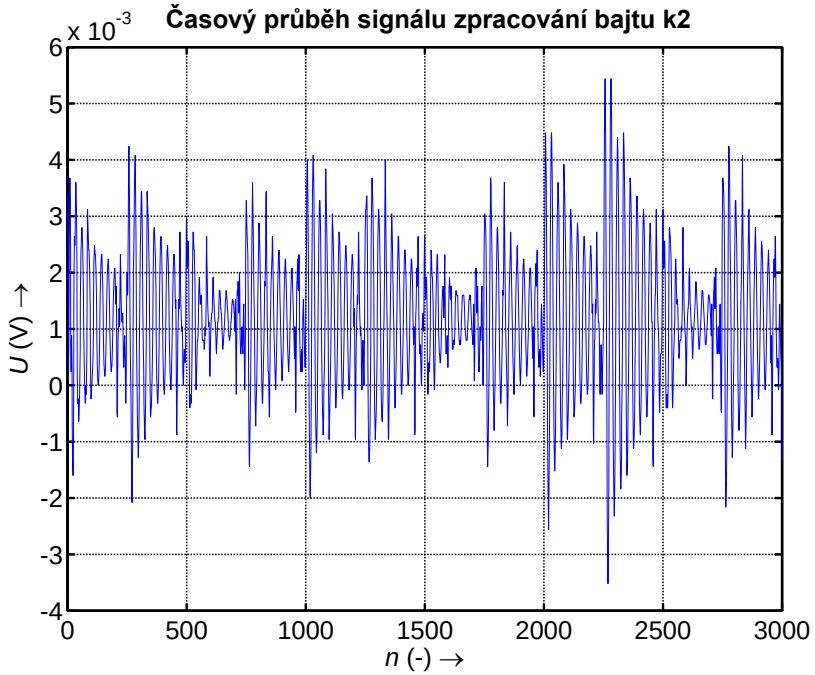
Další měření probíhala výhradně pro signál sondy z oblasti zpracování bajtu k2. Výstupní průběh signálu bajtu k2 zachycuje obrázek 4.5. Porovnáním průběhů pro různé polohy nenulového bitu v bajtu byla zjištěna oblast, ve které dochází ke změnám v průběhu. Tato oblast je označena na obrázku 4.6. Průběh takto získaného užitečného signálu sondy pro analýzu je uveden na obrázku 4.7.



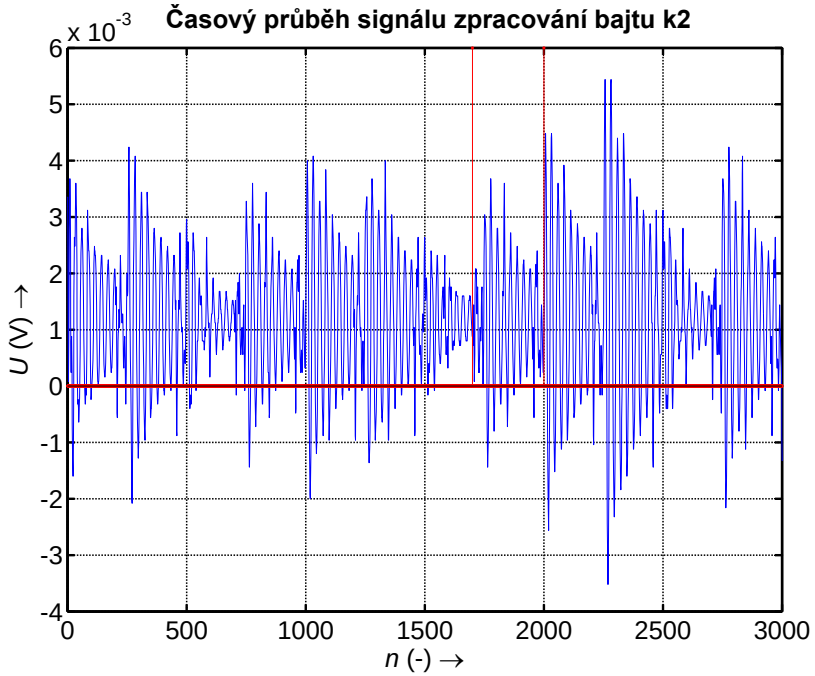
Obr. 4.3: Průběh upraveného signálu sondy.



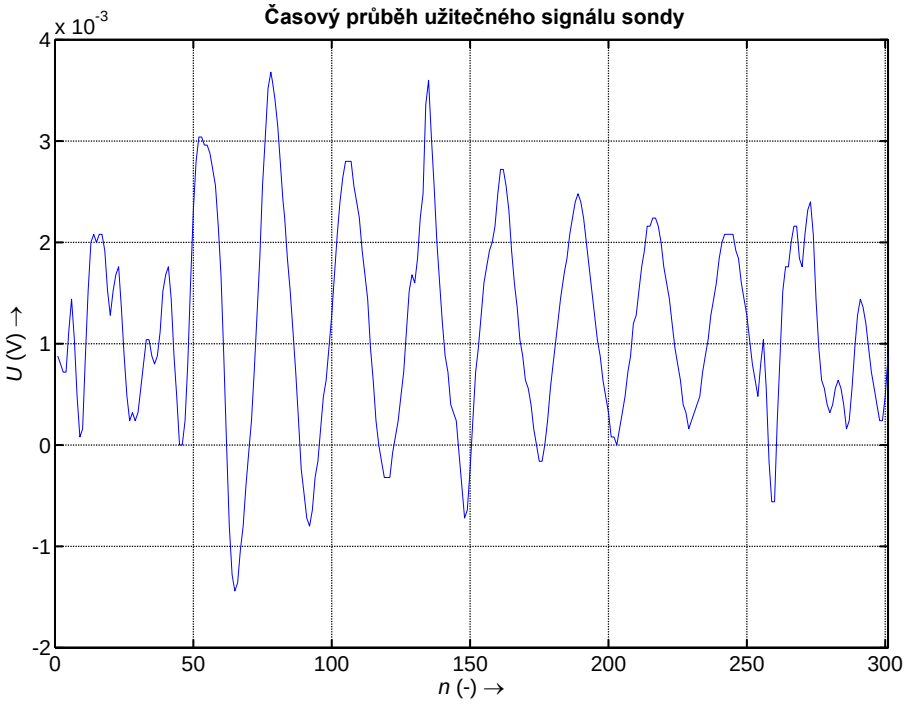
Obr. 4.4: Označení bajtu k2 v upraveném signálu sondy.



Obr. 4.5: Časový průběh signálu oblasti zpracování bajtu k2.



Obr. 4.6: Označení oblasti změn dle polohy nenulového bitu v bajtu k2.



Obr. 4.7: Užitečný signál sondy pro analýzu.

4.2 Vytvoření souboru hodnot pro analýzu

Stejným způsobem jako u úvodního měření byly změřeny průběhy pro všech 256 možných hodnot klíče v bajtu k2. Následnou úpravou změřených průběhů do podoby užitečného signálu bajtu k2, uvedeného na obrázku 4.7, vznikla sada vzorových průběhů, která se skládá z 256 MAT souborů. MAT soubory obsahují pouze užitečnou část průběhu, ve které lze pozorovat změny průběhu v závislosti na poloze nebo počtu nenulových bitů v bajtu.

Tato sada slouží jako vzorová, následně bylo provedeno další měření, při kterém vznikla druhá sada průběhů určená pro testování a analýzu, tato sada je mírně odlišná od předchozí sady, jelikož se jednalo o samostatné měření je tato sada zatížena chybou nastavení polohy sondy, čímž více odpovídá reálnému měření při útoku.

Měření pro takto velký rozsah hodnot vyžadovalo přesnou kontrolu nastavených hodnot klíče, proto bylo pracoviště oproti předchozím měřením doplněno o komunikační rozhraní RS-232, jehož pomocí byla hodnota klíče odesílána v textové podobě do PC. Pro tato měření byl využit osciloskop Tektronix DPO4032 z důvodu zvýšení přesnosti měření, jelikož uvedený typ přístroje umožňuje export naměřených hodnot s celkovým počtem 100.000 hodnot v jednom souboru, navíc bylo možné snížit průměrování na hodnotu 16 a tím docílit menšího potlačení malých detailů v průběhu.

5 VÝSLEDKY MĚŘENÍ

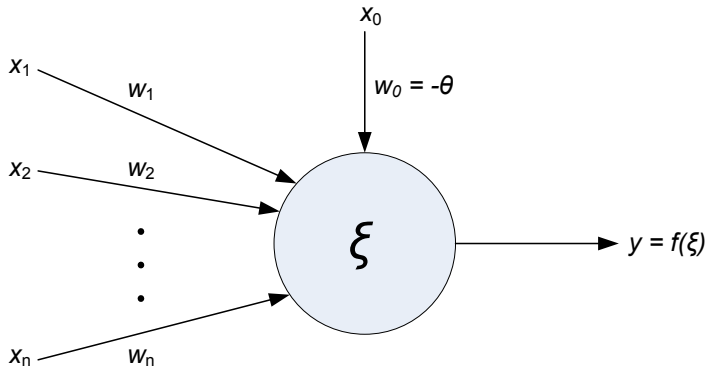
Zpracování naměřených dat bylo provedeno v prostředí Matlab. Toto prostředí poskytuje široké možnosti pro implementaci matematických metod zpracování signálů. Jedním z hlavních důvodů využití právě tohoto prostředí je možnost přímého zpracování CSV souborů, které jsou výstupním datovým formátem obou použitých osciloskopů. Prostředí Matlab disponuje velkým množstvím funkcí, které pak není třeba složitě implementovat. Výhodou je také dostupnost tzv. toolboxů, souborů funkcí a skriptů pro řešení konkrétních problémů. Pro zpracování dat z měření byla použita neuronová síť vytvořená pomocí Netlab Neural Network toolbox. Autory tohoto toolboxu jsou Ian Nabney a Christopher Bishop z Aston University v Birminghamu. Toolbox je volně ke stažení na adrese:
<http://www1.aston.ac.uk/eas/research/groups/ncrg/resources/netlab/>, [17].

5.1 Umělá neuronová síť

Umělá neuronová síť je postavena na základech biologické neuronové sítě, stejně jako u biologické sítě dochází k učení a k následné aplikaci naučených znalostí. Poznatky získané ze studia biologických neuronových sítí byly aplikovány do matematického modelu, který stejně jako bilogická předloha zakládá svůj princip učení na změnách spojů mezi základními stavebními prvky sítě – neurony. V biologické síti dochází při učení k fyzickému vytvoření spoje mezi jednotlivými neurony, v umělé síti jsou spoje předem vytvořeny a dochází pouze ke změně parametrů spoje.

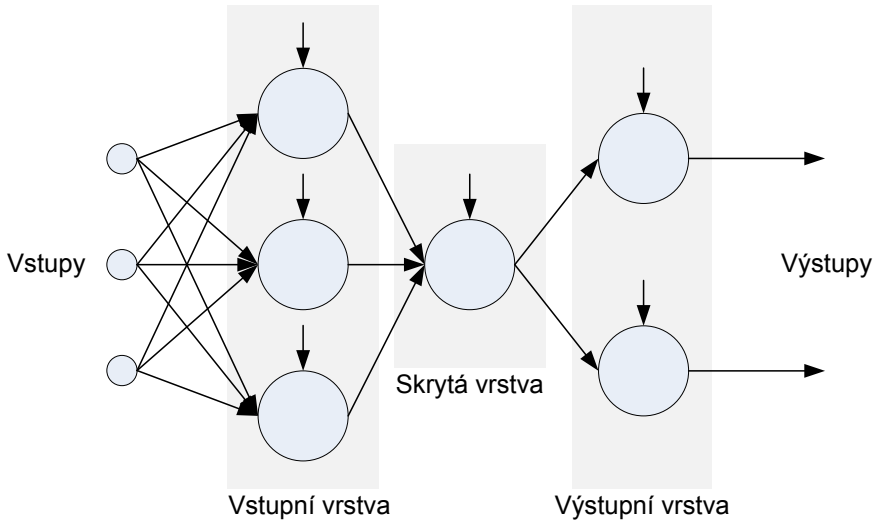
Základní prvek umělé neuronové sítě je formální neuron, v literatuře též perceptron. Jeho jednoduchý model je znázorněn na obrázku 5.1. Formální neuron má x vstupů o vahách w. Vstup x_0 s váhou $w_0 = -\theta$ určuje prahovou hodnotu neuronu. Při učení neuronu dochází k přepočtu hodnot vah za účelem co nejbližšího přiblížení se k požadované výstupní hodnotě. Nejprve probíhá výpočet post-synaptického potenciálu, který je definován jako vnitřní funkce neuronu $\xi = \sum_{i=1}^{n} x_i w_i - \theta$ a má nejčastěji sigmoidní průběh. Z výsledné funkce ξ je pak vypočtena výstupní hodnota neuronu $y = f(\xi)$, [18].

Jeden formální neuron není možné samostatně použít s vyjímkou ukázkových a výukových příkladů. Pro řešení složitějších problémů jsou využívány sítě neuronů, jejichž topologií je dán konkrétní okruh problémů, pro jejichž řešení jsou tyto sítě vhodné. V nejjednodušším případě je síť složena ze dvou vrstev, vrstvy vstupní a vrstvy výstupní. Vstupní vrstva obsahuje tolik neuronů, kolik vstupních hodnot je třeba pomocí sítě zpracovávat. Výstupní vrstva analogicky ke vstupní obsahuje tolik neuronů, kolik obsahuje výsledek hodnot. Pro řešení složitých problémů však toto



Obr. 5.1: Formální neuron.

uspořádání nemusí být výhodné zejména s ohledem na dobu učení sítě, proto je běžně závaděna jedna nebo více tzv. skrytých vrstev, které se podílí na urychlení a upřesnění učení dané neuronové sítě. Označení základní topologie sítě je pak uváděno dle počtu neuronů v jednotlivých vrstvách např. 3–1–2, což odpovídá 3 neuronům ve vstupní vrstvě, 1 neuronu ve skryté vrstvě a 2 neuronům ve výstupní vrstvě. Uvedená topologie sítě je znázorněna na obrázku 5.2, [18].



Obr. 5.2: Umělá neuronová síť 3–1–2.

Celou funkci umělé neuronové sítě lze shrnout do dvou základních fází. První fází je fáze učení, v literatuře též trénování, sítě. V podstatě se jedná o matematický postup úpravy jednotlivých vah tak, aby výstup sítě odpovídal zadanému vzoru. K tomu je využito výpočtu chyby sítě, na jehož základě jsou hodnoty jednotlivých vah postupně upravovány.

Učení probíhá v cyklu opakování, kdy nejprve dojde k nastavení jednotlivých vah, následně k výpočtu výstupní hodnoty a výpočtu chyby oproti požadované hodnotě. Poté jsou na základě vypočtené chyby váhy jednotlivých neuronů přenastaveny a probíhá znovu výpočet výstupu a chyby pro zjištění, zda došlo ke snížení chyby a zda byla změna vah provedena správně. Jeden cyklus učení nazýváme iterací. Pro naučení sítě je v závislosti na typu sítě a řešeném problému zapotřebí provést stovky až tisíce iterací, aby bylo dosaženo optimálních výsledků. Uvedený princip je obecně nazýván jako zpětné šíření chyby a patří k nejpoužívanějším principům učení neuronových sítí. Existují i další principy, které jsou založeny na jiných principech učení, např. bez vzoru, s dopředným šířením chyby atd. Tyto však nebudou blíže rozebrány, neboť neuronová síť použitá pro zpracování hodnot elektromagnetické analýzy je založena právě na principu zpětného šíření chyby.

Druhou fází funkce umělé neuronové sítě je využití naučené sítě k řešení problému. Po předložení vstupních hodnot je pomocí sítě vypočten požadovaný výsledek. Tím může být například zařazení vzorku do skupiny.

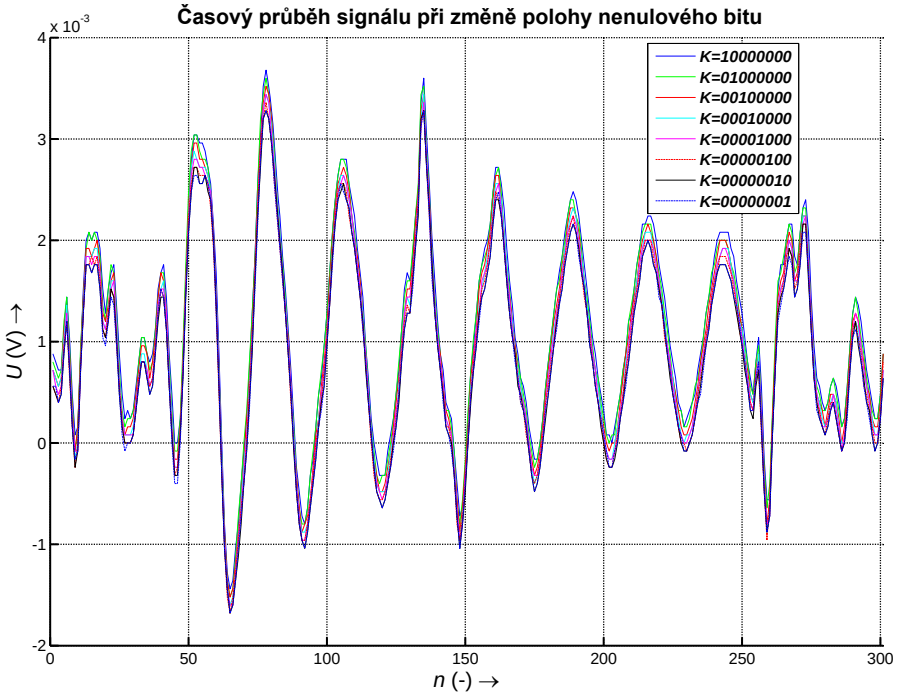
V tomto konkrétním případě jde o určení podobnosti průběhů signálu ze sondy. Použitá síť má topologii 762–50–762×počet vzorů. Počet neuronů ve vstupní vrstvě odpovídá počtu hodnot v průběhu, výstupní vrstva obsahuje násobek této hodnoty v závislosti na počtu předložených vzorů, neboť výstup sítě je počítán atypicky a to pro každou hodnotu průběhu zvlášť, tím je pak možné přesněji určit míru podobnosti vzorku a vzoru. Skrytá vrstva obsahuje takový počet neuronů, aby výstup byl dostatečně přesný a chyba sítě během učení klesala co nejrychleji. Počet neuronů ve skryté vrstvě ovlivňuje také náročnost výpočtu a tím celkovou dobu učení sítě.

Z praktického testování vlivu skryté vrstvy lze odvodit, že pro malé počty vzorů je výhodné použít menší počet neuronů a menší počet iteračních cyklů, např. pro 3 vzory a 10 neuronů ve skryté vrstvě dojde k naučení sítě asi po 150 iteracích, přičemž všech 400 iterací trvá zhruba 5 s, při změně na 100 neuronů ve skryté vrstvě se zvýší doba zpracování 400 iterací na zhruba 38 sekund a síť není naučená. Pro optimální konfiguraci skryté vrstvy je tedy nutné ověřit dobu učení sítě a chybu sítě pro každý konkrétní případ a nastavit adekvátně k počtu neuronů také počet iterací.

Výstupem sítě je vektor indexů podobností v pořadí odpovídajícím vzorům. Pro každý vzor je pak vypočtena průměrná hodnota, která udává celkový index podobnosti pro daný vzor. Index podobnosti lze interpretovat jako hodnotu určující míru podobnosti vzorku s naučenými vzory, rozmezí hodnot je 0 až 1 s možnou odchylkou mimo tento rozsah. V oboru kladných čísel lze index podobnosti považovat za procentuální hodnotu [17].

5.2 Závislost průběhu na poloze nenulového bitu

Oblast užitečného signálu sondy uvedená v kapitole 4.1.2 byla sledována pro všech 8 možných poloh nenulového bitu v bajtu, postupně od první do osmé pozice. U všech průběhů je možné sledovat velmi malé změny ve tvaru a také postupné snižování úrovně signálu o velmi malou hodnotu. Všechny průběhy jsou znázorněny na obrázku 5.3, detail průběhů je uveden na obrázku 5.4.

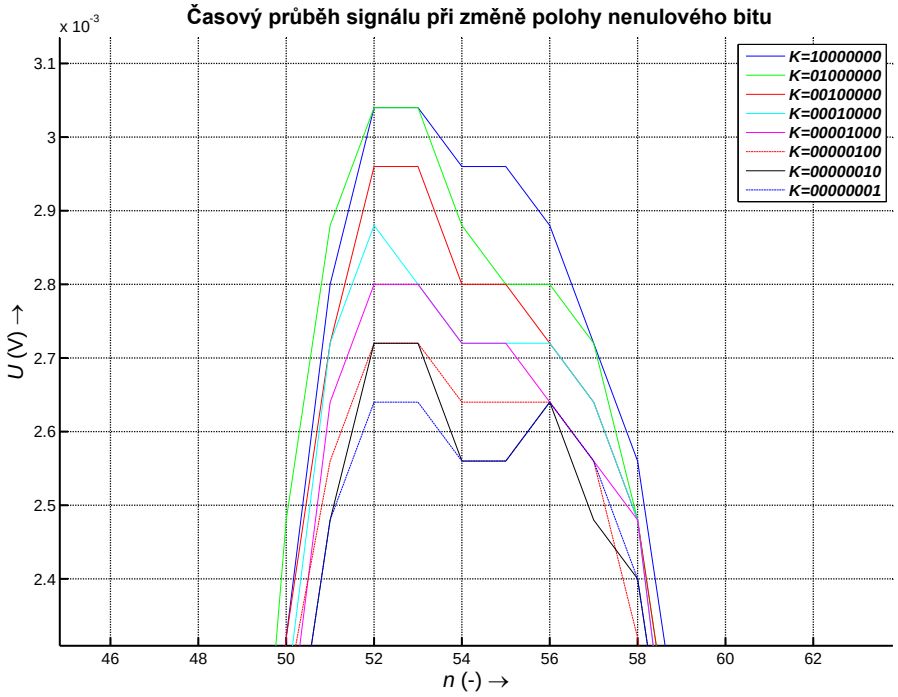


Obr. 5.3: Průběhy signálu ze sondy pro různé polohy nenulového bitu.

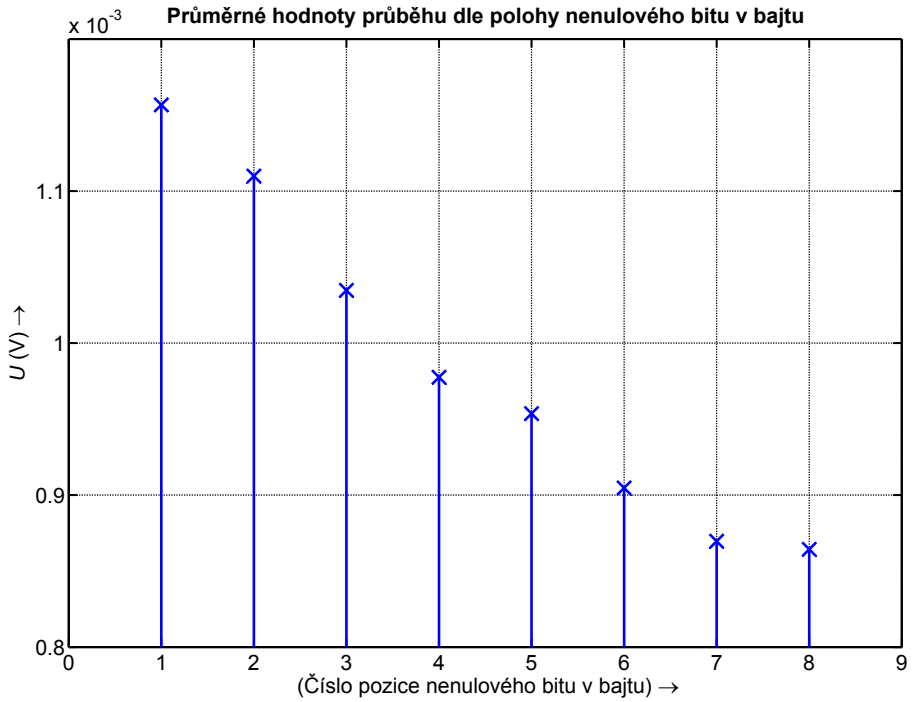
Porovnání změn signálů bylo provedeno pomocí výpočtu průměrné hodnoty jednotlivých vzorků signálu v prostředí Matlab. Rozdíl mezi vypočtenými hodnotami zavisí na stejnosměrné složce zpracovávaného signálu. Sestavením vypočtených hodnot do grafu je možné sledovat změnu úrovně signálu v závislosti na poloze nenulového bitu v bajtu. Graficky je tato závislost znázorněna na obrázku 5.5.

5.3 Závislost průběhu na hodnotě klíče

Celý postup zpracování naměřených hodnot pro zjištění přímého vztahu mezi průběhem signálu sondy a šifrovacím klíčem je koncipován jako hlavní skript s voláním funkcí v prostředí Matlab. První důležitou funkcí je příprava hodnot pro zpracování,



Obr. 5.4: Průběhy signálu ze sondy pro různé polohy nenulového bitu - detail.

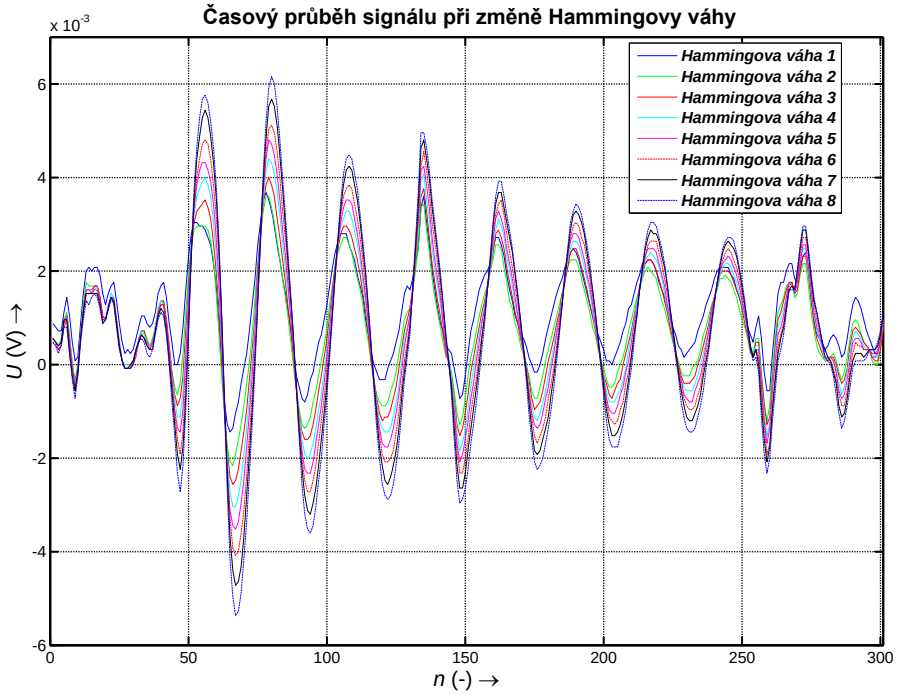


Obr. 5.5: Závislost průměrné hodnoty průběhu na poloze nenulového bitu v bajtu.

což je načtení hodnot z CSV souborů a extrakce užitečné části signálu s následným uložením do MAT souborů, jak již bylo uvedeno v kapitole 4.2.

V hlavním skriptu `main.m` je tato funkce volána následovně: `predzpracovani_dat(adresar_dat, adresar_vzoru)`, parametry funkce určují adresář, ve kterém jsou uloženy CSV soubory a adresář, kam mají být uloženy výsledné zpracované MAT soubory.

Porovnáním hodnot s různým počtem nenulových bitů v bajtu, tedy s různou Hammingovou váhou, byla zjištěna změna velikosti napětí v závislosti na počtu nenulových bitů v bajtu. Grafické znázornění průběhů pro jednotlivé Hammingovy váhy je uvedeno na obrázku 5.6.

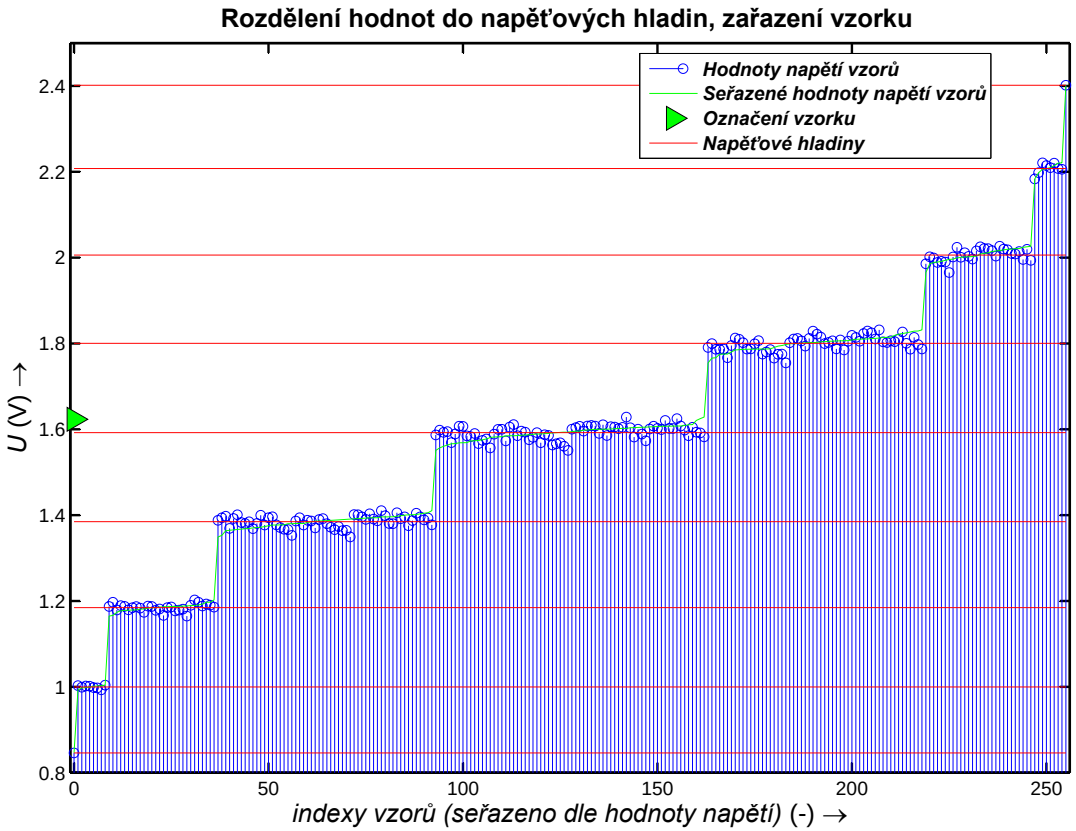


Obr. 5.6: Časový průběh signálu při změně Hammingovy váhy.

Funkce `vypocet_napetovych_hladin` zajišťuje výpočet sumy absolutních hodnot vzorku, jejíž pomocí je určena napěťová hladina a tím i Hammingova váha. Všechny hodnoty průběhu jsou převedeny na absolutní hodnotu a následně sečteny. Tímto výpočtem jsou zohledněny i velmi malé rozdíly mezi průběhy a vzniká tak jediná číselná hodnota vypovídající o důležitých rysech průběhu. Suma hodnot byla zvolena namísto průměrné hodnoty z důvodu zvýšení řádu pro určování napěťových hladin, které jsou odvozeny od změny velikosti napětí v závislosti na Hammingově váze.

Výstupem této části skriptu je graf uvedený na obrázku 5.7. Grafické znázornění

a zařazení je uvedeno pro vzorek s dekadickou hodnotou klíče 210, binárně 11010010, který byl použit z druhé sady průběhů.



Obr. 5.7: Rozdělení hodnot do napěťových hladin, zařazení vzorku.

Grafické zobrazení napěťových hladin a zařazení vzorku do dané napěťové hladiny je doprovázeno textovým výstupem v příkazovém okně Matlabu:

```
Průměrná suma absolutních hodnot napětí zadaného vzorku je: 1.6234 V
Výpočet průměrných napěťových hladin dle počtu nenulových bitů v bajtu
Vzorek náleží do 4. napěťové hladiny
Počet nenulových bitů ve vzorku: 4
```

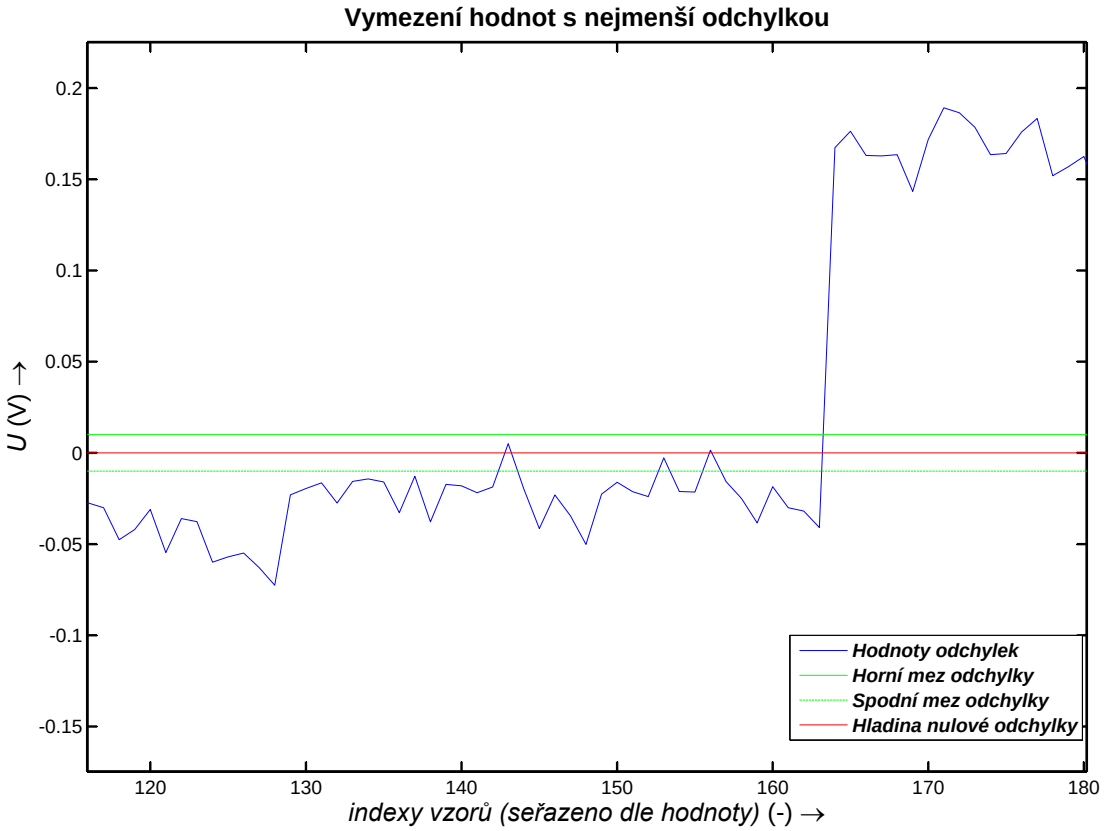
Vypočtená hodnota sumy absolutních hodnot vzorku je porovnána funkcí `klasifikace_sum` se sumami absolutních hodnot průběhů ze vzorové sady. Porovnáním je určena množina vzorů, jejichž sumy absolutních hodnot nejsou od hodnoty vzorku odchýleny o více než 0,01V. Touto selekcí je dán i fakt, že výstupní množina pravděpodobných vzorů obsahuje pro různé vzorky různé počty hodnot v závislosti na tom, kolik hodnot splňuje danou podmínku.

Graficky je výběr hodnot s danou maximální odchylkou znázorněn na obrázku 5.8. V příkazovém okně Matlabu je výstupem funkce následující výpis:

```
Výpočet skupiny pravděpodobných hodnot k zadanému vzorku

indexy_vzoru =
210 202 170

pocet_vzoru =
3
```



Obr. 5.8: Vymezení hodnot s nejmenší odchylkou.

Vybraná množina průběhů je následně využita pro rozpoznání tvarové podobnosti pomocí neuronové sítě. Rozpoznávání tvarové podobnosti uvedených vzorů se zadaným vzorkem zajišťuje funkce `klasifikace_tvar`. Tato funkce zajišťuje naučení neuronové sítě na vybrané vzory a následné určení indexu pravděpodobnosti vzhledem k zadanému vzorku.

Příkaz `nn = mlp(762, 50, (pocet_vzorku*762), 'linear')` zajišťuje vytvoření neuronové sítě s 50 neurony ve skryté vrstvě, příkaz `options(14) = 400;` určuje počet iteračních cyklů při učení sítě. Oba tyto parametry mají rozhodující vliv na funkci rozpoznávání a je třeba je nastavovat individuálně pro každý rozpoznávaný vzorek. Vliv nastavení těchto parametrů je blíže popsán v kapitole 5.1. Příkaz `options(1) = 1;` aktivuje výpis chyby během učení, tím je možné kontrolovat správnost nastavení výše uvedených parametrů. Výstupem skriptu v příkazovém okně Matlabu je výpis:

```
Rozpoznávání dat

vysledek =
0.439989345918218 0.329113058730403 0.229599595148610

indexy_vzoru =
170 210 202
```

Z výše uvedeného výpisu je možné určit zhruba 34% podobnost zadaného vzorku se vzorem pro hodnotu klíče 210 a 43% podobnost se vzorem pro hodnotu klíče 170. Nejvyšší index podobnosti je určen u nesprávného vzoru, což je způsobeno velkou podobností všech průběhů, chybou měření tak dochází ke stavům, kdy jsou jako shodné označeny nesprávné průběhy. Při výpočtu sumy absolutní hodnoty byla provedena základní kompenzace rozdílu stejnosměrné složky mezi sadami, u rozpoznávání tvarové podobnosti nebyla tato skutečnost nijak kompenzována, proto je u této funkce vyšší pravděpodobnost výskytu chyb.

5.4 Shrnutí výsledků měření

Výsledkem laboratorního měření je určení oblasti signálu, ve které je možné pozorovat změny průběhu signálu závislé na poloze nenulového bitu v bajtu. Provedením série měření a jejich zpracování v prostředí Matlab byla zjištěna konkrétní souvislost mezi polohou nenulového bitu a průběhem magneto-motorického napětí.

Provedením dalších měření byly vytvořeny sady vzorů průběhů magneto-motorického napětí pro všechny hodnoty klíče bajtu. S využitím sady vzorů byl sestaven algoritmus, jehož výstupem jsou dva vektory určující nejpravděpodobnější hodnoty klíče pro předloženený vzorek, který obsahuje průběh signálu sondy. První vektor hodnot je sestaven na základě napěťových hladin, druhý na základě tvarové podobnosti průběhů.

Pro náhodně vybrané vzorky jsou níže uvedeny vektory pravděpodobných hodnot klíče určené algoritmem:

Pro vzorek 210
```
210 202 170
170 210 202
```

Pro vzorek 52
```
98 88 49 176 76 70 38 14 44 224 28 50 52 97 84 161 152 35 25 104 100 22
52 28 88 38 44 104 97 49 76 98 100 22 161 50 70 176 25 35 84 14 224 152
```

Pro vzorek 125
```
63 119 125 123 252 249 190
123 63 119 125 190 249 252
```

Pro vzorek 33
```
160 129 9 136 144 33 10 34 3 18 66 192 65 5 17 132 20 40 80
33 66 18 9 10 34 3 20 65 129 5 40 160 136 17 80 132 144 192
```

Pro zvolené vzorky vykazoval algoritmus poměrně dobré výsledky, v obou metodách klasifikace byl odhadnut správný šifrovací klíč. Počet odhadnutých klíčů byl závislý na nastavených mezích odchylky, kterou se zužuje nebo rozšiřuje výběr hodnot dle předpokládané chyby měření. Jak je patrné z vektorů, pro některé hodnoty jsou meze odchylky poměrně úzké, pro některé naopak široké, tato skutečnost je ovlivněna také tím, že vzory byly děleny dle Hammingovy váhy, čímž je také ovlivněn počet hodnot ve vektorech, neboť některé skupiny obsahovaly výrazně větší množství vzorů.

Získaná množina možných klíčů umožňuje provedení útoku hrubou silou na algoritmus AES a snižuje počet možností na řešitelnou úroveň dnes dostupnými technologiemi. Jelikož se ovšem jednalo o experimentální měření, je nutné zohlednit i problémy reálné aplikace, zejména synchronizací průběhů a nastavováním polohy sondy při útoku.

6 OBRANA PROTI ÚTOKU POSTRANNÍM KANÁLEM

6.1 Obecné principy obrany

Útoky postranními kanály jsou založeny na analýze fyzikálních projevů kryptografického modulu při jeho činnosti. Různé principy konkrétních útoků uvádí kapitola 2.3. Z podstaty fungování kryptografického modulu je však zřejmé, že omezit samotné fyzikální projevy je v mnoha případech obtížné, často nemožné. Obranu pak lze rozdělit na následující možnosti:

- softwarová úprava algoritmu,
- odstínění nežádoucích emisí,
- úplné zabránění přístupu útočníka.

6.1.1 Softwarová úprava algoritmu

Softwarovou úpravou algoritmu např. sjednocením doby vykonávání jednotlivých operací, doplněním maskovacích operací, případně úpravou výpočtu nebo generováním akustických signálů lze s relativně nejnižšími náklady ztížit nebo zcela zabránit aplikaci některých útoků postranními kanály.

Sjednocením doby vykonávání jednotlivých operací lze zabránit využití časového postranního kanálu, v případě aditivních maskovacích operací lze ztížit aplikaci elektromagnetického postranního kanálu. Doplněním generování akustického signálu při stisku tlačítka nebo klávesy lze zabránit útoku akustickým postranním kanálem. Vhodnou úpravou chybových hlášení lze omezit útoky vedené prostřednictvím chybového postranního kanálu.

Softwarové úpravy algoritmu patří k nejjednodušším možným opatřením a jsou proto vhodné pouze pro omezení velmi jednoduchých útoků nebo jako doplňková obrana proti útokům složitějším.

6.1.2 Odstínění nežádoucích emisí

V případě útoků emisními postranními kanály je jako obranu možné použít stínění daných emisí. Vhodnými stínícími kryty je možné omezit emisi světla, tepla a elektromagnetického záření do okolí kryptografického modulu a tím využití postranních kanálů značně omezit nebo zcela vyloučit.

6.1.3 Úplné zabránění přístupu útočníka

Nejspolehlivější obranou je úplně zabránění přístupu útočníka do blízkosti kryptografického modulu, to lze provést umístěním kryptografického modulu do zabezpečených prostor, případně umístěním v nepřístupné poloze. Zabráněním útočníkovi v přístupu k zařízení však stále zůstávají další možnosti útoků např. využitím přívodních vedení a je proto nutné provést další opatření.

6.2 Obrana proti útoku elektromagnetickým postranním kanálem

Elektromagnetický postranní kanál spadá do skupiny útoků vedených analýzou emise. Jelikož vznik elektromagnetického pole je vázán na konkrétní operace modulu, je možné využít softwarovou úpravu algoritmu a mezi operace algoritmu vložit maskovací operace, které ovlivní elektromagnetické pole v okolí modulu. Taktéž je možné využít složitější matematické metody vedoucí ke stejným výsledkům s více kroky, čímž se opět změní elektromagnetické pole v okolí modulu.

Z úvodního měření uvedeného v kapitole 4.1 vyplynuly další aspekty ovlivňující možnosti provedení útoku. Jedná se zejména o nutnost přiblížení sondy na co nejmenší vzdálenost k mikrokontroléru. Znemožněním takto blízkého přístupu pevným krytem je útok omezen pouze na měření napájecích vodičů, u kterých však může být elektromagnetické pole značně ovlivněno dalšími prvky obvodu. Ideálním řešením je pak uzemněný vodivý kryt, který odstíní vzniklé elektromagnetické pole. Při předpokladu přístupu útočníka přímo k zařízení a možnosti poškození krytu za účelem měření je pak vhodné dodržet malou vzdálenost mezi mikrokontrolérem a taktovacím krystalem. Krystal produkuje taktovací pulzy, které ovlivňují elektromagnetické pole v okolí mikrokontroléru a tím působí jako rušivý element elektromagnetické analýzy.

7 ZÁVĚR

Cílem práce bylo prostudování možností využití elektromagnetické analýzy, seznámení se s pracovištěm elektromagnetické analýzy na Ústavu telekomunikací Vysokého učení technického v Brně a provedení série měření podložených výsledky simulací. Úvod do teorie kryptografie obsahuje kapitola 1, která popisuje základní pojmy a definice dané oblasti. Konkrétní možnosti útoků na kryptografické moduly uvádí kapitola 2.3, ve které jsou popsány základní principy útoků a útoky využitím postranních kanálů, mezi které patří i elektromagnetická analýza.

Samotné elektromagnetické analýze je podrobněji věnována kapitola 3, ve které jsou uvedeny základní pojmy z dané oblasti. Dále je uveden princip vzniku elektromagnetického pole a princip jeho snímání a vyhodnocování pomocí sondy jeho magnetické složky. V této kapitole je také popsána konkrétní konstrukce sondy a pracoviště elektromagnetické analýzy na Ústavu telekomunikací Vysokého učení technického v Brně. V kapitole je popsán také postup přípravy laboratorního měření, je uveden popis a důležité vlastnosti použitého mikrokontroléru PIC 16F84A. Stručně je zmíněna příprava jednoduchého zdrojového kódu simulujícího část šifrovacího algoritmu AES, jehož princip je také zmíněn. V této kapitole jsou uvedeny výsledky simulací chování logických invertorů, které jsou základním stavebním prvkem CMOS zařízení.

Praktické laboratorní měření je popsáno v kapitole 4, která uvádí postupy měření, zpracování hodnot a zaměřuje se na užitečnou část změřeného signálu. Po zjištění konkrétní oblasti, ve které je možné pozorovat souvislost mezi polohou nenulového bitu v bajtu šifrovacího klíče, byla provedena série měření, jejímž výsledkem je sestavení grafické závislosti, která zachycuje vliv pozice nenulového bitu v bajtu na velikost průměrné hodnoty měřené oblasti signálu. Naměřené hodnoty odpovídají teoretickým předpokladům o vzniku elektromagnetického pole a odpovídají také hrubému odhadu velikosti indukovaného magneto-motorického napětí sondy. Další provedená měření zahrnovala všechny hodnoty šifrovacího klíče v bajtu.

Zpracování naměřených hodnot zahrnovalo vytvoření demonstračních skriptů v prostředí Matlab, které provádějí porovnání hodnot a na základě napěťové hladiny vzorku a tvaru průběhu odhadují možnou hodnotu šifrovacího klíče v bajtu. Jelikož nebylo možné otestovat funkci pro celý rozsah hodnot z důvodu časové náročnosti učení neuronové sítě, bylo náhodně vybráno několik vzorků u nichž proběhla analýza. Výstupní vektory omezují počet hodnot použitelných pro útok hrubou silou na rozsah 1 až 15 hodnot. U vzorků uvedených v kapitole 5.4 jsou však výsledky výrazně lepší. S ohledem na chyby měření a možné abnormální odchylky průběhu je pravděpodobné, že pro některé vzorky nebude možné pomocí skriptu odhadnout hodnotu klíče. Během kontrolního testování 20 různých vzorků byly nalezeny 2 vzorky, u kte-

rých odhad klíče nebyl správný. Teoreticky tak lze přepodkládat v celém rozsahu úspěšnost zhruba 90%. Zdrojové kódy, naměřené hodnoty a skripty pro zpracování jsou uvedeny v elektronické příloze.

Kapitola 6 rozebírá základní možnosti omezení aplikace postranních kanálů, uvádí základní možnosti obrany proti útokům a příklady jejich realizací. Součástí kapitoly jsou také poznatky získané při prováděných měřeních, které je možné využít pro omezení útoku elektromagnetickým postranním kanálem.

LITERATURA

[1] PINKAVA, J. *Úvod do kryptologie* [online]. Odborný článek, květen 1998 [cit. 10. 11. 2011]. Dostupné z URL: <http://cryptoworld.info/pinkava/uvod/uvod98.pdf>.

[2] KŘÍŽ, J. *Postranní kanály v kryptografii*. Bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2007, 57 str., vedoucí bakalářské práce Ing. Petr Daněček.

[3] KOCHER, P., JAFFE, J., JUN, B. *Introduction to Differential Power Analysis and Related Attacks* [online]. San Francisco, 1998. [cit. 16. 11. 2011] Dostupné z URL: <http://www.cryptography.com/resources/whitepapers/DPATechInfo.pdf>.

[4] KOCHER, Paul C. *Timing Attacks on Implementations of Diffie - Hellman, RSA, DSS, and Other Systems* [online]. San Francisco, USA : [s.n.], [1996] [cit. 15. 11. 2011]. Dostupné z URL: <http://www.cryptography.com/public/pdf/TimingAttacks.pdf>.

[5] MACHŮ, P. *Nové postranní kanály v kryptografii* Diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2011. 63 s. Vedoucí diplomové práce Ing. Zdeněk Martinásek.

[6] HLAVÁČ, M. FERRIGNO, J. *When AES blinks: introducing optical side channel*. In *IET Information Security*, 1st edition. [s.l.] : [s.n.], 2008. s. 5.

[7] KOLOFÍK, J. *Optický postranní kanál*. Bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2010. 51 s. Vedoucí bakalářské práce Ing. Zdeněk Martinásek.

[8] DANĚČEK, P., BŘEZINA, M. *Útok výkonovým postranním kanálem na hardwarový kryptografický modul* Elektrorevue [online]. 14.8.2006, 2006, 31, [cit. 11. 11. 2011] Dostupné z URL: <http://www.elektrorevue.cz/clanky/06031/index.html#DPA>.

[9] NEČAS, O. *Útok elektromagnetickým postranním kanálem*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2011. 84 s. Vedoucí diplomové práce Ing. Peter Stančík.

[10] PEETERS, Eric; STANDAERT, Francoi-Xavier; QUISQUATER, Jena-Jacques *Power and Electromagnetic Analysis: Improved Model, Consequences and Comparisons* [online]. Belgium: [s.n.], 2006 [cit. 15. 11. 2011]. Dostupné z URL:

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.1619&rep=rep1&type=pdf>.

[11] Agrawal, D., Archambeault, B., Rao, J., Rohatgi, P. *The EM SideChannel(s).* pp. 29-45 (2003) [online]. DOI, [cit. 15. 11. 2011]. Dostupné z URL: <http://dx.doi.org/10.1007>.

[12] Microchip *PIC16F84A Data Sheet* [online]. [cit. 20. 11. 2011] Dostupné z URL: <http://ww1.microchip.com/downloads/en/devicedoc/35007b.pdf>.

[13] Microchip *PICDEM^{TM} 2 Plus Demonstration Board Usersś Guide* [online]. 2006, [cit. 20. 11. 2011] Dostupné z URL: <http://ww1.microchip.com/downloads/en/DeviceDoc/PICDEM_2_Plus_Users_Guide_51275c.pdf>.

[14] DEUTSCHMANN, Bernd; PITSCH, Harald; LANGER, Gunter *Near Field Measurements to Predict the Electromagnetic Emission of Integrated Circuits* [online]. [s.l.] : [s.n.], [2007] [cit. 20. 11. 2011] Dostupné z URL: <http://www.langeremv.de/fileadmin/website/dokumente/fachbibliothek/en_NFMEmission-Integrated-Circuits.pdf>.

[15] JOAN, Daemen; VINCENT, Rijmen *AES Proposal: Rijndael* [online]. 1997, [cit. 22. 11. 2011] Dostupné z URL: <http://www.nist.gov/CryptoToolkit>.

[16] Federal Information Processing Standards Publication 197 *ADVANCED ENCRYPTION STANDARD (AES)* [online]. 26.11.2001, 1, [cit. 22. 11. 2011] Dostupné z URL: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

[17] Bishop C. M., Nabney I. T. *NETLAB Online Reference Documentation*, [online]. 1997 [cit. 20. 4. 2012], dostupné z URL: <http://www1.aston.ac.uk/EasySiteWeb/GatewayLink.aspx?alId=40589>.

[18] KOUDELKA, V. *Neuronové sítě pro modelování EMC malých letadel.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 53s. Vedoucí diplomové práce prof. Dr. Ing. Zbyněk Raida.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

E energie

h Planckova konstanta

f frekvence

$\vec{B}$ magnetická indukce

μ permeabilita

I elektrický proud

$\vec{dl}$ vektor délky diferenčního elementu

$\hat{r}$ vzdálenost mezi zdrojem el. mag. záření a místem jeho měření

U_{emf} magneto-motorické napětí

N počet závitů vodiče magnetické sondy

$d\Phi$ změna magnetického toku

dt doba trvání

Nr počet rund (opakování)

+Ucc napájecí napětí

GND ground

CMOS Complementary Metal Oxide Semiconductor

MOSFET Metal Oxide Semiconductor Field Effect Transistor

AES Advanced Encryption Standard

SEZNAM PŘÍLOH

A OBSAH PŘILOŽENÉHO DVD

- dp.pdf – elektronická verze práce
- adresář `poloha_pocet_bitu` obsahuje naměřené průběhy a skripty pro zjištění souvislostí mezi průběhy a polohou nebo počtem nenulových bitů v bajtu:
  - porovnani_pocet.m – skript pro porovnání průběhů dle Hammingovy váhy,
  - porovnani_poloha.m – skript pro porovnání průběhů dle polohy nenulového bitu,
  - csv_import.m – skript pro načítání CSV souborů,
  - popis_namerenych_hodnot.txt – popis k naměřeným průběhům,
  - ALL0002.csv až ALL0016.csv – soubory s naměřenými průběhy.
- adresář `prubeh_klic` obsahuje naměřené hodnoty pro zjištění souvislotí mezi průběhy a hodnotou šifrovacího klíče:
  - main.m – hlavní soubor pro spouštění algoritmu odhadu klíče,
  - offset.m – pomocý skript pro korekci offsetu,
  - predzpracovani_dat.m – skript pro úpravu signálu a vytvoření sad vzorů,
  - vypocet_napetovych_hladin.m – skript pro výpočet napěťových hladin a zařazení vzorku,
  - klasifikace_sum.m – skript pro odhad hodnoty klíče dle hosnoty sumy absolutních hodnot průběhu,
  - klasifikace_tvar.m – skript pro odhad hodnoty klíče dle tvarové podobnosti průběhů,
  - csv_import.m – skript pro načítání CSV souborů,
  - adresář NETLAB – toolbox pro práci s neuronovou sítí,
  - adresáře osc1 a osc2 (pouze na DVD) - adresáře s CSV soubory naměřených průběhů,
  - adresáře data1 a data2 - adresáře s upravenými průběhy, pouze užitečná část pro analýzu,
  - popis.txt – stručný popis pro spuštění hlavního skriptu a jeho nastavení.
- adresář `zdrojovy_kod_add` obsahuje zdrojový kód pro mikrokotrolér PIC16F84A:
  - AddRoundKey.txt – výpis zdrojového kódu pro mikrokontrolér PIC16F84A.