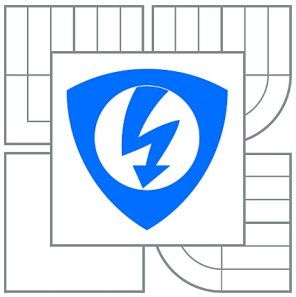
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

ÚTOK ELEKTROMAGNETICKÝM POSTRANNÍM KANÁLEM

ELECTROMAGNETIC SIDE CHANNEL ATTACK

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

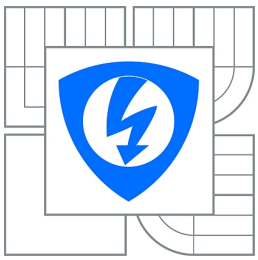
AUTOR PRÁCE — Bc. ONDŘEJ NEČAS

AUTHOR

VEDOUCÍ PRÁCE — Ing. PETER STANČÍK

SUPERVISOR

BRNO 2011



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Ondřej Nečas	***ID:***	72869
Ročník:	2	***Akademický rok:***	2010/2011

NÁZEV TÉMATU:

Útok elektromagnetickým postranním kanálem

POKYNY PRO VYPRACOVÁNÍ:

V diplomové práci navrhněte a sestavte pracoviště pro měření nežádoucího úniku elektromagnetického záření z mikročipu PIC. Navrhněte a zhotovte potřebnou sondu, otestujte její vlastnosti. Prozkoumejte vliv odstranění pouzdra čipu na úroveň vyzařování. Vyberte a použijte vhodnou metodu pro analýzu rozdílů v naměřených hodnotách pro různé instrukce. Zjistěte do jaké míry je realizovatelná analýza chování čipu při provádění algoritmu (DES, AES). Navrhněte případná protiopatření.

DOPORUČENÁ LITERATURA:

[1] Paul C. Kocher: Timing Attacks on Implementations of Diffe-Hellman, RSA, DSS, and Other Systems, Advances in Cryptology-Crypto 96, Lecture Notes in Computer Science # 1109, pp 104-113.
[2] Micheal Tunstall: Attacks on smartcards, Smart Card Lecture Notes, Royal Holloway Information Security Group, 2005.
[3] Thomas S. Messerges Ezzy A. Dabish and Robert H. Sloan: Investigations of Power Analysis Attacks on Smartcards, In Proc. of the usenixWorkshop on Smartcard Technology (Smartcard'99). usenix Association, 1999.

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

Vedoucí práce: Ing. Peter Stančík

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

UPOZORNĚNÍ:

Autor diplomové práce nesmí při vytváření diplomové práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ABSTRAKT

Cílem této práce je navrhnou a sestavit měřicí pracoviště pro zkoumání elektromagnetického postranního kanálu v kryptografii. A dále pak seznámit čtenáře se základními způsoby útoků elektromagnetickými a výkonovými postranními kanály, které představují efektivní způsob kryptoanalýzy moderních kryptosystémů.

V teoretické části práce jsou uvedeny základní útoky postranními kanály, včetně jejich historie a modelů, z nichž vychází. Stěžejní část práce se věnuje vysvětlení základních principů útoků výkonovými a elektromagnetickými postranními kanály. Následně jsou v práci popsány fyzikální principy vzniku elektromagnetického pole a jsou zároveň popsány i metody, kterými lze vzniklé pole měřit. Uveden je rovněž příklad vzniku elektromagnetického pole u mikroprocesorů. V další části této práce jsou uvedeny teoretické základy potřebné pro úspěšnou realizací měření elektromagnetického pole mikroprocesorů PIC. Další část kapitoly je věnována šifrovacímu standardu AES, jehož činnost je zkoumána v praktické části. Dále jsou v této práci popsány parametry sond, které byly sestrojeny podle teoretických znalostí. V této kapitole je rovněž popsáno navržené měřicí pracoviště. A jsou zde zároveň uvedeny jednotlivé přístroje, používané v praktické části práce.

V praktické části jsou popsány realizační aspekty, které mají za cíl dosažení ideálních podmínek měření jako je například volba vhodné sondy, zajištění vhodné polohy a vzdálenosti sondy od měřeného zařízení a v neposlední řadě správné nastavení osciloskopu a synchronizačního signálu. Dále jsou v práci zobrazeny naměřené elektromagnetické průběhy pro vybrané instrukce. Následuje analýza jednotlivých rund šifrovacího standardu AES i jeho analýza jako celku. Posléze jsou ještě provedeny metody jednoduché a diferenciální elektromagnetické analýzy.

Na základě poznatků získaných v praktické části práce jsou popsány možná protiopatření, zaváděná proti útokům výkonovým a elektromagnetickým postranním kanálem. V závěru je provedeno stručné zhodnocení výsledků práce.

KLÍČOVÁ SLOVA

Postranní kanály
Mikroprocesor
Elektromagnetická a výkonová analýza
AES
Kryptografie

ABSTRACT

The aim of this thesis is, firstly, to design and create the measuring environment for the research of electromagnetic side-channel attacks in cryptography; and secondly, to inform readers about the basics of electromagnetic and power side-channel attacks which present effective ways of the modern cryptosystems' cryptoanalysis.

In the theoretical part, the basic side-channel attacks, including their history and models, are described. The main part is focused on the explanation of the basic principles of power and electromagnetic side-channel attacks. Then, the work describes the basic physical principles of electromagnetic fields; and also the methods which can be used to measure the electromagnetic field. An example of the origination of the electromagnetic field in microprocessors is included. In the next part of the work the theoretical foundation necessary for successful implementation of the measurement of electromagnetic fields on the PIC microprocessor is presented. Next part of the chapter is devoted to the AES encryption standard, the activity of which is examined in the practical part. Furthermore, the magnetic probes, designed according to the theoretical knowledge are described. Also the research environment is described in this chapter. The list of measuring instruments used in the practical part is also included.

The practical part of the work deals with the implementation aspects designed to achieve the ideal measurement conditions, such as the choice of appropriate probe, the appropriate location and distance between the probe and the measured system, setup of the oscilloscope and signal synchronization. Furthermore, the measured electromagnetic waveforms for selected instructions are presented. After that follows an analysis of the individual rounds of the AES encryption standard; the analysis of whole AES standard is also included. Then, the methods of simple and differential electromagnetic analysis are implemented.

With regard to the knowledge gained in the practical part of the work, the possible countermeasures implemented against the power and electromagnetic side channel attacks are described. The final part of the work comprises a brief review of results.

KEYWORDS

Side Channels
Microprocessor
Electromagnetic and Power Analysis
AES
Cryptography

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.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma Útok elektromagnetickým postranním kanálem jsem vypracoval samostatně pod vedením Ing. Petera Stančíka 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.“

V Brně dne 26.5.2011 ……..

PODĚKOVÁNÍ

Děkuji vedoucímu diplomové práce Ing. Petru Stančíkovi, za velmi užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce.

Obsah

Seznam obrázků

Seznam tabulek

ÚVOD

Útoky postranními kanály představují relativně novou oblast kryptoanalýzy, která se stále ještě vyvíjí a lze předpokládat, že ještě dlouhou dobu se budou objevovat nové druhy a způsoby zjišťování informace unikající ze systémů zpracovávajích nebo přenášejících informace. Cílem této práce je navrhnout, sestavit a popsat měřicí pracoviště pro měření emise EM pole a dále pak seznámit čtenáře se základními metodami útoku elektromagnetickým a výkonovým postranním kanálem, které jsou v částech měření a vyhodnocení získaných informací a signálů velmi podobné.

Teoretická část se soustředí na vysvětlení základních pojmů a modelů postranních kanálů a jsou zde rovněž vysvětleny možnosti přístupu k zařízení. Zároveň je v této části uveden přehled nejběžnějších útoků postranními kanály. Následně se čtenář seznámí s teorií vzniku a měření elektromagnetického pole a se studií vzniku elektromagnetického pole v okolí mikroprocesorů založených na nejrozšířenější technologii výroby polovodičových součástí – CMOS. Dále jsou v práci popsány základní funkce mikroprocesorů PIC, na kterých bude prováděno praktické měření a také principy šifrovacího standardu AES, jehož implementace bude v praktické části práce zkoumána. Zároveň jsou v této části práce popsány i některé aspekty ovlivňující praktickou část této práce. Následně jsou v práci popsány parametry měřicích sond, vyrobených podle teoretických poznatků, uvedených v teoretické části. Dále byl proveden a popsán návrh měřicího pracoviště pro měření elektromagnetického pole mikroprocesorů PIC, včetně rozpisu jednotlivých částí měřicího pracoviště.

Praktická část této práce je zaměřena především na optimalizaci měřicího pracoviště, s cílem dosažení nejlepších výsledků měření. V této kapitole je provedeno srovnání všech realizovaných měřicích sond. Dále je navázáno studií vlivu vzájemné polohy a vzdálenosti snímací sondy a mikroprocesoru na úroveň indukovaného napětí v měřicí cívce. Dále jsou v této kapitole probrány vhodná nastavení osciloskopu a synchronizačního signálu a zároveň i některé aspekty, na které je potřeba si dát pozor. Následuje porovnání elektromagnetického signálu s výkonovým, a analýza vybraných instrukcí, posléze je prováděna analýza průběhu šifrovacího standardu AES a to jak celkového průběhu, tak jeho jednotlivých částí. Na konci této kapitoly jsou popsány praktické metody jednoduché a diferenciální analýzy na algoritmu AES.

V další části byly na základě poznatků získaných v praktické části měření probrány možnosti ochrany proti útokům elektromagnetickým postranním kanálem a to v podobě možných protiopatření, které se již v některých případech využívají. V závěru jsou shrnuty poznatky a zkušenosti získané v průběhu vypracovávání této práce.

1 POSTRANNÍ KANÁLY V KRYPTOGRAFII

Kryptoanalýza postranními kanály je jedním z nejnovějších oborů aplikované kryptoanalýzy, která nabývá od poloviny 90. let na významu. Výzkum v této oblasti prokázal, že i nechtěný únik některých fyzikálních veličin způsobený implementací matematického zabezpečovacího algoritmu v systému, může být z hlediska bezpečnosti systému rozhodující. Důsledkem takového úniku informace z kryptosystému může být i odhalení tajného klíče jednotlivých implementací. Důvod, proč jsou útoky postranními kanály v současné době velmi efektivní, je velmi prostý. V 90. letech panoval v oblasti zabezpečení dat, s výjimkou několika tajných vojenských projektů, trend vytváření co nejrobustnějších šifrovacích schémat a protokolů. Útoky postranními kanály ale využívají nechráněné oblasti reálného světa. Tedy okolí klávesnic, monitorů, tiskáren a zařízení, která pracují s daty. Velkou výhodou většiny nejmodernějších útoků postranními kanály je, že za sebou nezanechávají žádnou stopu, nenarušují data, soubory ani zařízení, nezpůsobují chyby chování systému a nezůstává po nich žádná hmatatelná stopa a jsou tak v podstatě nedetekovatelné.

V reálné situaci jsou vždy kryptografické algoritmy zpracovávány fyzickými zařízeními, která jsou vždy ovlivněny interakcí s okolním prostředím. Tyto fyzické interakce zařízení se svým okolím mohou být potenciálním útočníkem monitorovány a mohou vést k úspěšnému dešifrování tajných informací. Tento druh informace se nazývá informace postranního kanálu a útoky využívající těchto informací se nazývají útoky postranními kanály – SCA (Side-Channel Attacks). Princip SCA spočívá v tom, že se zaměřuje na způsob, jakým jsou kryptografické algoritmy zpracovávány, spíše než na algoritmus samotný. Konvenční způsoby kryptoanalýzy chápou kryptografické algoritmy jako matematické objekty, kdežto kryptoanalýza postranními kanály uvažuje především nad implementací těchto algoritmů, proto se často SCA útoky nazývají implementačními útoky.

1.1 Historie útoků postranními kanály

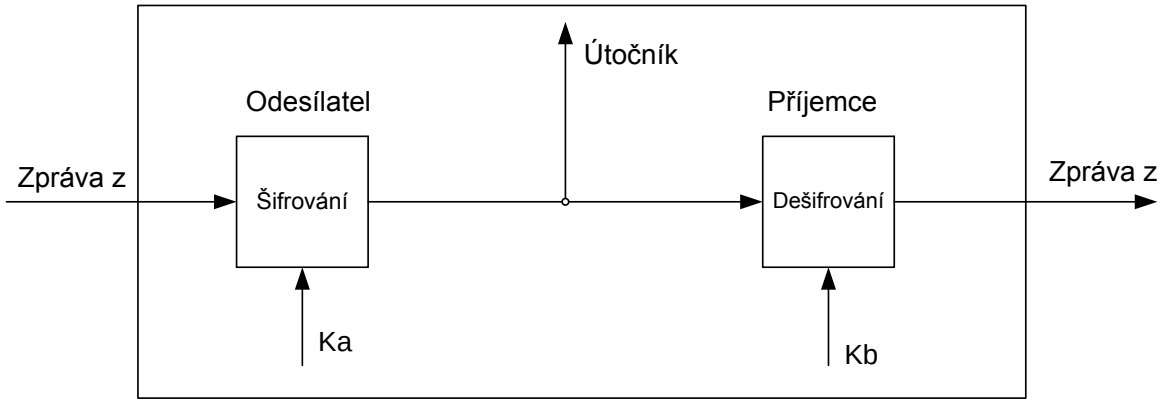
První zmínka vztahující se k SCA se datuje do roku 1965, kdy Britský vědec Peter Wright zjistil, že se Britská tajná služba MI5 snažila prolomit šifru Egyptské ambasády v Londýně. Přičemž jejich pokusy byly zpočátku neúspěšné, především kvůli v té době ještě velmi omezené výpočetní síle jejich strojů. MI5 si tehdy údajně pomohla tak, že umístila mikrofon k rotoru šifrovacího zařízení, které používali Egypťané, aby zjistili zvuk, který přístroj vydává při stisknutí určitých kláves. Odposlechem zvuků, které stroj vydával při resetování rotorů každé ráno, byla MI5 schopna odvodit výchozí pozici dvou ze tří rotorů daného zařízení a tato dodatečná informace snížila výpočetní výkon potřebný k rozluštění šifry. MI5 tak mohla odposlouchávat komunikaci Egyptských velvyslanců dlouhé roky. [1]

Za průkopníka v oblasti SCA je považován především americký kryptograf Paul Carl Kocher, který se zasloužil především o vývoj časové analýzy. Zároveň se spolupodílel na rozvoji výkonové analýzy PA, nemalé zásluhy má i na sestavení zařízení zvaného Deep Crack[1].

1.2 Model útoků postranními kanály

Na kryptografický primitiv lze nahlížet ze dvou úhlů pohledu. Z pohledu klasické kryptografie se na něho nahlíží jako na abstraktní matematický objekt, jehož parametrem je klíč a který podle zadaného parametru přemění určitý vstup na daný výstup. Na druhé straně z pohledu kryptoanalýzy postranními kanály tento primitiv bude muset být implementován v programu, který poběží v zadaném procesoru a v určitém prostředí a bude proto nutně vykazovat určitou charakteristiku chování. Výhodou kryptoanalýzy postranními kanály je, že toto charakteristické chování může v některých případech odhalit některý z tajných parametrů výpočtu.

Při klasické kryptoanalýze se při posuzování bezpečnosti kryptografického protokolu předpokládá, že útočník zná kompletní popis šifrovacího protokolu a veřejné klíče, ale nezná tajné klíče. Mimo to je možné, že útočník může mít zachyceny některé konkrétní části komunikace mezi autorizovanými účastníky (např. některé zprávy při útoku na zachycení konkrétních zpráv podpisového schématu). Poté je cílem útočníka využít těchto znalostí k odhalení tajného klíče výpočtem nebo nalezením nějaké vady v návrhu protokolu.

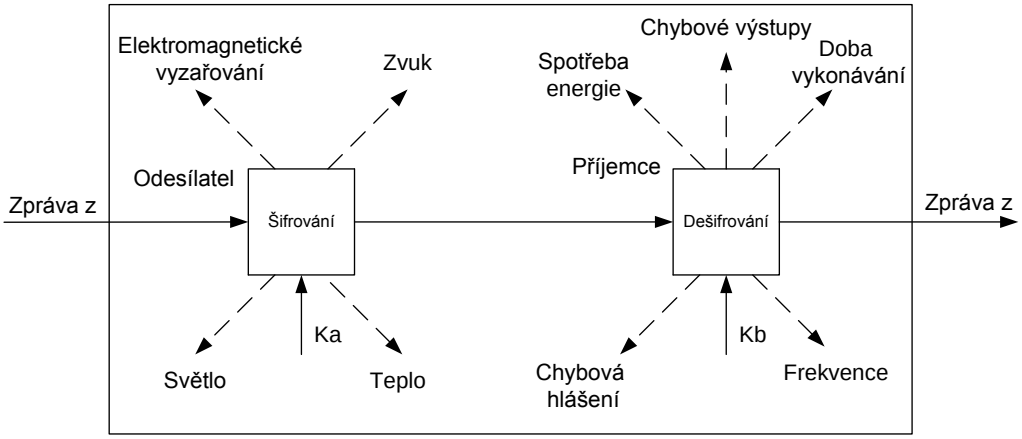


Obr. 1.1: Tradiční kryptografický model.

V případě útoku na tradiční kryptografický model viz obr. 1.1, dochází k napadení matematické specifikace protokolu, popřípadě k útokům hrubou silou, kdy jsou vyzkoušeny všechny kombinace hodnot klíče, kterých může nabývat. SCA se zaměřuje na zachycení a zpracování informací uniklých během zpracovávání protokolu výpočetním systémem a nejsou proto uvažovány v tradičním kryptografickém modelu.

[1] Deep Crack je zařízení navržené k realizaci útoku hrubou silou na klíč DES

Klasickým případem útoku postranními kanály může být měření úrovně vyzářeného elektromagnetického výkonu při zpracovávání výpočetních operací šifrování. Dalším příkladem může být měření doby vykonávání kryptografických operací nebo analyzování chování kryptografického systému při vzniku určitých chyb. Kryptografický model s postranním kanálem je zachycen na obr. 1.2.



Obr. 1.2: Kryptografický model s postranním kanálem.

1.3 Možnosti přístupu k zařízení

Při analyzování bezpečnosti kryptografického zařízení je praktické provést přehled možných útoků. Podle sady různých fyzikálních, elektrických a logických útoků, které mohou na zařízení být prováděny potenciálním útočníkem, jsou tyto útoky rozděleny do tří základních skupin vybraných podle jejich fyzického dopadu na kryptografické zařízení, jedná se o: Invazivní útoky, semi-invazivní útoky a neinvazivní útoky.

1.3.1 Invazivní útoky

Při invazivním fyzickém útoku je potřeba odstranit ochrannou vrstvu a je nutno získat přímý přístup k vnitřním součástkám nebo modulům kryptografického zařízení. Klasickým příkladem invazivních útoků je odstranění pouzdra kryptografického zařízení za účelem získání přístupu k vodivým spojením nebo k datové sběrnici, tento způsob odstranění vnější ochranné vrstvy zařízení se nazývá dekapsulace. Poté většinou následuje přesměrování nebo přerušení vodivých cest v zařízení, které útočníkovi zpřístupní vnitřní zapojení zařízení.

U některých kryptografických zařízení s vyšší úrovni zabezpečení se využívají některé z technik zabraňující invazivním útokům. Nejčastěji se využívají mechanismy s detekcí pokusu o narušení. Ty fungují tak, že při detekci pokusu o průnik k některé

z částí kryptografického zařízení dojde k vynulování pamětí zařízení nebo k přerušení činnosti zařízení a informováním obsluhy o pokusu narušení.

Obecně platí, že invazivní útoky bývají časově náročné a destruktivní. U některých druhů invazivních útoků dochází k fyzickému zničení některých částí systému.

1.3.2 Semi-invazivní útoky

Semi-invazivní útok vyžaduje přístup k zařízení, avšak bez nutnosti zničení ochranné vrstvy nebo vytvoření přímého vodivého kontaktu s vodivými částmi zařízení. Avšak útočník potřebuje získat přímý přístup k zařízení v jeho blízkém okolí nebo alespoň na přímou viditelnost. Jedním ze známých semi-invazivních útoků, kterým lze změnit obvodové řešení zařízení bez destruktivních účinků[2], je využití fokusovaného iontového svazku FIB (Focused Ion Beam) a sítě snímacích sond. Tento způsob však vyžaduje velmi drahé speciální zařízení, což činí tento způsob velmi složitým a náročným. Proto je v současné době prakticky proveditelný pouze na vědecké úrovni.

1.3.3 Neinvazivní útoky

Neinvazivní útoky vyžadují bližší pozorování kryptografického zařízení avšak bez nutnosti fyzického zásahu do zařízení. Tyto útoky využívají informaci z postranního kanálu, která určitým způsobem uniká z pozorovaného zařízení. Největší výhodou neinvazivních útoků je, že jsou nezjistitelné, jelikož nijak nezasahují do běžného chodu zařízení a ani nijak zařízení nepoškodí. Další výhodou je, že neinvazivní útoky lze za určitých podmínek a s různými stupni úspěchu realizovat i s relativně nízkými finančními prostředky a v tomto ohledu tak představují poměrně dosti velkou hrozbu pro některá kryptografická zařízení.

1.4 Nejznámější druhy útoků postranními kanály

SCA proti kryptografickým zařízením využívají charakteristických informací získaných pozorováním chování zařízením při provádění kryptografických operací a protokolů. Tyto informace se získávají pozorováním a to nejčastěji ve formě měření spotřeby energie, elektromagnetického záření, doby zpracování operací nebo vyvoláním hardwarových a softwarových chyb, potažmo změnami frekvence nebo teploty zařízení. SCA tak využívá charakteristických vlastností hardwarových a softwarových prvků kryptografického zařízení stejně jako implementace struktury kryptografických primitiv.

[2] Tento způsob útoku je de facto neinvazivní, jelikož nedochází k trvalému poškození systému, avšak myšlenka změny obvodového řešení systému, vychází z teorie invazivních útoků. Proto je tento způsob na pomezí obou druhů útoků.

Výše uvedené má za následek, že samotná implementace kryptografických protokolů hraje velmi důležitou roli a i pouze malá změna v implementaci může ve výsledku znamenat velký rozdíl ve výsledné bezpečnosti systému. V kryptografii je bezpečnost celého systému závislá na bezpečnosti nejslabšího článku řetězce, právě proto je tento článek nejčastěji napadán útočníky, jelikož právě zde mají nejvyšší šanci uspět. Při pohledu na současné kryptografické algoritmy a protokoly, dojdeme k zjištění, že tyto algoritmy zcela jistě nejsou nejslabším článkem kryptografického řetězce. Do dnešního dne bylo vyzkoumáno několik různých druhů útoků postranním kanálem a tyto útoky budou probrány v následující kapitole. [2]

Časová analýza:

Časová analýza chování kryptografického systému je jedním z prvních realizovaných útoků postranními kanály. Cílem časové analýzy je zjistit tajnou informaci prováděním přesných měření času, který uživatelskému zařízení zabere výpočet určitých kryptografických operací, respektive statistickým prozkoumáním rozdílů doby provádění jednotlivých operací. Toho lze docílit tím, že útočník na vstup programu posílá různá data a měří, jak dlouho trvá jejich zpracování.

První zmínky o časové analýze kryptografických systémů jsou uvedeny v práci Paula C. Kochera – Časová analýza implementace kryptografických protokolů D-H, RSA, DSS a dalších systémů (Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems) [3]. Autor v této práci navrhl způsob, jakým realizovat útok pomocí přesného měření doby zpracovávání operací soukromým klíčem, který vedl k odhalení tajných klíčů jednotlivých protokolů.

Útok byl založen na předpokladu, že šifrovacímu systému trvalo různou dobu zpracovat různá vstupní data. Tyto doby se nejčastěji lišily z důvodů výkonové optimalizace, větvení a různé doby provádění strojových instrukcí apod. Mohlo by se zdát, že informace postranního kanálu, která uniká při časové analýze, poskytuje pouze malé množství informace o kryptosystému. Nicméně opak je pravdou a útoky, které využívají přesného měření času provádění operací některými kryptografickými systémy, mohou vést k odhalení celého tajného klíče. Množství informace potřebné k úspěšné realizaci útoku závisí na mnoha faktorech: Návrhu kryptosystému, návrhu centrální procesorové jednotky, použitých algoritmech, přesnosti měření atd.

Útok zaváděním chyb

Princip útoku zaváděním chyb spočívá v záměrném zavádění chybných vstupních parametrů na vstup zařízení vedoucí k chybným výpočtům při implementaci algoritmu. U většiny zařízení, které vykonávají kryptografické operace platí, že pracují velmi spolehlivě. Proto se předpokládá, že bezpečnost vykonávaných operací závisí na spolehlivosti zařízení, které je provádí. V rozporu s tímto předpokladem je však fakt, že hardwarové chyby, které se projeví v průběhu operace kryptografického zařízení, vážně

ohrožují bezpečnost systému. Toto chybné chování a výstupy pak představují postranní kanály, přes které dochází k úniku informace, a proto velmi snižují bezpečnost použité šifry.

Útoky zaváděním chyb byly světu poprvé představeny autory Danem Bonehem, Richardem A. DeMillem a Richardem J. Liptonem v roce 1997 [4]. Ve své práci přišli s novým druhem útoku, který vychází z předpokladu, že čas od času systém provádějící výpočty může vykazovat chyby. Zároveň představili několik chybových modelů, které umožňují útočníkovi způsobovat chyby systému.

Akustický útok

Tento druh postranních kanálových útoků sice byl, jak již bylo naznačeno v úvodu, dříve využíván k odposlechu mechanických kryptografických zařízení. V současné době jsou výpočetní procesory mnohonásobně rychlejší a tišší, než například různé rotory a relé, proto se v současné době akustických útoků příliš hojně nevyužívá. Nicméně v roce 2004 Adi Shamir předvedl koncept, ve kterém naznačil, že existuje souvislost mezi zvuky vydávanými procesorem a operacemi, které provádí. Toto relativně nové pole ještě vyžaduje hlubší zkoumání. V současné době se také rychle rozvíjí analýza zvuků, a tudíž v blízké budoucnosti nejspíš bude možné odposlechnout zvuky, které například vydává stlačení jednotlivých písmen při psaní na klávesnici a tyto zvuky zpětně vyhodnotit a rekonstruovat tak psaný text.

Útok viditelným světlem

V roce 2002 Markus G. Kuhn ve své práci [5] analyzoval a vyzkoušel experiment, při němž dokázal úspěšně rekonstruovat obraz CRT monitoru. Jeho experimenty dokázaly, že klasický barevný CRT monitor dokáže emitovat vysokofrekvenční záření, v němž zůstává dostatek informace potřebné k úspěšné rekonstrukci čitelného textu pomocí dekonvoluce přijatého signálu v rychlých fotosenzorech. Dále pak dokonce dokázal, že je možné obraz rekonstruovat i pomocí snímání průměrného difusního odrazu záření obrazu CRT monitoru od zdi, což ale platí pouze v dostatečně tmavých prostorách a s dobrou snímací výbavou. Nespornou výhodou tohoto druhu útoku je, že není potřeba fyzického přístupu ke snímanému monitoru a že tento útok je proveditelný i na větší vzdálenost. Zároveň je velmi užitečnou variantou k EM útoku na monitor (jelikož EM útok na monitor lze ztížit přídavným stíněním monitoru, kdežto samotný útok viditelným zářením není stíněním ovlivněn). Později bylo ověřeno, že tento útok je stejnou technikou realizovatelný i na LED displeje.

Útok založený na časové analýze při zápisu do vyrovnávací paměti

Tento druh útoku vychází z klasické časové analýzy systémů. Hlavní rozdíl v obou analýzách je v tom, že klasická časová analýza se prováděla především u starších systémů, které neobsahovaly vyrovnávací paměti.

U moderních výpočetních systémů, jsou velmi často využívány vyrovnávací paměti, a proto je implementován nový druh útoku. Vyrovnávací paměť je dočasná paměť, která umožňuje rychlejší čtení a zápis dat, než hlavní paměť. Tato paměť se nachází mezi výpočetní jednotkou a pomalejšími hlavními paměťmi. Pokud vznikne požadavek na čtení dat z hlavní paměti, hlavní výpočetní jednotka nejprve prohledá vyrovnávací paměť a pokud hledaná data nalezne, načte je z hlavní paměti. Princip samotného útoku pak spočívá v tom, že je měřeno zpoždění a počet chyb, které nastanou, pokud dojde k chybě při přístupu k vyrovnávací paměti (např. když nedojde k nalezení potřebné informace nebo odepření přístupu do paměti), musí se potřebná data načíst do výpočetní jednotky z hlavní paměti. Měření tohoto zpoždění může útočník odhalit četnost výskytu chyb ve vyrovnávací paměti. [6]

Frekvenční útok

Návrh frekvenčních útoků proti mobilním zařízením jako jsou PDA (Personal Digital Assistent – osobní digitální pomocník), pagery a mobilní telefony navrhl ve své práci Chin Chi Tiu v roce 2005 [7]. Zde předkládá návrh tzv. Diferenciální frekvenční analýzy (DFA – Differential Frequency Analysis), která vznikla na základě diferenciální výkonové analýzy. Jeho technika pracuje ve frekvenční oblasti a využívá výpočtu výkonové spektrální hustoty signálu (PSD). Důvodem využití frekvenční oblasti je, že občas dochází k nepřesnému zachycení elektromagnetických nebo výkonových tras, čímž je diferenciální elektromagnetická potažmo i výkonová analýza nerealizovatelná. Výhodou tohoto postranního útoku je, že DFA může být použita v kooperaci jak s EM analýzou (analýza se nazývá Diferenciální Elektromagneticko-Frekvenční Analýza – DEMFA) tak i s výkonovou analýzou (Diferenciální Výkonově-Frekvenční Analýza – DPFA).

Útok zkoumáním řetězce

Útoky zkoumáním řetězce SCB (Scan-Chain Based) jsou jedním z druhů útoků postranními kanály. SCB útok vznikl jako vedlejší produkt návrhového vzoru DFT (Design for Testability). Tento návrhový vzor, který se často využívá v moderních hardwarových zařízeních, přidává určitý stupeň testovatelnosti “sama sebe”. Na druhé straně však tato vlastnost však otevřela postranní kanál pro kryptoanalýzu a vystavila tyto zařízení možnosti SCB útoku. [8]

1.5 Odběrová analýza

V kryptografii je odběrová analýza nebo také výkonová analýza PA (Power Analysis) jedním z nejčastěji využívaných druhů útoků postranními kanály. Odběrová analýza využívá k odhalení informací o prováděných operacích změny výkonové spotřeby kryptografického zařízení v čase. Tento druh útoku je neinvazivní a je použitelný pouze na hardwarové části kryptografických systémů. Je dokázáno, že je

velmi úspěšný v případech útoku na smart karty a některé jednoúčelové systémy. Často se jej využívá právě v kombinaci s elektromagnetickými útoky.

V současnosti je útokům využívající výkonové analýzy v odborných kruzích věnována velká pozornost. Tento druh útoku se ukázal jako velmi efektivní útok na většinu implementací symetrickým veřejným klíčem.

Odběrová analýza se dělí na dvě základní oblasti: jednoduchou výkonovou analýzu SPA (Simple Power Analysis) a diferenciální výkonovou analýzu DPA (Differential Power Analysis).

Cílem SPA je monitorování výkonového odběru kryptografického systému při zpracovávání konkrétních instrukcí v daném čase a sledováním vstupních a výstupních hodnot v odpovídajících časech. Útočník proto k realizaci tohoto útoku potřebuje znát přesné znalosti o implementaci prováděných operací. SPA vychází z předpokladu, že různé operace kódu používají a spínají různý počet tranzistorů. Podle počtu tranzistorů se může lišit výkonový profil prováděné operace. SPA při vyšších rozlišeních umožňuje například identifikovat rozdíly mezi prováděnými operacemi a na základě těchto rozdílů operace jednoznačně identifikovat. Například u šifrování DES, resp. AES jsou patrné rozdíly mezi operacemi permutace a posunu.

SPA využívá především vizuální analýzu pro nalezení výkonových změn. DPA využívá statistickou analýzu získaných informací. Prvním krokem k úspěšné realizaci výkonové analýzy je sběr dat. Nejčastějším způsobem sběru dat je vzorkování výkonové spotřeby zařízení provádějícího kryptografické operace. Důležitým faktorem výkonové analýzy je nasbírání dostatečného množství dat. Hlavní výhodou DPA oproti SPA je, že zachycený signál lze dále zpracovat a tajný klíč lze získat i například ze zašuměného signálu.

Teorie útoku DPA

Útočník nejprve provede měření n průběhů výkonové spotřeby, resp. úrovně elektromagnetického pole a každý z průběhů navzorkuje na *k* hodnot. Tyto průběhy lze pak reprezentovat jako dvourozměrné pole T[0…n][0…k], kde první index určuje pořadí operace a druhý definuje konkrétní vzorek. Korespondující otevřené texty jsou reprezentovány v poli P[0…n], popřípadě zašifrované texty jsou zaznamenávány do pole C[0…n].

Naměřené průběhy lze následně rozdělit pro každý odhad klíče do dvou podmnožin na základě hodnoty bitu b. Bit b je závislý na vnitřních stavech kryptografického modulu. Předpokladem je, že bit b zařadí naměřený výkonový průběh do jedné ze dvou podmnožin. Získané podmnožiny lze definovat vztahy:

$$T_0 = \{T_i : b = 0\}, T_1 = \{T_i : b = 1\} \qquad (1.1),(1.2)$$

V případě, že otevřené zprávy budou náhodné, bude rozložení průběhu v obou podmnožinách rovnoměrné. Každá podmnožina je dále reprezentována průměrem všech průběhů v ní. Průměrný vektor pro každou podmnožinu pro j =1… k , lze zapsat:

$$A_0[j] = \frac{1}{|T_0|}\sum_{T_i \in T_0} T_i\,[j]\,,\; A_1[j] = \frac{1}{|T_0|}\sum_{T_i \in T_0} T_i\,[j] \qquad (1.3),(1.4)$$

,kde $|T_1|+|T_0| = n$ a $T_i[j]$ představuje j-tou hodnotu z měřené výkonové spotřeby T_i. Diferenciální průběh je získán rozdílem obou průměrných průběhů reprezentující danou podmnožinu. Průměrný průběh pro každou podmnožinu pro j = 1…k, lze zapsat následovně:

$$\Delta[j] = A_1[j] - A_0[j] \qquad (1.5)$$

Tyto dva průměrné průběhy budou rozdílné pouze v časových okamžicích, na které má vliv bit b, jelikož vliv ostatních bitů na výkonový průběh je zastoupen v obou podmnožinách stejně. Na základě toho lze pro diferenciální průběh v časových okamžicích j*, kdy jsou prováděny operace s bitem b zapsat takto:

$$E[T_i[j^*]|b = 1] - E[T_i[j^*]|b = 0] = \varepsilon \qquad (1.6)$$

V časových okamžicích, j ≠j*, kdy výkonová spotřeba je na bitu b nezávislá, platí:

$$E[T_i[j]|b = 1] - E[T_i[j]|b = 0] = 0 \qquad (1.7)$$

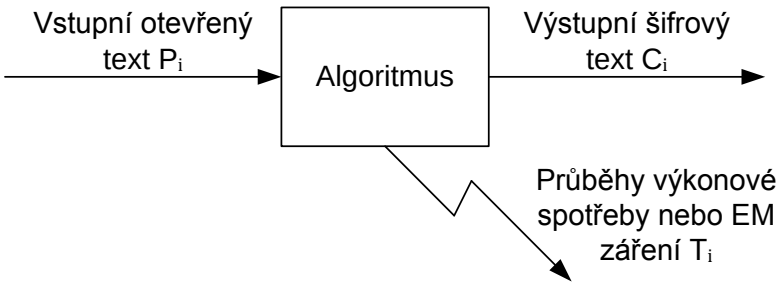
V případě, že je k dispozici dostatek naměřených výkonových průběhů, tak $A_0[j]$ a $A_1[j]$ konverguje k $E[T_i[j]|b = 0]$ a $E[T_i[j]|b = 1]$, pak lze psát:

$$\lim_{n\to\infty} \Delta\,[j] = \lim_{n\to\infty} A_1\,[j] - \lim_{n\to\infty} A_0\,[j] = \varepsilon\,, \text{pro j} = j^* \qquad (1.8)$$

Vztah 1.8 popisuje diferenciální průběh v případě správného rozdělení naměřených průběhů. Takovýto výpočet obsahuje několik zákmitů o odchylce ε v místech působnosti bitu b, okolní získané zákmity mají výrazně menší úroveň. V případě, že jsme zvolili špatný odhad, tak vztah 1.8 neplatí a diferenciální průběh bude dosahovat nulové hodnoty. Správnost přiřazení bitu b tak rozhoduje o podobě diferenciálního průběhu. Bit b se přiřazuje pro každý průběh na základě hypotézy zahrnující odhad šifrovacího klíče. Praktické způsoby realizace SPA a DPA jsou uvedeny v kapitole 3.2.1 a následně v praktické části práce, jelikož vyžadují vysvětlení základních principů fungování šifrovacího algoritmu AES. [9,10]

Základní techniky DPA analyzují informaci vytvářením diferenčních průběhů pro signály s různými vstupními hodnotami. Existují ale i další varianty DPA vyššího řádu, které využívají analýzu signálů z více zdrojů nebo zpracování signálu z jednoho zdroje různými způsoby. Diferenciální výkonová analýza vyšších řádů HO-DPA (High-Order Differential Power Analysis) umožňuje analyzovat signály z více zdrojů a s různými časovými posuvy, např. informace posbírané z různých zdrojů pomocí různých měřicích

technik. Dnes jsou HO-DPA jedním z nejsledovanějších oborů moderní kryptoanalýzy, tato metoda má veliký potenciál v oboru kryptoanalýzy postranním kanálem. Její nevýhodou je například oproti SPA a DPA složitější zpracování více signálů a s tím spojené vyšší výpočetní požadavky. [11]



Obr. 1.3: Základní princip útoku výkonovým a EM postranním kanálem.

1.6 Elektromagnetická analýza

Elektromagnetická analýza má relativně pestrou historii. V dnešní době se mnoho mezinárodních institucí po celém světě zabývá problematikou snižování EM záření, zařízeními emitujícími záření a výzkumem jak EM útoků, tak i výzkumem obranných mechanismů proti EM analýze. Patrně nejznámější pracovní skupina zabývající se vývojem a potenciální hrozbou útoku elektromagnetickým postranním kanálem fungovala ve Spojených Státech pod tajným názvem "TEMPEST" [12], která je akronymem "Transient Electromagnetic Pulse Emanation Standard" tedy Standardy pro přechodné elektromagnetické vyzařování. Některé části tohoto standardu byly v září roku 2001 na základě zákona o svobodě informací odtajněny a započala tak nová éra v oblasti útoků postranními kanály.

Ve veřejném sektoru se o významný posuv na poli elektromagnetických útoků zasloužil nizozemský vědec van Eck, který jako první dokázal, že je možné zachytit a změřit velikost elektromagnetického pole počítačových monitorů a z naměřených průběhů extrahovat snímaný obraz. Obranu proti tomuto útoku vynalezli vědci Kuhn a Anderson, jednalo se o speciální stínící fólii, která snižovala elektromagnetické záření monitoru, která činila snímání EM záření o mnoho těžším.

První veřejně publikovanou prací na téma EM analýzy integrovaných obvodů a výpočetních jednotek provádějících kryptografické operace, byla v roce 2001 práce Electomagnetic Analysis: Concrete Results autorů Gandolfiho, Mourtela, Oliviera [13]. Útok prováděli pomocí několika antén umístěných v blízkosti výpočetních integrovaných obvodů čipové karty. Tento útok byl invazivní, což znamená, že vyžadoval porušení pouzdra čipové karty, tak aby bylo možné umístit antény co nejblíže pasivační

vrstvě. Na tuto práci následně navázali o rok později Agrawal, Archambeault, Rao a Rohatgi [14], kteří ve své práci The EM-Side-Channels: Attacks and Assessment Methodologies využili odtajněných materiálů z projektu TEMPEST a ukázali, že útoky EM postranním kanálem na kryptografická zařízení jsou prakticky realizovatelné a zároveň, že některé informace unikající EM kanálem, šlo dříve získat z výkonového postranního kanálu pouze velmi obtížně. Kromě toho v jejich práci nastínili nové možnosti útoků EM postranním kanálem využívající nepřímých EM záření vznikající vazbami mezi jednotlivými částmi kryptografického systému. Dále jejich práce obsahovala systematickou studii EM úniků informace z výpočetních vybavení jako např. čipové karty, výpočetní procesory a krypto akcelerátory. [15,16,17]

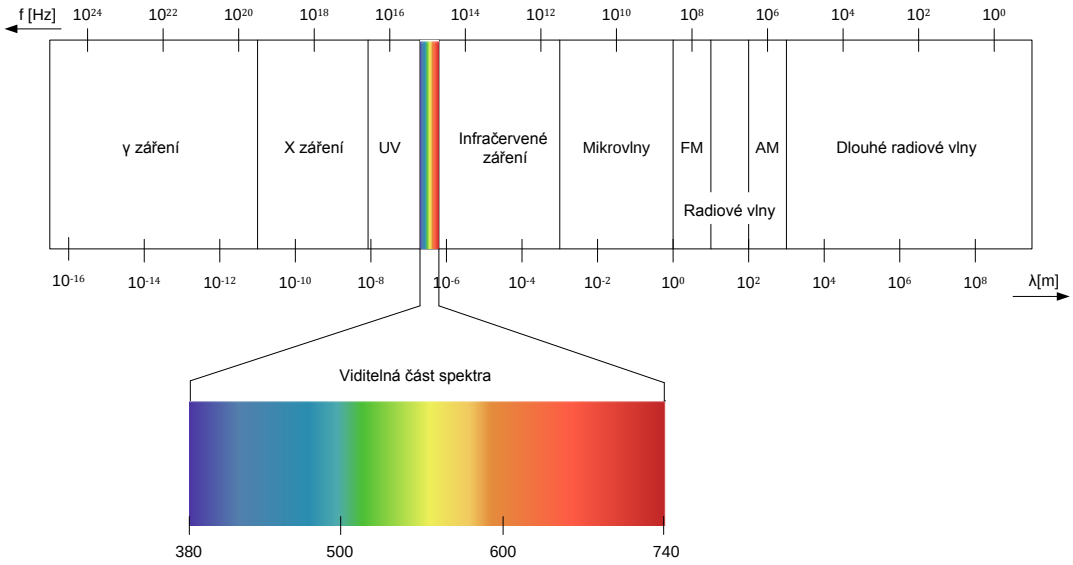
Podobně jako u výkonové analýzy, existují základní dva druhy dělení elektromagnetické analýzy, analogicky k PA, to jsou jednoduchá elektromagnetická analýza SEMA (Simple Electromagnetic Analysis) a diferenciální elektromagnetická analýza DEMA (Differencial Electromagnetic Analysis). SEMA a DEMA prakticky vycházejí z teorie SPA a DPA, jejich matematické principy jsou stejné, jediné co se liší je fyzikální podstata zpracovávaného signálu. Útoky SEMA a DEMA, jsou podrobně popsány v práci ElectroMagnetic Analysus (EMA): Measures and Counter-Measures for Smart Cards autorů Jean Jacques Quisquatera a Davida Samydea [18].

2 TEORIE ELEKTROMAGNETICKÉHO ZÁŘENÍ

Elektromagnetické záření je kombinací příčného postupného vlnění magnetického a elektrického pole tedy elektromagnetického pole. Elektrické a magnetické složky záření jsou vzájemně kolmé, a zároveň jsou kolmé ke směru šíření energie. Elektromagnetické záření se dělí do několika skupin rozdělujících se podle frekvence (popř. délky vlny) záření. Tyto skupiny jsou zobrazeny na obr. 2.1.

Jednou z částí elektromagnetického spektra je malá spektrální oblast s vlnovou délkou mezi 380 a 740 nm, která je vnímána lidským okem, tato část se nazývá viditelnou částí spektra. Elementární částice, která popisuje kvantum elektromagnetické energie, se nazývá foton, který je základní "částí" světla a ostatních elektromagnetických záření.

Elektromagnetické vlnění bylo poprvé popsáno Jamesem Maxwellem a následně byly jeho teorie potvrzeny Heinrichem Hertzem. Maxwell odvodil vlnovou formu elektrických a magnetických rovnic, popisující vlnové vlastnosti elektrických a magnetických polí a jejich symetrii. Jelikož rychlost EM vlnění odvozené z vlnových rovnic se shodovala s rychlostí světla, došel Maxwell k závěru, že světlo samo o sobě je EM vlnění. [19]



Obr. 2.1: Elektromagnetické spektrum.

Z Maxwellových rovnic vyplývá, že prostorově proměnné elektrické pole generuje časově proměnné magnetické pole a naopak, obě tyto oscilující pole dohromady tvoří elektromagnetické vlnění.

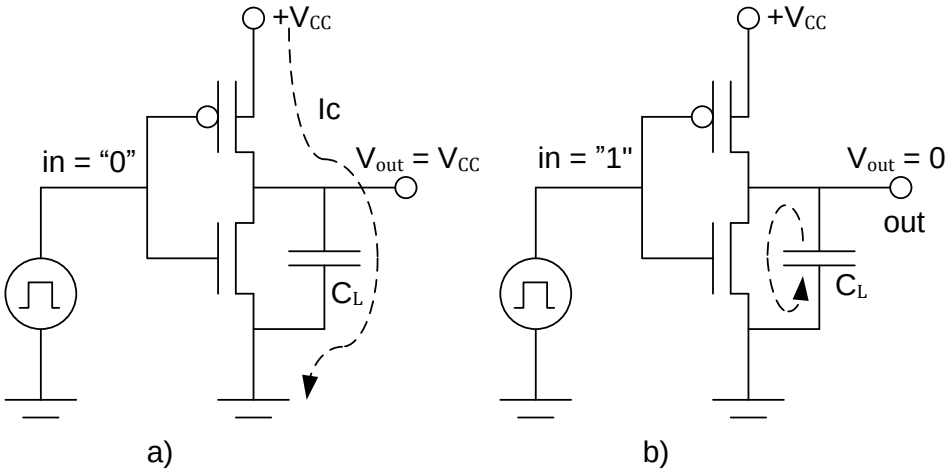
Elektromagnetické vlnění vykazuje jak vlnovou, tak částicovou povahu. Vlnové charakteristiky jsou zřejmé při měření EM záření v delším časovém úseku a na větších

vzdálenostech, naopak částicová povaha světla se projevuje především při měření v menších časových měřítcích a na kratších vzdálenostech.

- **Vlnový model EM záření** - Elektromagnetické záření je příčná vlna, u které je směr kmitání elektrické a magnetické složky kolmý na směr šíření vlny a přenosu energie. Jedním z nejdůležitějších faktorů elektromagnetického záření je jeho frekvence. Frekvence vlnění udává počet kmitů za jednotku času a její jednotkou je hertz, který má rozměr s^{-1}. Světlo má obvykle spektrum frekvencí, které se skládají ve výslednou vlnu. Dalším důležitým pojmem z vlnového pohledu na EM záření je vlnová délka záření. Vlnová délka určuje vzdálenost mezi dvěma body vlny, které po sobě následují po době jedné periody.
- **Částicový model EM záření** - jelikož energie EM vlny je kvantována, z hlediska částicového modelu se vlna skládá z diskrétních kvant energií zvaných fotony. Frekvence vlny je úměrná energii částic, kterými je tvořena. Fotony, které lze považovat za nositele energie jsou emitovány a pohlcovány nabitými částicemi. Pokud je foton absorbován atomem, předá svou energii atomu a atom je tak excitován, což se projeví přeskočením elektronu na vyšší energetickou úroveň. Pokud se elektron dostal na nejvyšší energetickou úroveň, může uniknout z jádra a být odtržen od atomu při procesu zvaném fotoionizace. Obráceně platí, že elektron, který sestoupí na nižší energetickou hladinu, v atomu excituje foton, který má energii rovnou rozdílu obou energetických hladin. Z toho vyplývá, že energetické hladiny elektronů v atomech jsou diskrétní.

2.1 Zdroje EM záření a teorie snímání EM pole

Většina zařízení s integrovanými obvody a čipy je vystavěna na základě technologie CMOS (Complementary Metal-Oxide Semiconductor). Základním prvkem technologie CMOS je logický invertor zachycený na obr. 2.2. Funkce invertoru je jednoduchá, nízká úroveň na vstupu má za následek přivedení napětí V_{CC} na výstup a naopak vysoká úroveň na vstupu způsobí propojení výstupu se zemí.



Obr. 2.2: CMOS invertor.

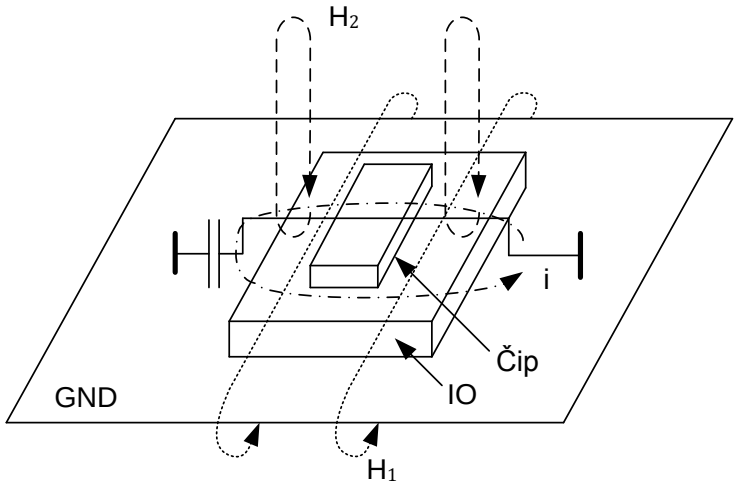
CMOS tranzistory mají tři hlavní zdroje rozptylu proudu. První dva zdroje rozptylu, jsou způsobeny tokem proudu v tranzistoru respektive tím, že oba tranzistory jsou po velmi krátkou dobu zapnuty zároveň. Tyto změny nemají významný vliv na velikost celkového proudu. Největší vliv na změnu velikosti proudu má nabíjení a vybíjení kondenzátoru C_L viz obr. 2.2 b). Následkem nabíjení a vybíjení C_L, vzniká v obvodu skoková změna proudu, projevující se emitací elektromagnetického pole v blízkém okolí invertoru.

Soudobé integrované obvody jsou složeny z milionů tranzistorů a spojů, ve kterých protékají proudy, které jsou závislé na přenášených datech. Tyto proudy generují proměnné elektromagnetické pole, které může být v okolí měřeno pomocí sond.

Způsoby, jakými se projevuje EM záření emitované integrovanými obvody, jsou následující:

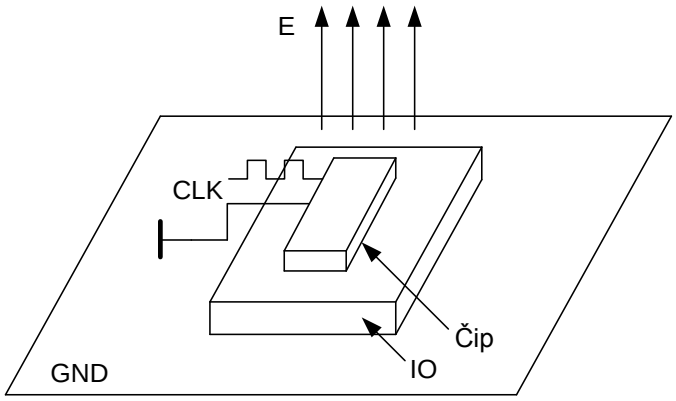
- Vodivá emise – se projevuje na pinech integrovaného obvodu, respektive v cestách na ně připojených, kdy se vlivem skokové změny proudu tyto cesty mohou chovat jako antény emitující rušení.

- Elektrická a magnetická emise v blízkém poli – EM pole je generováno vlivem proudových smyček v IO. Magnetická složka pole lze rozdělit na dvě části H_1 a H_2, viz obr. 2.3. Pole H_1 se uzavírá kolem zemnícího kontaktu tištěného spoje, pole H_2 je generováno proudy ve vnitřních kondenzátorech a uzavírá se v oblasti nad povrchem IO v dosahu přibližně do 10 mm. Magnetické pole H_2 je výrazně větší než pole H_1.



Obr. 2.3: Princip přímé emise magnetického pole IO.

Elektrické pole se nachází v okolí součástí pod napětím. V IO jsou zdrojem elektrického pole vnitřní vodivé spoje. Na obr. 2.4 je zobrazena emise elektrickým polem způsobená hodinovým signálem. Většina toku se uzavírá do země, ale část toku je vyzářena do okolí.



Obr. 2.4: Princip přímé emise elektrického pole IO.

Vyjdeme-li z předpokladu, že IO generuje elektromagnetické pole, pak je možné charakterizovat elektromagnetickou emisi IO, pomocí měření těchto polí. Tato měření se realizují pomocí elektrických a magnetických sond. Měření pomocí rozměrově malé magnetické sondy slouží k zjištění velikosti magnetické složky blízkého EM pole. Výhodou těchto sond je, že mohou být umístěny co nejblíže ke zdroji záření a zvyšují tak přesnost měření. Pokud se sonda umístí do větší vzdálenosti[3], pak bývá zachycen u mikroprocesorů hodinový signál CLK. Důvodem je, že CLK signály jsou v uvedených zařízeních dominantní a jejich úroveň významně převyšuje úroveň ostatních signálů. Pokud sondu umístíme do blízkosti některého zařízení, je možné pozorovat emisi konkrétního části zařízení (např. CPU, sběrnice, paměti apod.). Užitečné EM signály, které jsou závislé na zpracovávaných datech lze zachytit v oblastech procesoru a pamětí kryptosystému. [20,21]

K zachování věrnosti měření by měla veškerá měření probíhat v blízké zóně, tedy ve vzdálenosti do maximálně délky vlny od zdroje. V této zóně všechny signály mohou být považovány za kvazistatické. Proto lze definovat Biot-Savartův zákon popisující magnetickou indukci pole $\vec{B}$:

$$d\vec{B} = \frac{\mu I\, \overrightarrow{dl} \times \hat{r}}{4\pi |\vec{r}|^2} \tag{2.1}$$

, kde μ je permeabilita prostředí, I je proud, $\overrightarrow{dl}$ je vektor jehož rozměr určuje délku diferenčního elementu a jeho směr určuje směr konvenčního proudu a $\vec{r}$ je vektor specifikující vzdálenost mezi zdrojem záření a bodem měření, pro $\hat{r}$ platí $\hat{r} = \vec{r}\,/|\vec{r}|$. Dále lze pomocí Faradayova zákona vyjádřit hodnotu magnetomotorického napětí, které se bude v sondě indukovat:

$$U_{emf} = -N\frac{d\Phi}{dt} \tag{2.2}$$

[3] U smart karet a procesorů se za větší vzdálenost považuje více než 1 cm sondy od zdroje

, kde U_{emf} je magnetomotorické napětí, N je počet závitů sondy (cívky) a dΦ vyjadřuje změnu magnetického toku za dobu dt. Z výše uvedeného vyplývá, že bude potřeba volit kompromis v počtu závitů cívky měřicí sondy, jelikož velikost magnetomotorického napětí je přímo úměrná počtu závitů cívky. Ale naopak z teorie snímání EM pole vychází požadavek na co nejkratší měřicí cívku. [20]

2.2 Praktické využití elektromagnetické emise

První práce publikované těsně po roce 2000 na téma EM vyzařování byly soustředěny především na přímou EM emisi. Měření přímého vyzařování vyžaduje naprosto přesné umístění sond co nejblíže povrchu kryptografického systému a i tak může být poměrně dosti složité rozpoznat konkrétní, hledaný signál, jelikož kolem zařízení se objevuje mnoho silnějších signálů (především hodinový signál), šumů a interferencí, které lokalizování hledaného signálu velmi ztěžují. V průběhu času hlubší porozumění EM záření vyústilo v možnost zachycení několika dalších druhů EM signálů. Mezi ně patří EM záření způsobené vazbami mezi jednotlivými komponenty systému, které se nazývá nepřímé vyzařování. Nepřímé vyzařování se projevuje modulací nosných signálů systému, které je možné po příjmu patřičným demodulátorem (nejčastěji amplitudovým - ADM nebo úhlovým - PDM) demodulovat a získat tak původní signál. Pokud útočník disponuje dostatečným technickým vybavením a znalostmi a je-li schopen zachytit a zpracovat více signálů v daném čase, pak může využít kombinace výše uvedených druhů EM záření pro následnou EM analýzu. Způsoby, kterými se přistupuje k měření elektromagnetického pole, se liší podle způsobu vyzařování tohoto pole.

2.2.1 Přímé vyzařování

Přímé vyzařování (Direct Emanation) je vyvoláno průchodem proudu vnitřními obvody zařízení. V čase proměnný elektrický proud má za následek vznik elektromagnetického pole popsaného Maxwellovými rovnicemi. V obvodech CMOS se proudy skládají z krátkých impulsů s ostrými náběžnými hranami, které nastávají v průběhu spínání obvodů. Tyto proudové impulsy mají za následek elektromagnetickou emisi měřitelnou v širokém frekvenčním pásmu. Pro útočníka bývá častěji užitečnější pásmo vyšších frekvencí, jelikož na nižších frekvencích dochází k většímu zašumění pásma a častějším interferencím. U komplexnějších obvodů může být právě vlivem interferencí s ostatními signály poměrně obtížné izolovat jeden konkrétní přímo vyzařovaný signál. K izolování takového signálu a odstranění interferencí je potřeba umístit sondu do těsné blízkosti zdroje EM záření. Často jsou potřeba i přídavné filtry k odfiltrování nežádoucích složek interferujících signálů. Měření přímého vyzařování bude stěžejní pro praktickou část této práce.

2.2.2 Nepřímé vyzařování

Nepřímé nebo též neúmyslné vyzařování (Unintentional Emanation) vzniká v důsledku centralizace jednotlivých komponent systému do jednoho celku. V moderních zařízeních dochází k umisťování různých okruhů a komponent do poměrně malého prostoru, což má za následek vytváření elektromagnetických vazeb mezi komponentami. Velikost vazeb pak závisí na jejich vzájemné vzdálenosti a poloze. Naprostá většina těchto vazeb je pro funkci systému nepodstatná, proto jim není věnována při návrhu větší pozornost. Z hlediska bezpečnosti informace však tyto vazby mohou poskytovat zdroj informací postranního kanálu. Toto vyzařování se totiž projevuje modulací nosných signálů zpracovávaných zařízením. V závislosti na druhu vazby může modulační signál (tj. signál způsobený EM vazbou) způsobit amplitudovou nebo úhlovou modulaci nosné. Pokud je útočník schopen pomocí EM přijímače naladěného na kmitočet nosné zachytit modulovaný nosný signál, pak může být modulační signál zpětně obnoven pomocí příslušné demodulační techniky. Výhodou je, že tyto signály mohou být zachyceny i když je přijímač naladěn nejen na základní frekvenci nosné, ale stačí být naladěn i na některou z harmonických frekvencí. To naopak často bývá ještě výhodnější, jelikož na základní frekvenci se signál často ztrácí mezi signály ve stejném pásmu, kdežto nalézt harmonické složky může být snadnější.

Obecně platí, že ke správné analýze přímého vyzařování je potřeba malá vzdálenost přijímače od zdroje záření. Naproti tomu zachycení neúmyslného vyzařování je podmíněno použitím demodulátoru. Výhodou ale je, že některé modulované nosné signály mají vyšší úroveň a jsou tak snadněji detekovatelné. Proto je možné realizovat tyto útoky i z relativně velké vzdálenosti. [14]

3 TEORETICKÝ ÚVOD PRO MĚŘENÍ

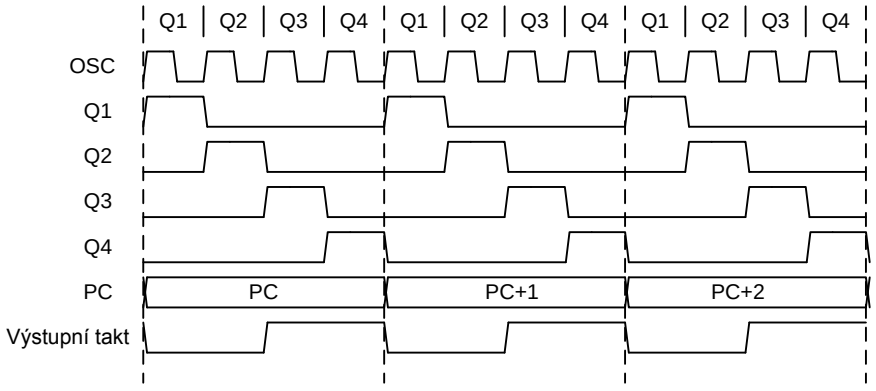
Protože měření elektromagnetického pole popsané v praktické části této práce probíhalo na mikroprocesoru PIC 16F84A, který byl naprogramovaný na provádění různých instrukcí a šifrování standardem AES, jsou v následující kapitole probrány základní vlastnosti použitého mikroprocesoru a šifrovacího standardu AES.

3.1 Mikroprocesory PIC

Tato kapitola je zkráceným průvodcem do světa mikroprocesorů. Samotná problematika mikroprocesorů není stěžejní částí této práce, proto jsou v této kapitole zařazeny pouze informace, které budou využity v praktické části.

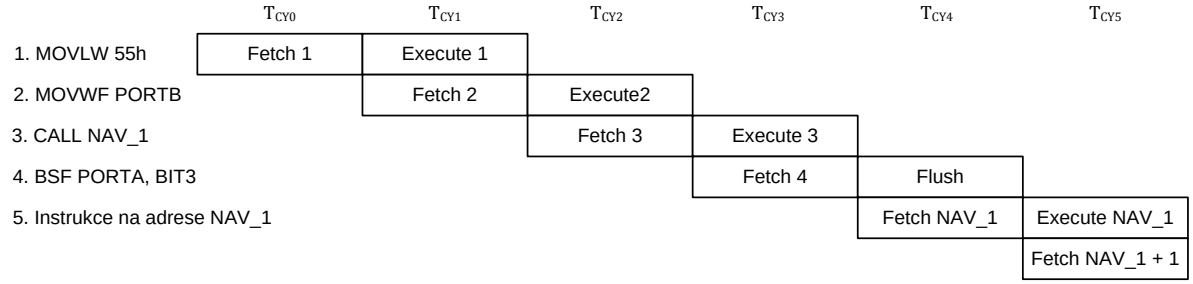
Mikroprocesory PIC 16F8X jsou nízkonákladové, výkonné, 8-bitové, CMOS mikrokontrolery. Všechny mikroprocesory z této řady mají oddělené instrukční a datové sběrnice a využívají Harvardské architektury. Dvouúrovňové instrukční zřetězení dovoluje zpracování všech instrukcí v jednom cyklu. Výjimkou jsou instrukce větvení programu, které jsou vykonávány během dvou instrukčních cyklů. Instrukční sada se skládá z 35 instrukcí. Rozložení pinů mikroprocesoru 16F84A je uvedeno v příloze B.1. Více informací a podrobností o instrukcích, pamětech, funkcích a parametrech použitých mikroprocesorů je dostupných v literatuře. [22,23]

Důležitým aspektem pro podrobnější analýzu a popis jednotlivých instrukcí je pochopení, jakým způsobem mikroprocesor instrukce postupně načítá, zpracovává a provádí. Tento proces je zachycen na obr. 3.1, který zobrazuje časové schéma taktovacího signálu a k němu přidružené instrukční cykly. Taktovací vstup z oscilátoru je interně dělen čtyřmi, za účelem vygenerování 4 kvadraturních časovacích signálů nazvaných Q1, Q2, Q3 a Q4. Interní čítač pozice PC (Position Counter) se inkrementuje při každé Q1. Instrukční cyklus se skládá ze čtyř Q cyklů. Během cyklu Q1 je každá instrukce čtena z paměti programu a je uložena do instrukčního registru. Během cyklu Q2 je instrukce dekódována. Poté proběhne její vykonání během intervalu Q3 a nakonec probíhá zápis výsledků během intervalu Q4.



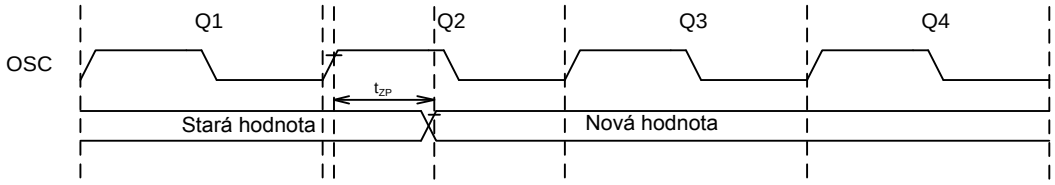
Obr. 3.1: Taktovací a instrukční cyklus.

Výše uvedený proces však u mikroprocesorů PIC úplně neplatí, protože je prováděn tzv. pipelining, který v podstatě provádí zřetězení dvou sousedních instrukcí. Princip pipeliningu je zachycen na obr. 3.2, princip je následující: Během cyklu T_{CY0} je první instrukce načtena z paměti programu, poté je tato instrukce během intervalu T_{CY1} vykonána, zatímco druhá instrukce je načtena z paměti programu. Obdobně je během intervalu T_{CY2} prováděna druhá instrukce, zatímco probíhá načítání 3. instrukce z paměti programu. Během T_{CY3} je načtena čtvrtá instrukce (BSF) a instrukce CALL NAV_1 (která provádí volání podprogramu), je vykonávána. Ve chvíli, kdy je dokončeno vykonání třetí instrukce, CPU zapíše adresu 4. instrukce do zásobníku Stack (pro uložení místa návratu) a změní Position Counter na adresu NAV_1, proto musí být instrukce BSF, která byla načtena během T_{CY3} z "roury" odstraněna. Proto jsou instrukce větvení dvoucyklové, protože až do jejich samotného vykonání nelze předčíst následující instrukci. Samotné odstranění předečtené instrukce z roury je provedeno jako instrukce NOP během intervalu T_{CY4}, zároveň je načtena instrukce na adrese NAV_1. Ta je poté vykonána během doby T_{CY5} a analogicky se postupuje dále.



Obr. 3.2: Zřetězování instrukcí.

Poslední informací, která je uvedena s ohledem na analýzu jednotlivých instrukcí v souvislosti s jejich časováním a prováděním, je zkoumání časového intervalu mezi sepnutím taktovacího oscilátoru a momentem, kdy se objeví požadovaný výstup na příslušném výstupu mikroprocesoru. Tento vztah je zachycen na obr. 3.3, který zachycuje situaci, kdy během intervalu Q4 je instrukce vykonána, ale hodnota se na výstupu objeví až s určitým zpožděním, během intervalu následující Q1, zpoždění je podle výrobce u mikroprocesoru PIC 16F84A - $t_{ZP} < 125$ ns



Obr. 3.3: Doba zpoždění výstupu.

Dalším důležitým bodem této kapitoly je seznámení se se základními instrukcemi, které budou v praktické části analyzovány. Obecně se instrukce rozdělují do tří skupin -

na bytově orientované, bitově orientované a řídící. Instrukce, které budou v praktické části analyzovány, jsou následující:

- **ADDWF – Add W and f**

Syntaxe: ADDWF f,d

Popis: ADDWF je bytově orientovaná instrukce, která sečte obsah registru W s registrem f. Pokud je příznak ‘d‘ nastaven na 0, pak je výsledek uložen do registru W, pokud je ‘d‘ rovno 1, pak je výsledek uložen do f.

Operace: (W) + (f) -> (cíl)

- **BCF – Bit Clear f**

Syntaxe: BCF f,b

Popis: BCF je bitově orientovaná instrukce, která nastaví hodnotu bitu ‘b’ v registru f na 0.

Operace: 0 -> (f<b>)

- **BSF – Bit Set f**

Syntaxe: BSF f,b

Popis: BSF je rovněž bitově orientovaná instrukce, která naopak nastavuje hodnotu bitu ‘b’ v registru f na 1.

Operace: 1 -> (f<b>)

- **CALL – Call Subroutine**

Syntaxe: CALL k

Popis: CALL patří do skupiny řídících dvoucyklových instrukcí, která provádí skok do podprogramu. Návrat z podprogramu se provádí pomocí příkazu return, který provede návrat na adresu o jednu vyšší, než má volání Call.

- **DECF – Decrement f**

Syntaxe: DECF f,d

Popis: DECF je bytově orientovaná instrukce, která dekrementuje obsah registru f a výsledek uloží buďto do registru W, pokud je ‘d’ = 0 a nebo zpět do registru f, v případě, že ‘d’ = 1.

Operace: (f) - 1 -> (cíl)

- **DECFSZ – Decrement f, Skip if 0**

Syntaxe: DECFSZ f,d

Popis: DECFSZ je bytově orientovaná instrukce, která dekrementuje obsah registru f a výsledek obdobně jako DECF uloží buďto do registru W, pokud je ‘d’ = 0 a nebo zpět do registru f, v případě, že ‘d’ = 1. Navíc pokud výsledek bude 1,

vykoná následující instrukci, pokud bude výsledek roven 0, pak namísto ní vykoná instrukci NOP, proto je DECFSZ dvoucyklová instrukce.

Operace: (f) - 1 -> (cíl);
přeskoč následující instrukci, pokud výsledek = 0

- **GOTO – Goto Adress**

Syntaxe: GOTO k

Popis: GOTO je řídící instrukce skládající se ze dvou cyklů, která obsah registru f uloží na příslušné místo na základě nastavení příznaku ‘d‘. Pokud je d=0, pak je cílem registr W, pokud je d=1, cílem je registr f sám.

- **INCF – Increment f**

Syntaxe: INCF f,d

Popis: INCF se chová naprosto stejně jako instrukce DECF, s tím rozdílem, že provádí inkrementaci registru f.

Operace: (f) + 1 -> (cíl)

- **INCFSZ – Increment f, Skip if 0**

Syntaxe: INCFSZ f,d

Popis: I v případě INCFSZ platí, že je stejná jako instrukce DECFSZ s tím rozdílem, že namísto dekrementace registru f je prováděna jeho inkrementace, následné podmínky zůstávají v platnosti.

Operace: (f) + 1 -> (cíl);
přeskoč následující instrukci, pokud výsledek = 0

- **MOVF – Move f**

Syntaxe: MOVF f,d

Popis: MOVF je bytově orientovaná instrukce, která ukládá obsah registru f do cílového registru podle stavu ‘d‘. Když ‘d‘ = 0, cílem je registr W, pokud je‘,d‘ = 1, cílem je sám registr f.

Operace: f -> (cíl)

- **MOVWF – Move W to f**

Syntaxe: MOVWF f

Popis: MOVWF je bytově orientovaná instrukce provádějící přesun registru w do registru f.

Operace: (W) -> (f)

- **NOP – No Operation**

Syntaxe: NOP

Popis: NOP je bytově orientovaná instrukce, která nic neprovádí, v jednotlivých Q cyklech je definován pouze první cyklus dekódování, v ostatních cyklech se nic neprovádí.

- **XORWF – Exclusive OR W with f**

Syntaxe: XORWF f,d

Popis: XORWF je bytově orientovaná instrukce, která provádí operaci exkluzivního součtu obsahů registrů W a f. Podobně, jako u předchozích operací, pokud je příznak 'd' nastaven na 0, pak je výsledek uložen do registru W, pokud je 'd' rovno 1, pak je výsledek uložen do f.

Operace: (W) .XOR. (f) -> (cíl)

3.2 Advanced Encryption Standard – AES

AES je standard pro šifrování dat symetrickým klíčem. Jeho základy jsou postaveny na algoritmu Rijndael, pojmenovaného podle jeho tvůrců Joana Daemena a Vincenta Rijmena [24]. AES je symetrická bloková šifra umožňující zpracovat 128 bitové datové bloky, s použitím klíčů dlouhých 128, 192 nebo 256 bitů. AES je nástupcem standardu DES, který především kvůli krátkým délkám použitých klíčů přestal na začátku třetího tisíciletí vyhovovat účelům bezpečného šifrování. AES byl představen na konci roku 2001 ve Spojených Státech Amerických Národním institutem pro standardy a technologie (NIST – National Institute of Standards and Technology) v dokumentu FIPS PUB 197 [25].

Tab. 3.1: Pravdivostní tabulka XOR.

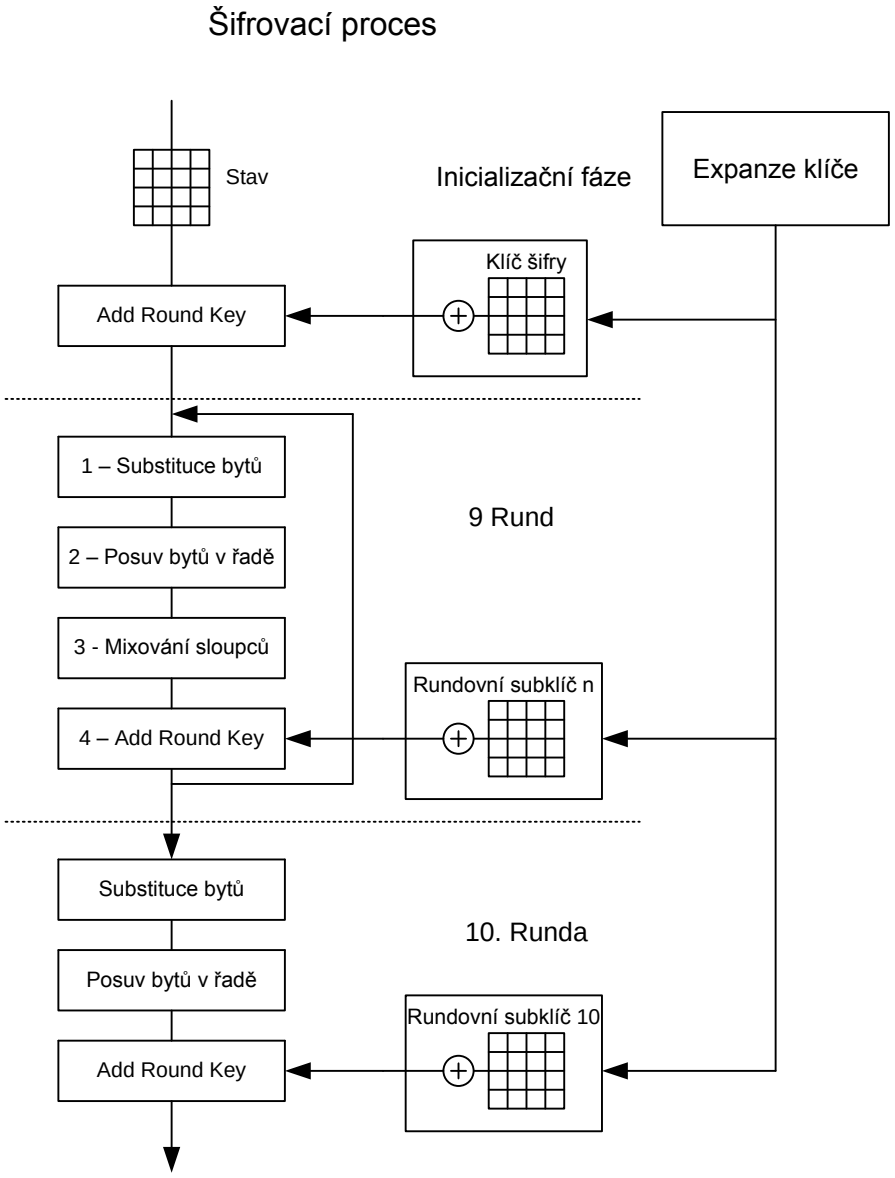
X	Y	$X \oplus Y$
0	0	0
0	1	1
1	0	1
1	1	0

Šifrování pomocí standardu AES je zachyceno na obr. 3.4. Jednotlivé funkce algoritmu jsou prováděny v následujících fázích:

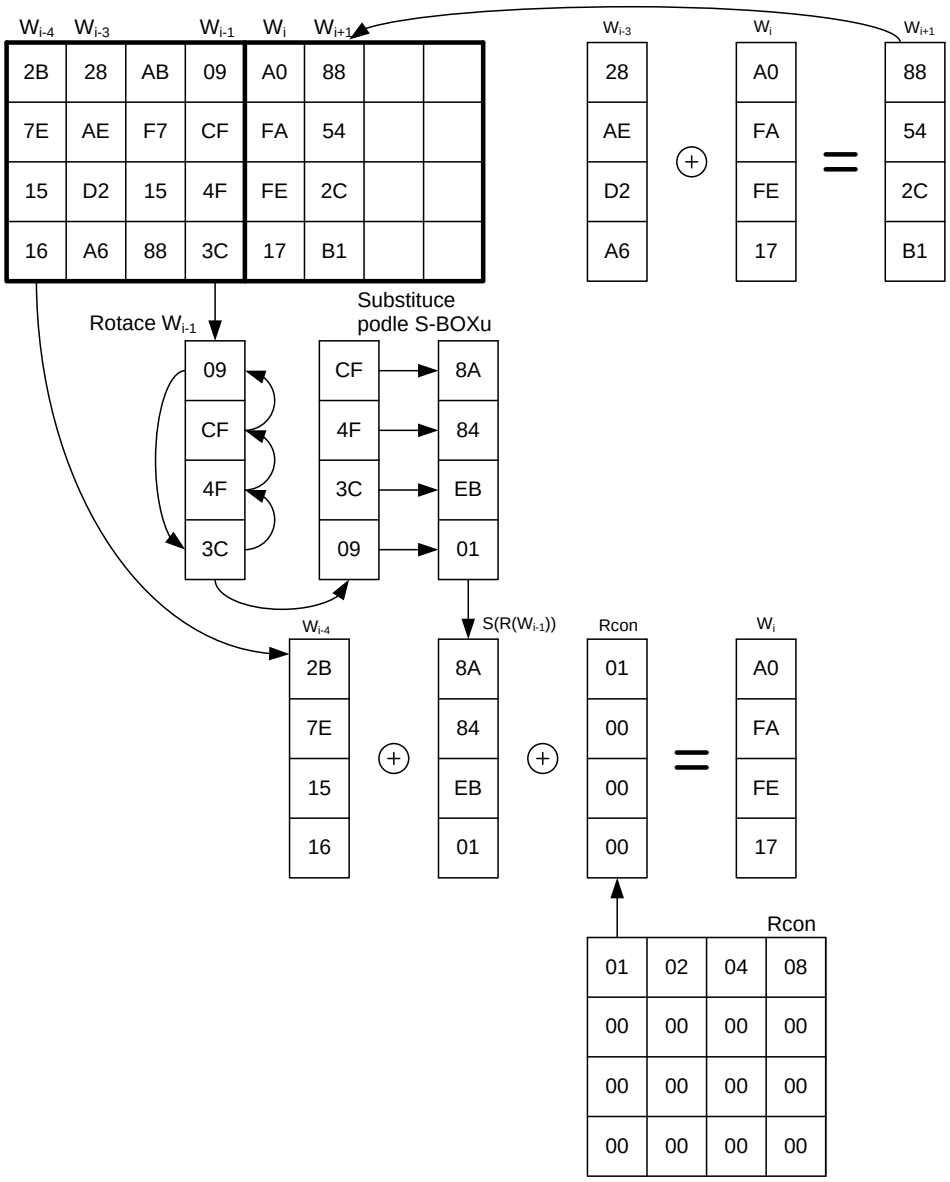
1. Expanze klíče – spočívá v odvození jednotlivých rundovních subklíčů.
2. Inicializační Runda
   a) Add Round Key – každý byte stavu je kombinován s bytem rundovního subklíče za pomocí operace xor (viz Tab. 3.1).
3. Rundy 1 ÷ 9
   a) Substituce bytů – je nelineární substituce, která znaky nahradí jinými znaky, podle substituční tabulky (tzv. S-BOX)[25], substituce je samotným jádrem šifrování.

b) Posuv bytů v řadě – je transpoziční krok, při kterém je každá řada stavu cyklicky posunuta o určitý počet kroků. Počet kroků odpovídá pořadí řady, pokud nejvrchnější řada bude označena jako nultá.
c) Mixování sloupců – v tomto kroku je každý sloupec stavu vynásoben určitou maticí, která je pro všechny sloupce stejná.
d) Add Round Key

4. Finální runda
   a) Substituce bytů
   b) Posuv bytů v řadě
   c) Add Round Key



Obr. 3.4: Šifrování AES 128b.



Obr. 3.5: Schéma plánování klíče AES 128b.

Schéma plánování klíče pro šifrovací standard AES-128 je zachyceno na obr. 3.5. První čtyři sloupce tabulky zobrazují 128b klíč, další čtyři sloupce reprezentují první odvozený rundovní subklíč. První sloupec prvního rundovního subklíče W_i se určí jako kombinace xor prvního sloupce klíče W_{i-4} se substituovaným a rotovaným 4. sloupcem klíče $S(R(W_{i-1}))$ a prvním sloupcem tabulky Rcon. Tento postup se analogicky opakuje pro každý první sloupec všech n rundovních subklíčů. Druhý sloupec rundovního subklíče W_{i+1} se vypočte pomocí xorování sloupců W_i a W_{i-3}. Toto pravidlo pak analogicky platí i pro třetí a čtvrtý sloupec jednotlivých rundovních subklíčů. Více informací k této problematice je uvedeno v [26,27].

Pro algoritmus AES-128 platí, že délka vstupního, výstupního bloku a stavů je vždy 128 bitů. V praxi jsou ale rovněž využívány verze AES se 192 a 256 bitovým klíčem, pro jednotlivé verze AES platí, že se liší počet jednotlivých rund prováděných během jedné operace šifrování viz Tab. 3.2.

Tab. 3.2: Standardy AES.

Standard	Délka klíče[b]	Velikost bloku [b]	Počet rund [-]
AES-128	128	128	10
AES-192	192	128	12
AES-256	256	128	14

3.2.1 Realizace SEMA/DEMA na algoritmus AES

Pro úspěšnou realizaci elektromagnetické analýzy na algoritmu AES, je nutné se nejprve seznámit s principem modelu Hammingovy váhy klíče. Hammingova váha určuje počet jedniček, který bitová kombinace obsahuje. Při zpracování dat s vyšší Hammingovou vahou, systém spotřebuje více energie, než při zpracování stejně dlouhé značky s nižší Hammingovou vahou. Podle teoretických předpokladů tak z procesoru uniká množství informace úměrné Hammingově váze dat, která jsou zpracovávána.

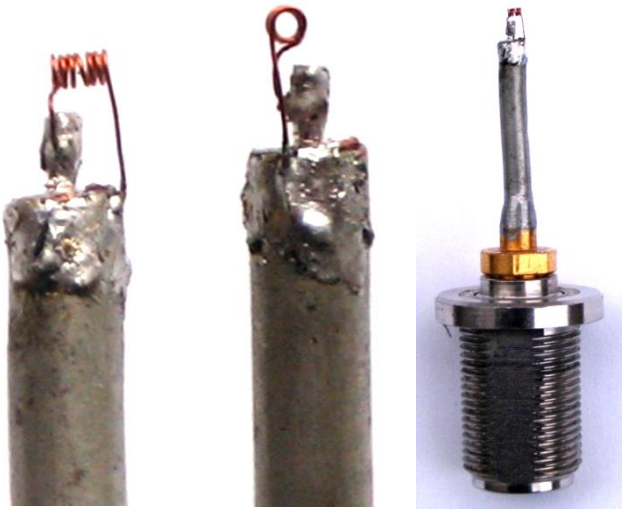
Cílem útoku na AES je stanovení Hammingovy váhy 128b klíče AES. Pokud je útočník schopný zjistit, kolik má klíč jedniček, resp. nul, výrazně mu to ulehčí práci, protože se sníží počet možných kombinací. Následně je možné vygenerovat všechny možnosti klíče s danou Hammingovou vahou a pomocí bruteforce útoku vybrat správný klíč. Pokud budeme realizovat útok EM postranním kanálem, pak jedinečnou možností, kdy zjistit Hammingovu váhu klíče je v inicializační fázi. Při počáteční operaci Add Round Key, při které je prováděna operace xor vstupního stavu a šifrovacího klíče. Při provádění operace xor je totiž změněn počet bitů, úměrný počtu jedniček v klíči[4]. Mimo tento model ještě existují některé sofistikovanější metody EMA, tyto jsou pak uvedeny pro konkrétní praktický případ v kapitole 5.5.

[4] Uvedený příklad platí pro případ, že jsou příslušné stavové bity nastaveny buďto všechny na hodnotu 1 nebo na hodnotu 0

4 NÁVRH MĚŘICÍHO PRACOVIŠTĚ A MĚŘICÍ TECHNIKY

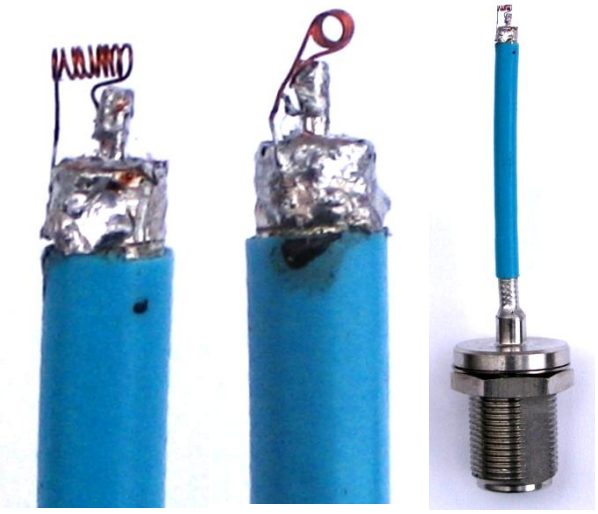
Na základě získaných teoretických poznatků uvedených v předchozích kapitolách, byla provedena realizace sond pro měření magnetické složky elektromagnetického pole pro měření v blízkém poli. Celkem byly vyrobeny 4 sondy s následujícími parametry:

- Sonda č. 1: Byla zhotovena z měděného drátu o průměru d = 0,15 mm, z 7 závitů navinutých do tvaru solenoidu s vnitřním průměrem 0,7 mm, naletovaného na přibližně 3 cm dlouhý postříbřený semi-rigid koaxiální kabel s charakteristickou impedancí 50 Ω s připojeným N konektorem. Viz obr. 4.1.



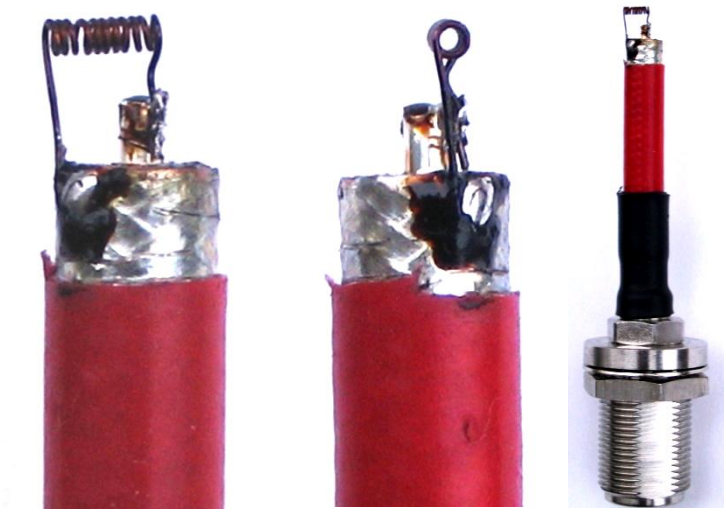
Obr. 4.1: Sonda č. 1.

- Sonda č. 2: Byla zhotovena z měděného drátu o průměru d = 0,15 mm, z 9 závitů navinutých do tvaru solenoidu s vnitřním průměrem 0,7 mm, naletovaného na přibližně 5 cm dlouhý koaxiální kabel s charakteristickou impedancí 50 Ω s připojeným N konektorem. Viz obr. 4.2.



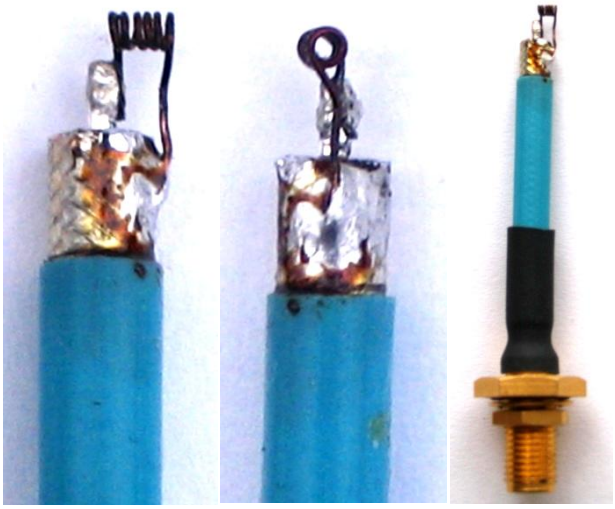
Obr. 4.2: Sonda č. 2.

- Sonda č. 3: Byla zhotovena z měděného drátu o průměru d = 0,3 mm, z 11 závitů navinutých do tvaru solenoidu s vnitřním průměrem 0,7 mm, naletovaného na přibližně 5 cm dlouhý koaxiální kabel s charakteristickou impedancí 50 Ω s připojeným N konektorem. Viz obr. 4.3.



Obr. 4.3: Sonda č. 3.

- Sonda č. 4: Byla zhotovena z měděného drátu o průměru d = 0,3 mm, z 6 závitů navinutých do tvaru solenoidu s vnitřním průměrem 0,7 mm, naletovaného na přibližně 3 cm dlouhý koaxiální kabel s charakteristickou impedancí 50 Ω s připojeným SMA konektorem. Viz obr. 4.4.



Obr. 4.4: Sonda č. 4.

Tab. 4.1: Zhotovené sondy.

Sonda	Průměr drátu d [mm]	Počet závitů	Konektor
Sonda č. 1	0,15	7	N
Sonda č. 2	0,15	9	N
Sonda č. 3	0,30	11	N
Sonda č. 4	0,30	6	SMA

4.1 Metodika měření a návrh měřicího pracoviště

Vlastnosti jednotlivých sond budou odzkoušeny při měření elektromagnetické emise procesoru PIC 16F84A. Měření by mělo prokázat vlastnosti jednotlivých sond. Na základě výsledků měření bude určeno, která sonda bude dosahovat nejlepších výsledků odstupu signál/šum a bude mít vhodné mechanické vlastnosti. S touto sondou budou prováděna další dílčí měření EM pole.

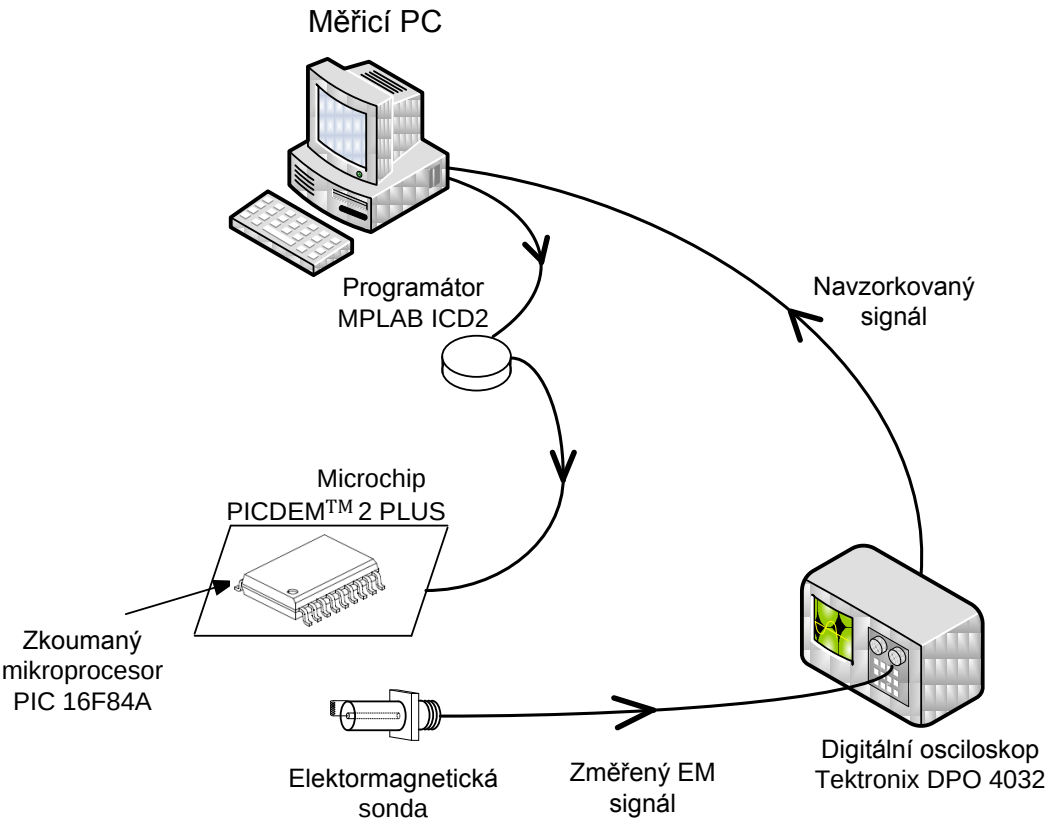
Další část měření se zaměří na zjištění ideální vzdálenosti a polohy cívky vůči sledovaného mikroprocesoru.

Měření bude provedeno na dekapsulovaném a nedekapsulovaném mikroprocesoru PIC 16F84A.

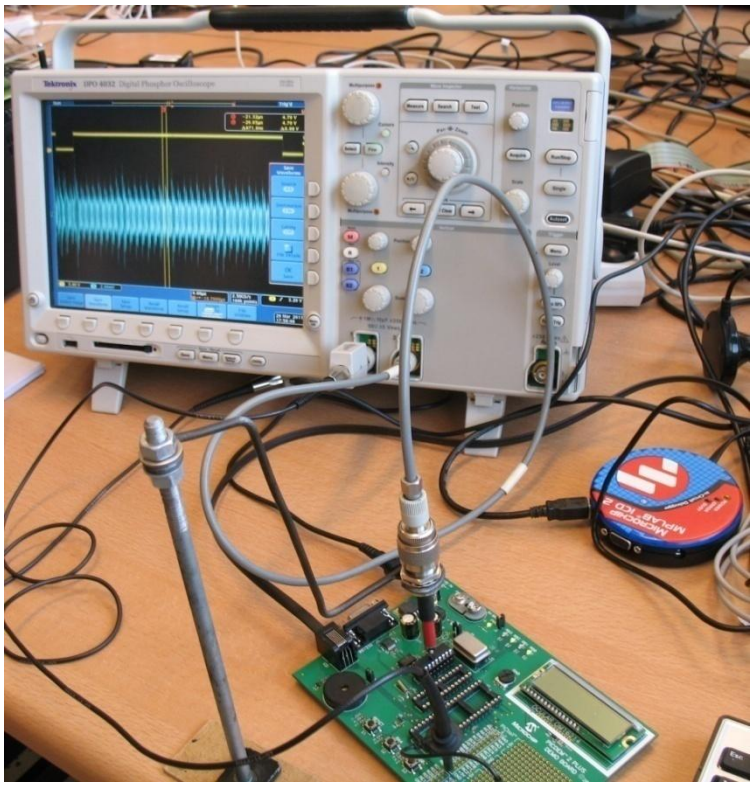
Poté již bude změřena velikost EM pole v okolí mikroprocesoru PIC 16F84A provádějícího vybrané instrukce a bude provedeno porovnání s paralelně měřeným výkonovým odběrem mikroprocesoru.

V poslední části bude provedena analýza šifrovacího standardu AES a to jak v jeho celkovém průběhu, tak v jednotlivých rundách a budou provedeny metody jednoduché a diferenční analýzy na šifrovacím algoritmu AES.

Pracoviště, na kterém budou prováděny jednotlivá měření, je zobrazené na obr 4.5 a 4.6.



Obr. 4.5: Zapojení měřicího pracoviště.



Obr. 4.6: Měřicí pracoviště.

4.1.1 Vybavení měřicího pracoviště

Měřicí stanoviště bylo vybudováno v laboratoři PA-339, pro měření přímé emise bylo zapojeno dle obr. 4.5, resp. 4.6 a bylo sestaveno z následujících přístrojů:

- *Měřicí PC*: Osobní počítač s operačním systémem Windows XP SP3 a s nainstalovaným softwarem MPLAB IDE v 8.63, umožňující práci s programátorem MPLAB ICD a s nainstalovaným programem MATLAB v. 7.0.1.

- *Elektromagnetická sonda*: Ručně vyrobená elektromagnetická sonda pro snímání magnetické složky blízkého EM pole, podrobněji popsaná výše v této kapitole.

Programátor MPLAB ICD2: Programátor pro programování mikrokontrolerů PIC s USB a RS-232 rozhraními. Programátor spolupracuje s vývojovým prostředím MPLAB IDE, nainstalovaným na měřicím PC.

- *Vývojová deska PICDEM™ 2 PLUS*: Vývojová deska s možností programování a ověřování funkčnosti 18, 28 a 40 pinových mikroprocesorů řady PIC16X a PIC18X, se zařazeným 4 MHz nebo 20 MHz oscilátorem, rozmístění součástek a schéma vývojové desky jsou uvedeny v příloze B. [28]

- *Digitální osciloskop*: Dvoukanálový digitální osciloskop DPO - 4032 s fosforovým displejem od firmy Tektronix s maximálním vzorkovacím kmitočtem 2,5 GSa/s a rozhraním USB pro ukládání dat. [29]

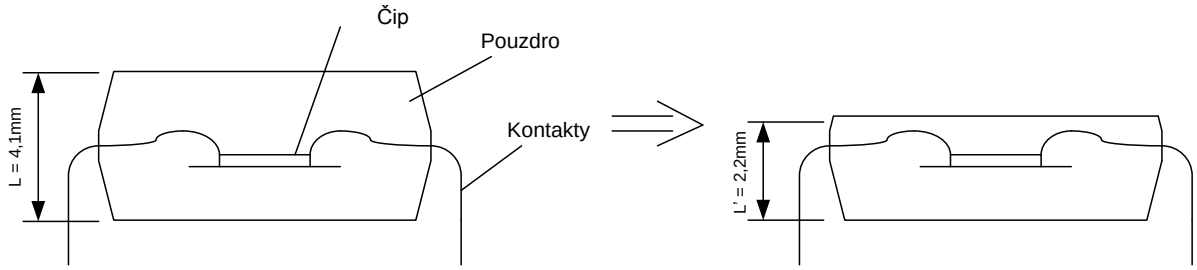
5 PRAKTICKÁ ČÁST

5.1 Úvodní měření

Cílem úvodních měření bylo sestavení měřicího pracoviště, porovnání jednotlivých sond a zjištění vlivu vzájemné polohy sondy a mikroprocesoru na měřený EM průběh a zajištění ideálních podmínek pro měření. Popsány byly rovněž nejdůležitější aspekty týkající se synchronizačního signálu, nastavení osciloskopu, taktovací frekvence apod. Zároveň byl v této kapitole popsán rozdíl v EM a výkonovém průběhu naměřeném na stejném cyklu.

5.1.1 Porovnání jednotlivých sond

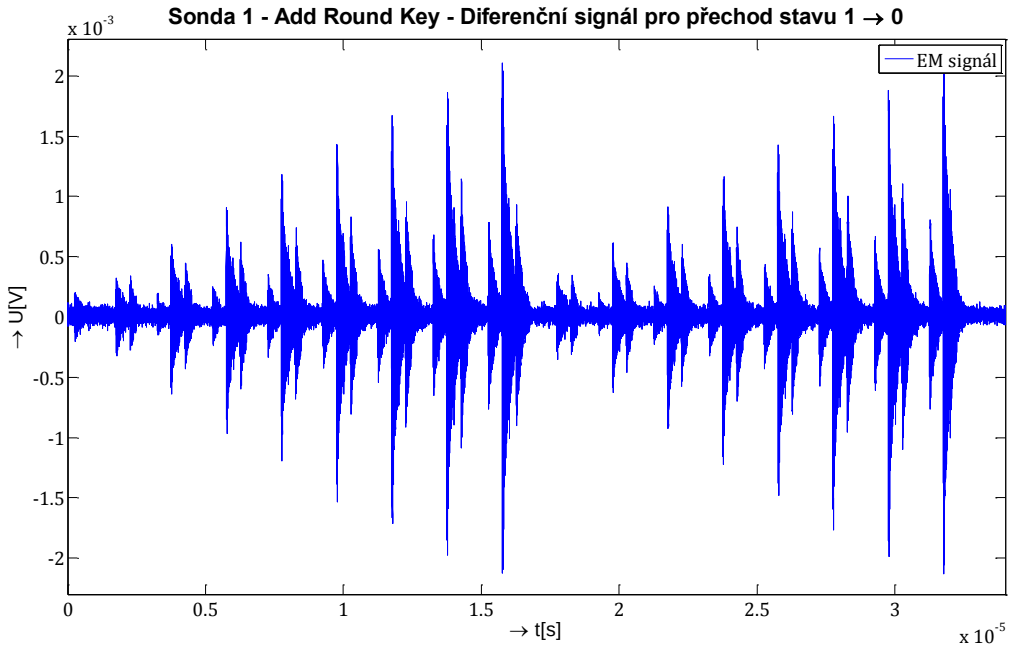
Úvodní měření bylo zaměřeno na porovnání jednotlivých sond při měření EM pole mikroprocesoru PIC 16F84A. Tento mikroprocesor byl pro měření EM pole mechanicky upraven obroušením pouzdra mikroprocesoru z vrchní strany čipu, tloušťku neodbroušené vrstvy, tedy vzdálenost sondy od samotného čipu mikroprocesoru, lze pouze stěží odhadnout, jelikož vývody od čipu k jednotlivým pinům vedou skrze pouzdro podle obr. 5.1 a dalším broušením by mohlo dojít k přerušení některých vodivých cest. Samotné měření probíhalo tak, že jednotlivé sondy byly přiloženy na pouzdro mikroprocesoru a bylo provedeno měření EM pole mikroprocesoru naprogramovaného na provádění jednotlivých programů uvedených v příloze.



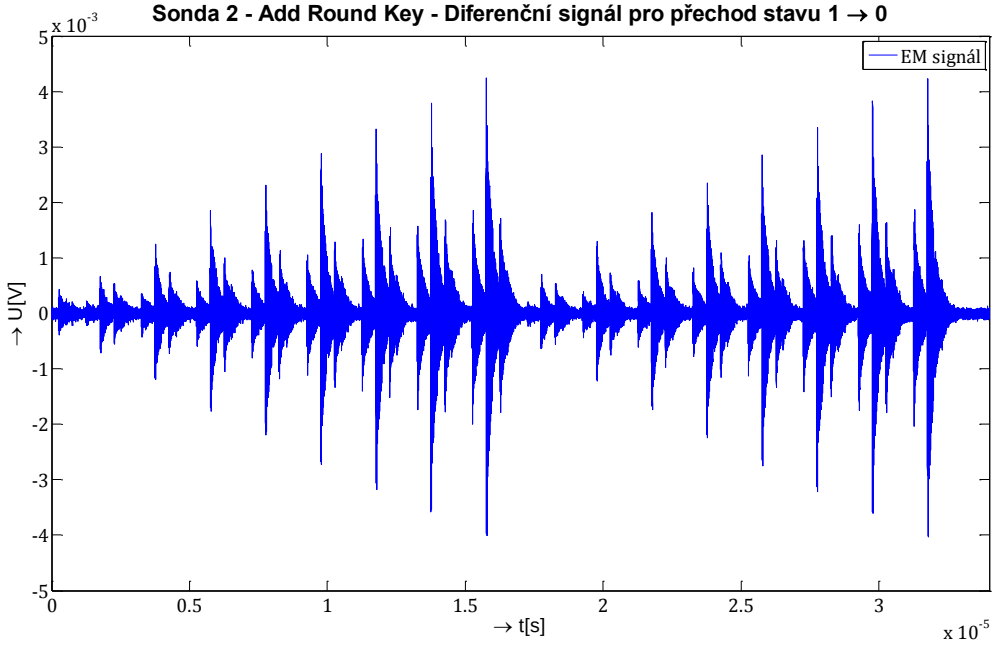
Obr. 5.1: Vnitřní řešení mikroprocesorů.

Porovnání vlastností sond bylo provedeno podle toho, nakolik byla užitečná informace jednotlivých sond ovlivněna šumem. V praxi tedy bylo přistoupeno k porovnání EM průběhů naměřených jednotlivými sondami na mikroprocesoru, který byl nejprve naprogramován na provádění operací xor se všemi stavy nastavenými na hodnotu 1 a nulovým klíčem. EM průběh naměřený v tomto cyklu, posloužil jako referenční hodnota. Následně byl mikroprocesor naprogramován na cyklické provádění operace xor s 8 bitovými hodnotami klíče, které byly voleny tak, aby postupně docházelo k zvyšování počtu jedniček v jednotlivých bytech klíče. Tento program tak postupně měnil počty tranzistorů, které byly spínány při zapisování výsledků operací xor do registrů. To se dále projevovalo zvyšováním amplitudy jednotlivých špiček v místě ukládání výsledků do paměti. Zobrazený diferenční signál vznikl odečtením signálu při

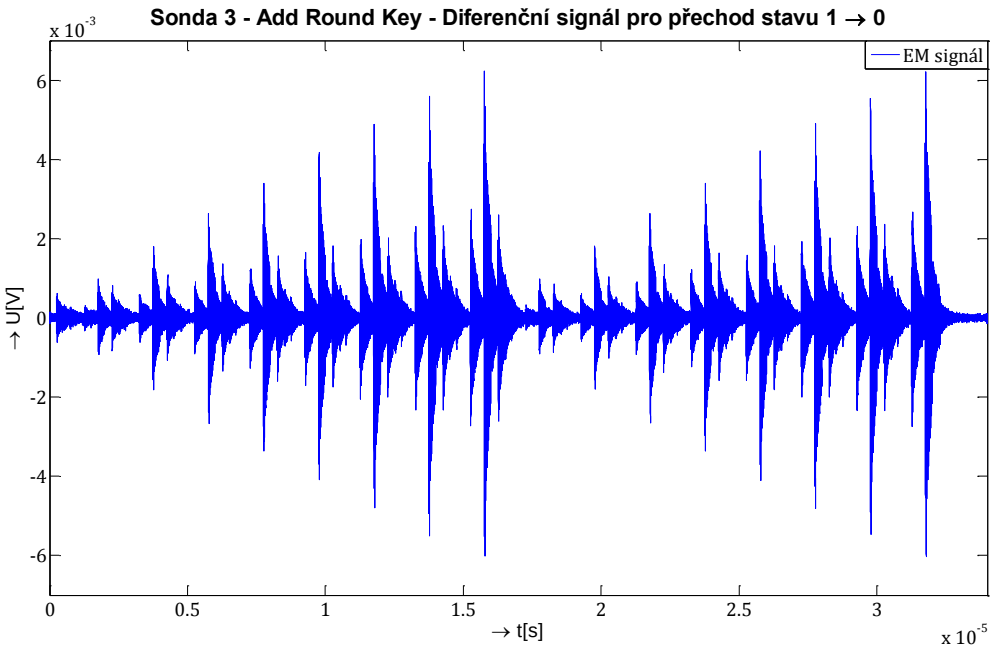
operaci xor při rostoucí hodnotě klíče a referenčního signálu změřeném při nulovém klíči. Průběhy naměřené na jednotlivých sondách jsou zobrazeny na následujících obrázcích 5.2 ÷ 5.5. Hlavní část programu *Add Round Key* je uvedena v příloze A.1.



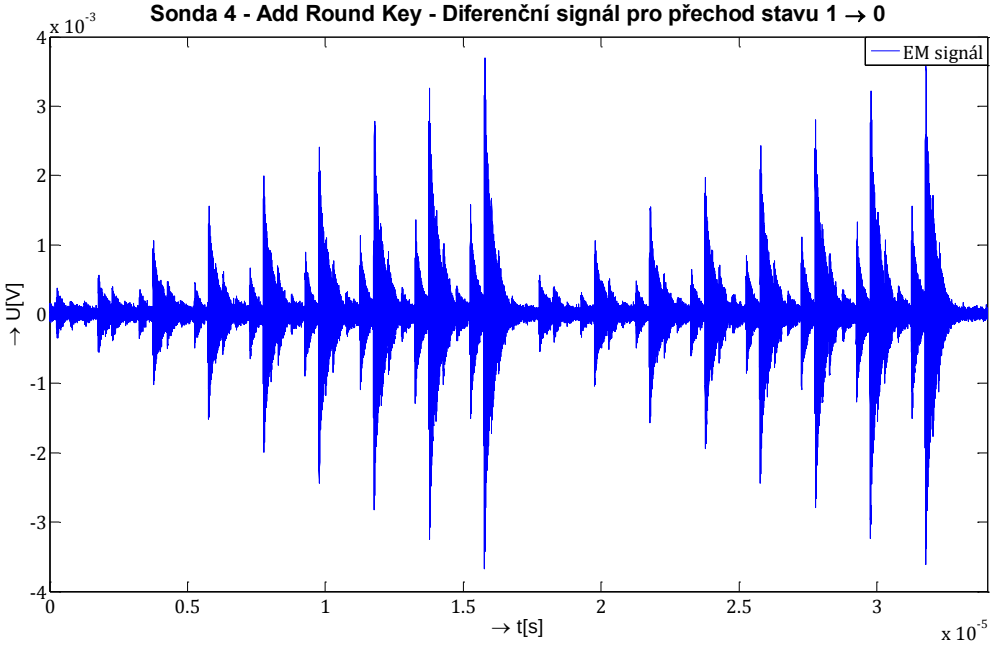
Obr. 5.2: Diferenční signál pro sondu 1.



Obr. 5.3: Diferenční signál pro sondu 2.



Obr. 5.4: Diferenční signál pro sondu 3.



Obr. 5.5: Diferenční signál pro sondu 4.

Praktický význam těchto průběhů bude probrán až kapitolách 5.4 a 5.5, v současné chvíli nás zajímá pouze vzájemné porovnání jednotlivých průběhů. Jak je patrné z předchozích obrázků, tak v podstatě všechny sondy vykazují téměř shodné výsledky a proto se dá předpokládat, že se všemi sondami by byla měření realizovatelná. Pro další měření však byla vybrána Sonda č. 3 a to především ze dvou důvodů: Prvním z nich bylo, že sonda má největší počet závitů (11) a tudíž úroveň indukovaného napětí byla nejvyšší, druhým důvodem bylo, že Sonda č. 3 je z drátu o průměru 0,3 mm, tudíž je mechanicky odolnější oproti sondám zhotoveným z drátu o průměru 0,15 mm. U těch díky časté manipulaci docházelo k ohýbání drátu cívky nebo odlamování cívky od koaxiálního kabelu. Vybrané zdrojové kódy zpracované v programu MATLAB v 7.0.1, pro zobrazení EM průběhů, jsou uvedeny v elektronické příloze.

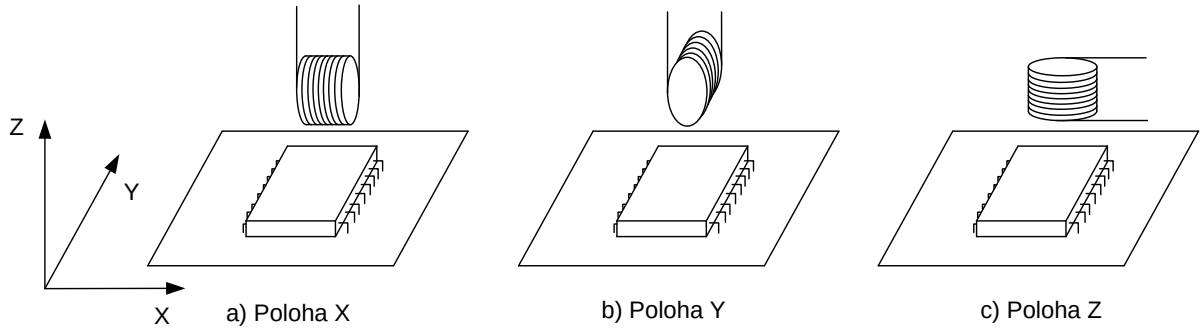
Tato úvodní měření probíhala při nastavení osciloskopu Tektronix DPO 4032, podle tab 5.1, většina měření, která jsou probraná v části praktického měření, probíhala se stejným nastavením osciloskopu, proto toto nastavení považujme za výchozí. V případě měření, kdy byl osciloskop nastaven jinak, je vždy nastavení uvedeno explicitně pro konkrétní měření. Dále budou v rámci této kapitoly probrány některé důležité aspekty, které mají vliv na měření a vyhodnocení výsledků.

Tab. 5.1: Nastavení osciloskopu pro měření EM emise.

Snímací mód	Průměrování – Average 64
Trigger mód	Nástupná hrana – Channel 1
Coupling	DC
Sampling rate	Max. 2,5 GSa/s
Channel 1	Synchronizační signál
Channel 2	EM signál

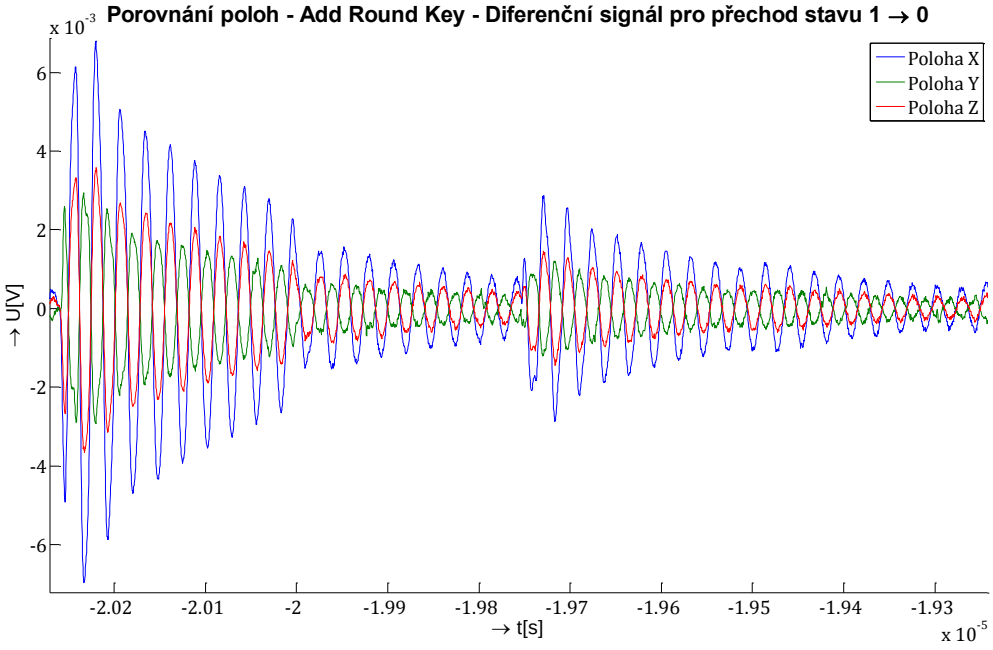
Vliv polohy měřicí cívky na měření

Kromě výběru vhodné měřicí cívky bylo rovněž nutné zjistit, ve které z poloh mezi měřicí cívkou a mikroprocesorem budou realizovaná následující měření. Polohy, do kterých bylo možné měřicí cívku uložit, jsou zobrazeny na obr. 5.6. Samotné měření bylo principiálně stejné jako úvodní měření porovnání sond, nyní však namísto jednotlivých sond byla měřena jedna vybraná sonda č. 3 ve třech různých polohách.



Obr. 5.6: Možné polohy měřicích sond.

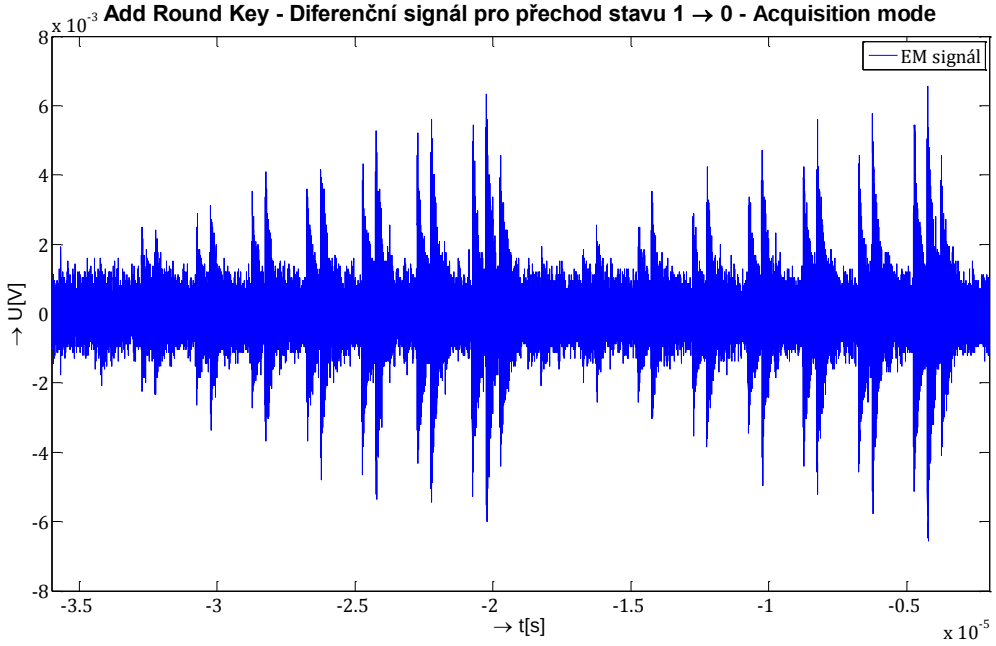
Při pohledu na obr. 5.7, který v detailu na nejvyšší diferenční špičku, zobrazuje stejný diferenční signál, jako v předchozím měření, je patrné, že nejvyšší diference indukovaného napětí vykazuje signál naměřený cívkou v poloze X. Zajímavý je také pohled na průběh v poloze Y, který má oproti průběhům změřeným v ostatních dvou polohách přesně obrácenou fázi. To bylo způsobeno tím, že cívka byla otočená o 180°, než měla být. Tento fakt však nijak neovlivňuje amplitudu průběhu. Z uvedených průběhů vyplývá, že další měření budou realizována v poloze X.



Obr. 5.7: Porovnání poloh měřicí sondy.

Volba snímacího módu osciloskopu

Měřicí osciloskop umožňuje měření v různých módech, prakticky využitelné jsou především dva módy – snímací mód s průměrováním (Averaging mode) a prostý snímací mód (Acquisition mode). Pokud bychom je měli oba teoreticky porovnat, tak snímací mód s průměrování snižuje vliv náhodného šumu a přispívá tak k lepšímu a přesnějšímu zobrazení výsledků. Prostý snímací mód je vhodný především pro změření jednoho, aktuálně zachyceného opakování daného cyklu. Diferenční signály na obr. 5.2 ÷ 5.5 byly změřeny ve snímací módu s průměrováním – Averaging 64, ten umožňuje průměrování z 64 posledních vzorků na příslušné pozici. Stejné průběhy byly pro porovnání snímány i v prostém snímací - Acquisition módu. Vliv šumu byl v Acquisition módu podle očekávání poměrně dosti výrazný viz obr. 5.8, na kterém je zachycen stejný diferenční signál pro přechody stavů z 1 do 0 pro postupně rostoucí hodnotu klíče. Tento průběh lze porovnat s průběhem na obr. 5.4, u kterého byly referenční průběhy snímány se stejným nastavením, v módu s průměrováním.

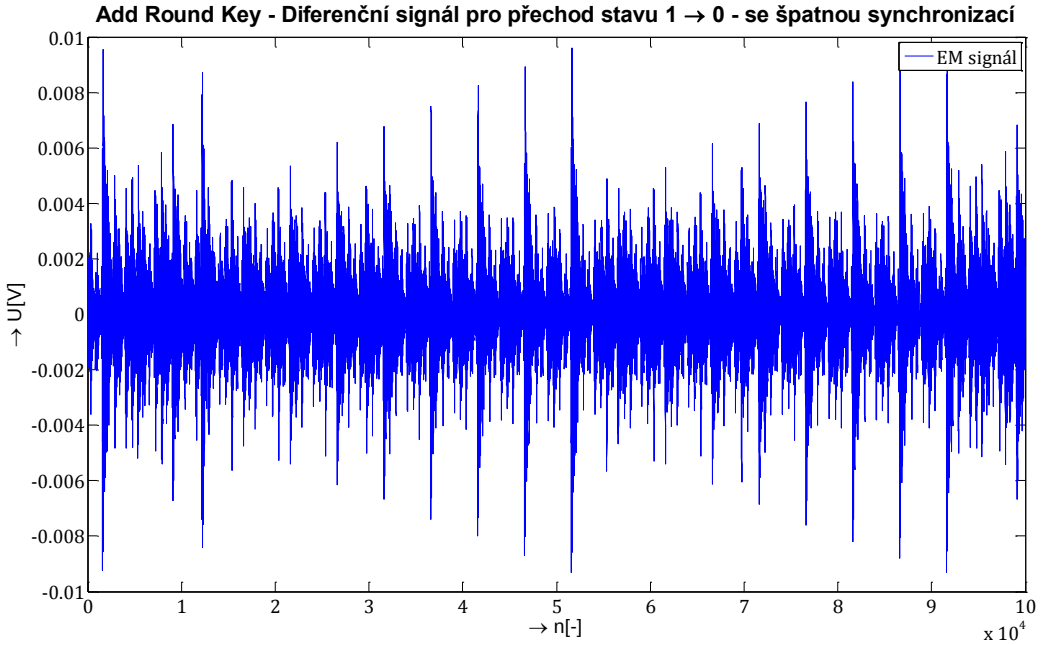


Obr. 5.8: Demonstrace vlivu šumu ve snímacím - Acquisition módu.

Synchronizace

Synchronizační signál byl odebírán z výstupu RB0, který byl nastaven na změnu hodnoty podle registru PORTB 0. Výhodou tohoto řešení bylo, že výstup RB0 byl zároveň nastaven tak, aby při hodnotě 1 rozsvěcel LED diodu na vývojovém kitu a při hodnotě 0 LED diodu zhasnul, tudíž bylo okamžitě možné vizuálně kontrolovat podle intenzity svícení dané LED, jestli byl daný program funkční.

Synchronizace je velmi důležitá především pro zpracování signálů, zvláště pak pro vytváření diferenčních signálů. Pokud nejsou dva signály naprosto dokonale časově synchronizovány, pak je prakticky nemožné provést jakoukoliv matematickou analýzu signálu. Demonstrace důležitosti synchronizace je na obr. 5.9, ve kterém došlo k posunutí jednoho ze signálů oproti druhému o deset vzorků. Při zachování správné synchronizace, by měl být průběh stejný jako na obr. 5.4. Pokud osciloskop ukládá pouze jednotlivé data bez informace o čase, pak je nutné dbát na správnou synchronizaci. Pokud však osciloskop ukládá k datům z jednotlivých kanálů i informaci o čase, synchronizace je pak snazší. Popřípadě je důležité dát si pozor na synchronizaci na nástupnou resp. sestupnou hranu, při jejichž přepínání v rámci jednoho měření, by osciloskop vytvářel vzájemně posunuté časové osy.

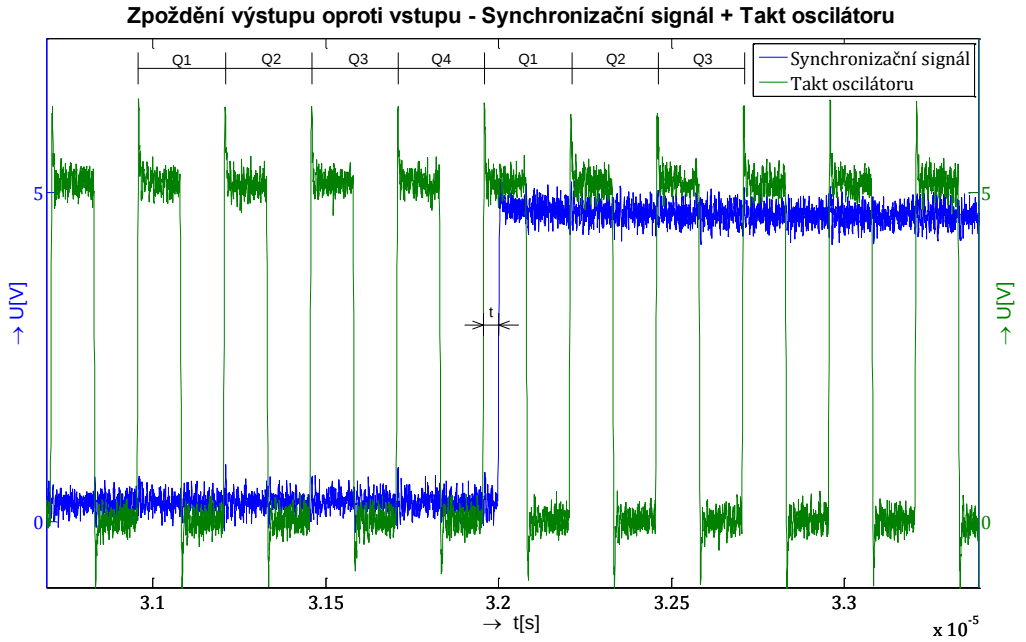


Obr. 5.9: Diferenční signál špatně synchronizovaných signálů.

Zpoždění

Zpoždění výstupu za vstupem mikroprocesoru, bylo teoreticky probráno v kapitole 3.1 Zpoždění výstupů měřeného mikroprocesoru, lze prakticky jednoduše odzkoušet pomocí zobrazení taktovacího signálu a synchronizačního signálu do jednoho grafu viz obr. 5.10. Z grafu je jasně patrné, že zapsání hodnoty do registru, které probíhá pro každou instrukci ve čtvrtém taktovacím cyklů Q4, je o interval t opožděné oproti vstupnímu taktu, hodnota je do registru zapsána až během dalšího intervalu Q1. Zpoždění měřeného mikroprocesoru PIC 16F84A t je 44 ns. S tímto zpožděním by bylo nutné počítat např. pokud by se prováděla analýza EM průběhu instrukcí, v závislosti synchronizace na taktu oscilátoru, kdy by se celý naměřený EM průběh musel o dané

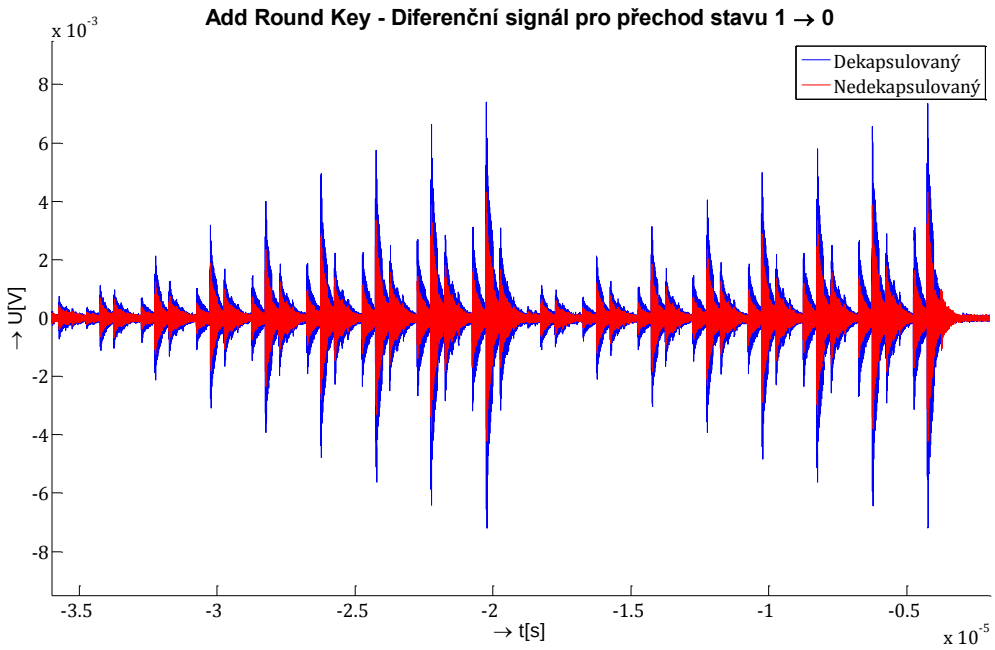
zpoždění posunout dopředu, aby korespondoval s průběhem oscilátoru. Protože v této práci probíhá porovnávání signálů podle synchronizačního signálu, který je rovněž výstupem mikroprocesoru, pak za předpokladu, že všechny výstupy jsou zpožděné stejně, nehrozí desynchronizace signálu.



Obr. 5.10: Zpoždění výstupu mikroprocesoru oproti vstupu.

Vliv dekapsulace mikroprocesoru na měření

Podle teoretických předpokladů uvedených v kapitolách 2.1, resp. 2.2, by měl být patrný rozdíl v úrovních napětí, při měření na nekapsulovaném a nedekapsulovaném mikroprocesoru. Toto měření bylo prováděno tak, že sonda byla vždy přiložena co nejtěsněji na povrch pouzdra nejdříve dekapsulovaného a poté i nedekapsulovaného mikroprocesoru. Při porovnání obou průběhů viz obr. 5.11, je patrné, že v diferenčních průbězích k výrazně velké změně nedochází. Jediné co přítomnost pouzdra mikroprocesoru ovlivňuje, je celková úroveň napětí indukovaná v cívce. To ovšem souvisí se vzdáleností měřicí cívky od zdroje EM pole, kdy intenzita EM pole se vzdáleností od zdroje záření exponenciálně klesá (viz dále v textu). Izolace mikroprocesorů je vyrobena typicky z plastu, který je z magneticky i elektricky nevodivého materiálu, takže vliv izolační vrstvy na EM pole je téměř identický jako vliv vzduchu. Pokud srovnáme úrovně nejvyšších napěťových špiček, pak zjistíme, že nejvyšší špička pro dekapsulovaný mikroprocesor má velikost napětí 7,39 mV, a pro mikroprocesor s pouzdrem je úroveň nejvyšší špičky v průběhu 4,31 mV.



Obr. 5.11: Porovnání EM průběhů při měření na nedekaps. a dekaps. procesoru.

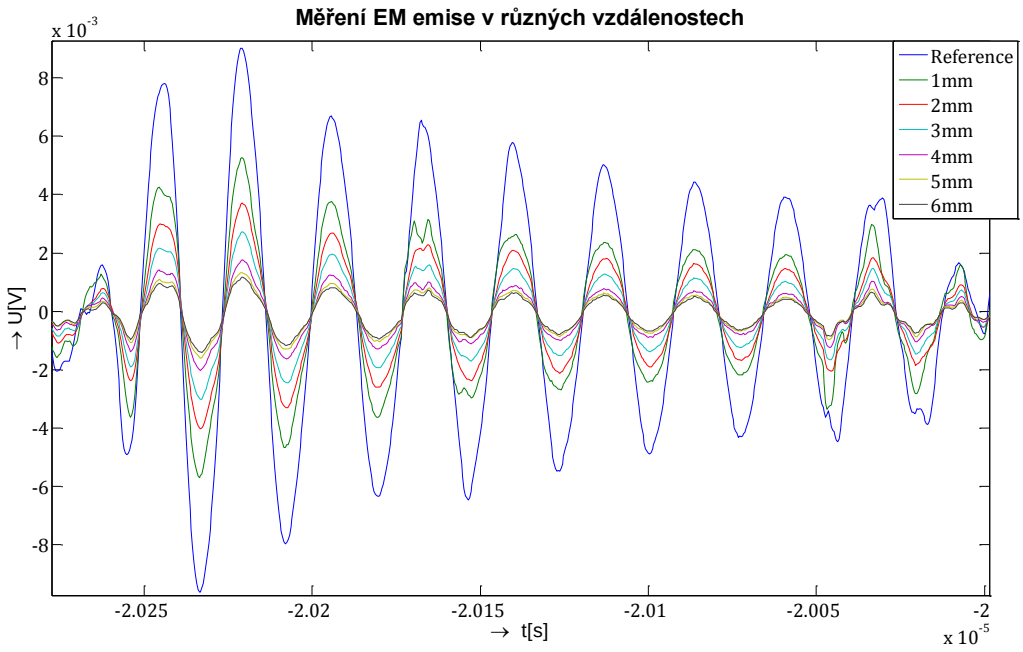
Vliv vzdálenosti měřicí cívky od mikroprocesoru na úroveň signálu

V tomto měření byly změřeny úrovně indukovaného napětí v cívce v závislosti na vzdálenosti měřicí cívky od povrchu mikroprocesoru. Za referenční polohu je považována poloha, kdy byla měřicí cívka přiložena natěsno na povrch dekapsulovaného mikroprocesoru. Poté byla zvyšována svislá výška sondy od mikroprocesoru. V každém kroku měření byla snaha umístit sondu v dané výšce do místa, ve kterém byla úroveň vyzařování nejvyšší.

Na obrázku 5.12 je zobrazen detail nejvyšší napěťové špičky, měřeného průběhu. Z průběhů je patrné, že velikost indukovaného napětí s rostoucí vzdáleností měřicí cívky od povrchu mikroprocesoru klesá exponenciálně. V tabulce 5.2 jsou uvedena naměřená maxima napěťových špiček pro jednotlivé vzdálenosti.

Tab. 5.2: Závislost úrovně indukovaného napětí na vzdálenosti.

Vzdálenost [mm]	Indukované napětí [mV]
Reference	9,064
1	5,260
2	3,712
3	2,725
4	1,758
5	1,322
6	1,185

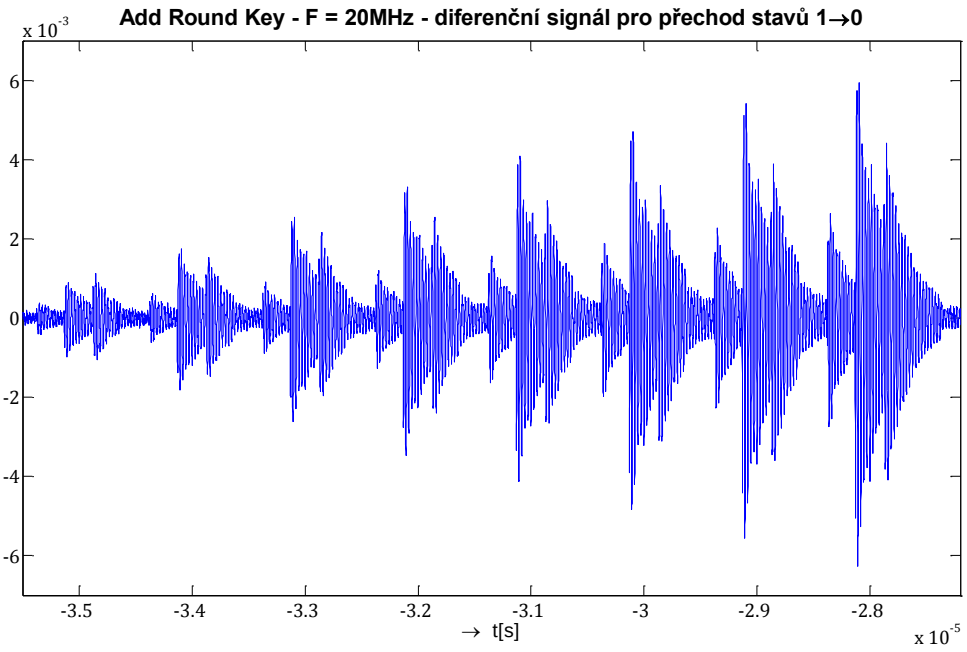


Obr. 5.12: Měření EM emise v různých vzdálenostech.

Z grafu vyplývá, že pro měření intenzity EM pole je žádoucí, aby snímací aparát byl k sledovanému zařízení umístěn co nejblíže. V tomto konkrétním případě lze předpokládat, že měření realizovaná v této práci na dekapsulovaném mikroprocesoru by byla s úspěchem proveditelná i na nedekapsulovaném mikroprocesoru nebo smart kartě. Při odstranění pouzdra dostáváme lepší výsledky. Obecně však úspěšnost realizace EM útoku záleží na konkrétním zařízení (na použitých součástkách) a implementaci konkrétního protokolu. Dále pak na kvalitě snímacího aparátu a popř. řetězce úpravy signálu před jeho zpracováním, kdy je možné zařadit do cesty například filtry nebo předzesilovače signálu.

Vliv frekvence taktovacího oscilátoru na měření

Cílem této části bylo prozkoumat, jaký zvolit oscilátor pro následná měření jednotlivých instrukcí a šifrovacího algoritmu standardu AES. Všechna dosavadní měření byla realizována se zařazeným oscilátorem s taktovací frekvencí 4 MHz. Měření, jehož výstup je uveden na obr. 5.13, bylo realizováno obdobným způsobem jako měření předchozí, s tím rozdílem, že byl použit 20 MHz oscilátor. Jak je vidět, tak při taktovací frekvenci 20 MHz jsou instrukce více ovlivněny pipeliningem, než při taktovací frekvenci 4 MHz. Proto následující měření budou prováděna s 4 MHz oscilátorem, u kterého byly výsledky transparentnější.

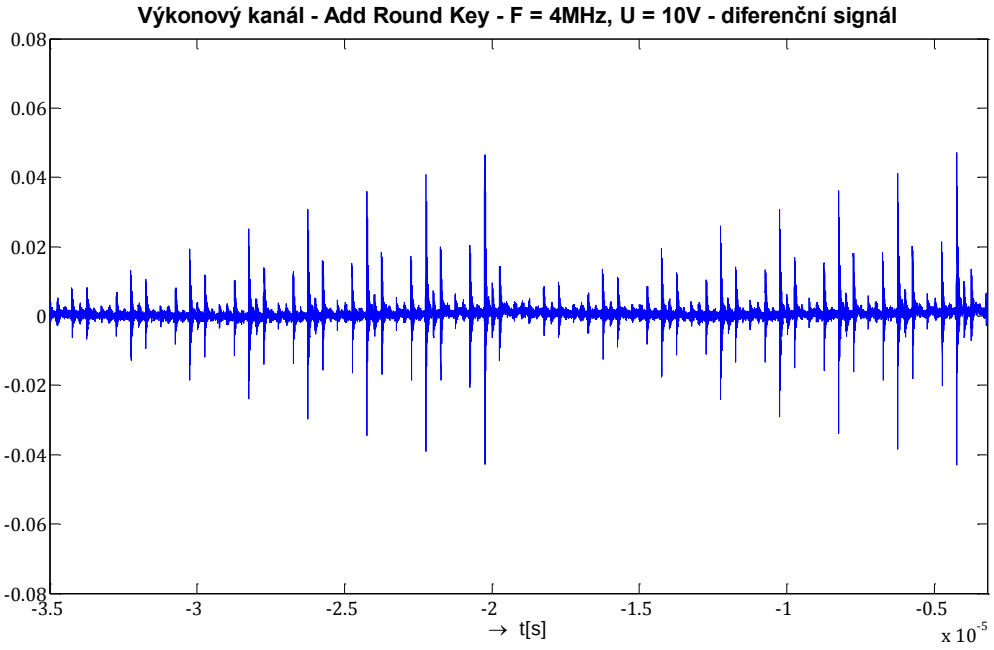


Obr. 5.13: Diferenční signál pro 20 MHz oscilátor.

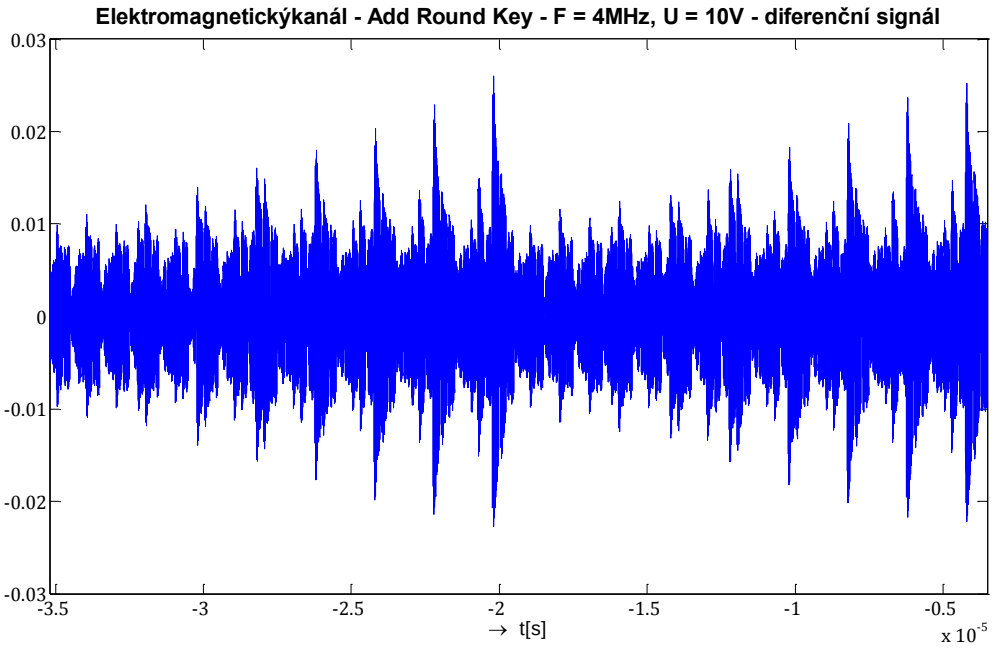
5.1.2 Porovnání elektromagnetického a výkonového průběhu

Cílem této části měření bylo vzájemně porovnat průběhy EM postranního kanálu a výkonového postranního kanálu ve stejných podmínkách. Nevýhodou bylo, že výkonový postranní kanál při napájecím napětí 5 V a taktovací frekvenci 4 MHz, které jsou v celé této práci používány pro měření EM postranního kanálu, nevykazoval v podstatě žádné diference v naměřených průbězích pro měnící se klíč. Diference byly však postřehnutelné, pokud se napájecí napětí mikroprocesoru přebudilo na hodnotu 10 V. Tento stav je zachycen na obr. 5.14. Napěťový signál byl změřen na rezistorovém 47 Ω bočníku, zařazeném v sérii k napájecímu napětí na jiné zkušební desce (sestrojené v rámci diplomové práce jednoho z kolegů, který realizoval útok výkonovým postranním kanálem). Tento průběh je možné srovnat s elektromagnetickým diferenčním signálem, který je pro stejné napájecí napětí - 10 V a taktovací frekvenci 4 MHz zobrazen na obr. 5.15. Velkou nevýhodou druhé zkušební desky bylo, že neměla možnost zapojení programátoru. Proto při měření signálu EM postranního kanálu docházelo v průběhu měření pro různé klíče ke změnám polohy snímací sondy, protože bylo nutné přenášet mikroprocesor do desky PICDEM™ 2 PLUS z důvodů změny programů pro jednotlivé klíče. Tento fakt tak přímo způsobuje poměrně velké zašumění v diferenčním průběhu, jelikož referenční hodnota nebyla přesná. Bohužel nebylo možné porovnat průběhy s EM průběhem, při uvedeném napájecím napětí, přímo v desce PICDEM™ 2 PLUS, protože zvýšená hodnota napájecího napětí by se na vývojové desce mohla negativně projevit. Proto porovnání výkonového a elektromagnetického kanálu má spíše informativní

charakter. Faktem však zůstává, že při dvojnásobném zvýšení napájecího napětí se napětí indukované v měřicí cívce EM pole více než 3x zvětšilo.



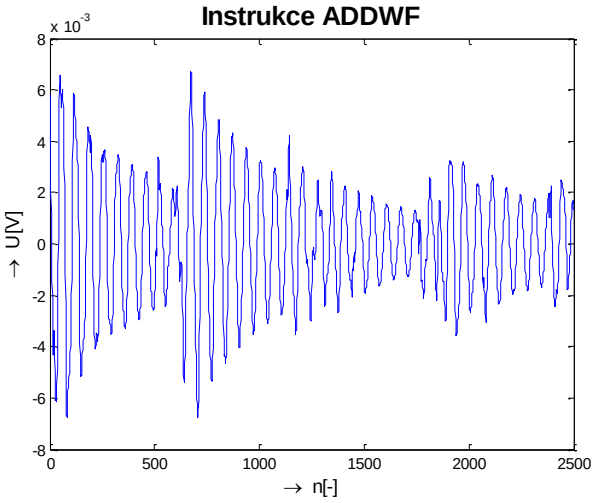
Obr. 5.14: Diferenční signál pro výkonový postranní kanál.

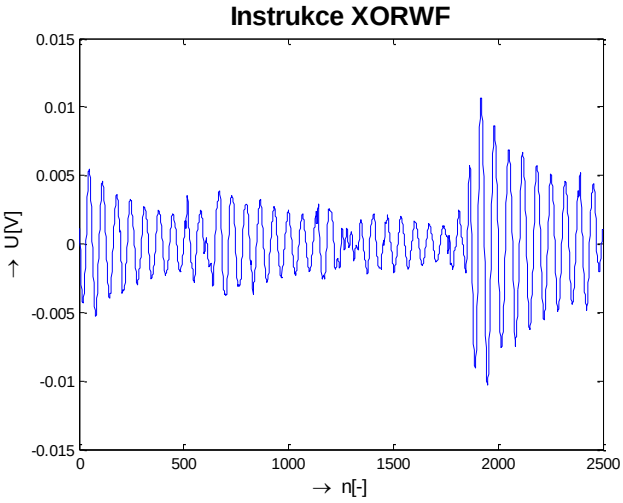


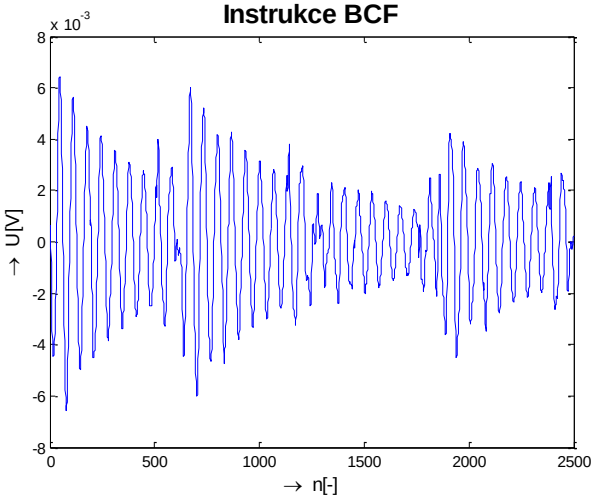
Obr. 5.15: Diferenční signál pro elektromagnetický postranní kanál.

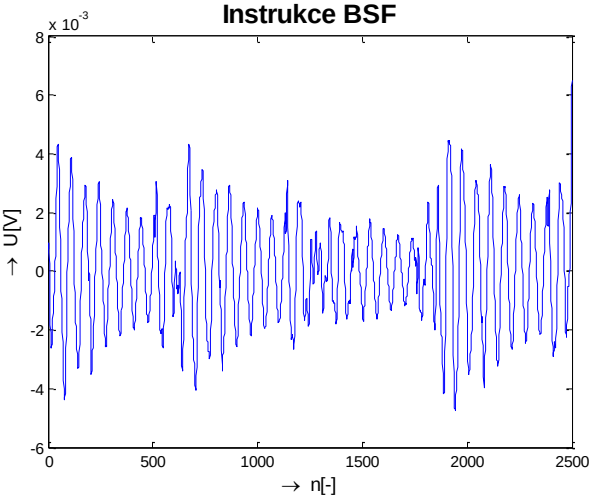
5.2 Analýza EM průběhu jednotlivých instrukcí

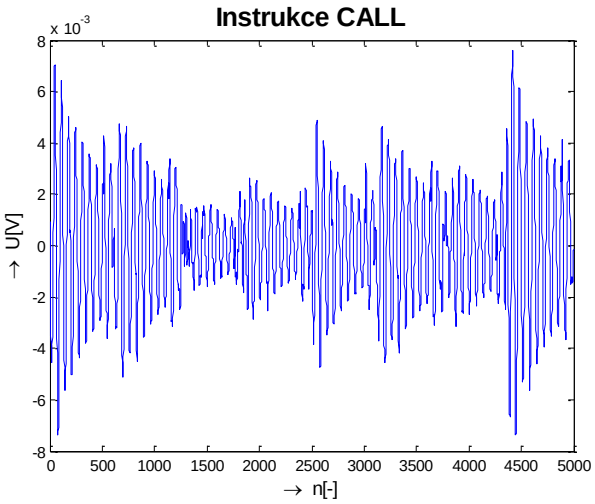
V této části byly postupně analyzovány EM průběhy pro jednotlivé instrukce, teoreticky probrané v kapitole 3.1. Synchronizace byla v tomto měření provedena na nástupnou hranu, což ovšem nehraje podstatnou roli. Ostatní nastavení osciloskopu bylo zachováno, vzorkovací frekvence byla 2,5 GSa/s. Na následujících čtrnácti obrázcích jsou zachyceny EM průběhy jednotlivých instrukcí a celkového cyklu. Program, na kterém bylo zkoumáno provádění instrukcí, je vložen v příloze A.2 pod názvem *Cykl*.

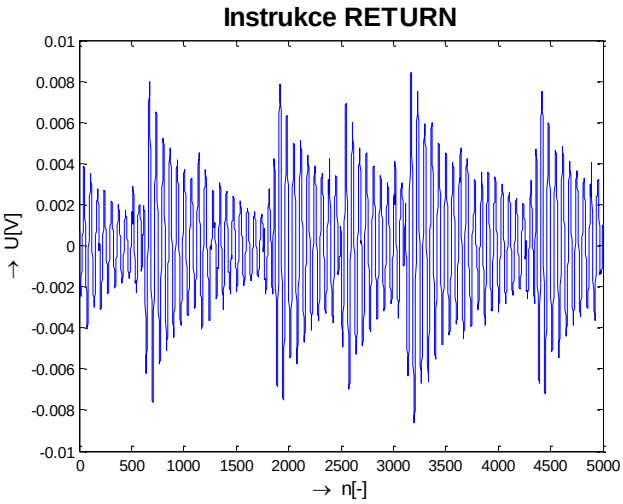


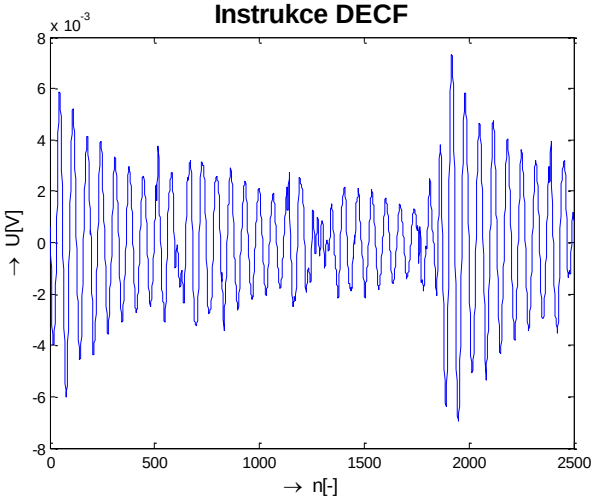


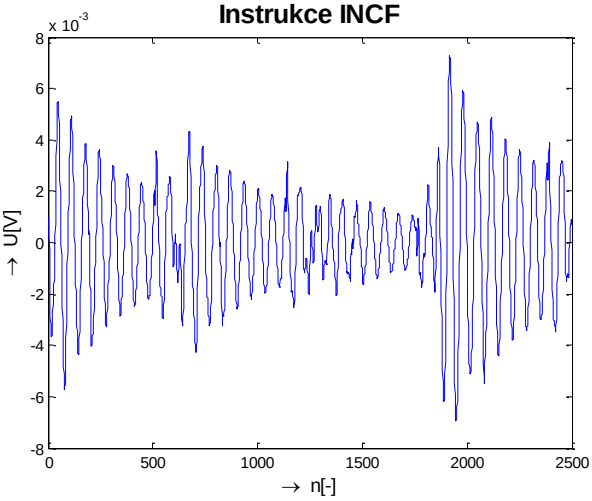


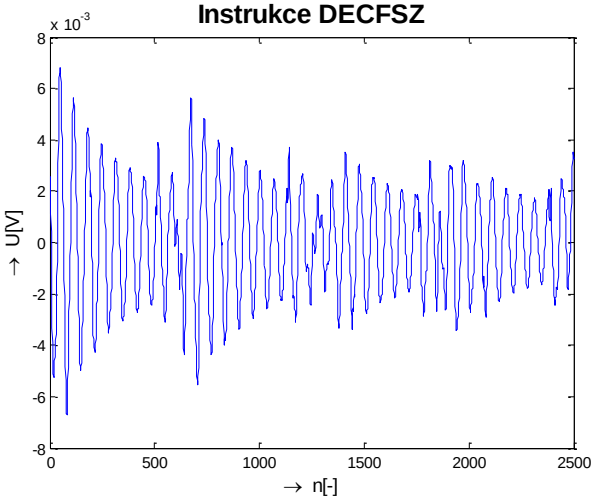


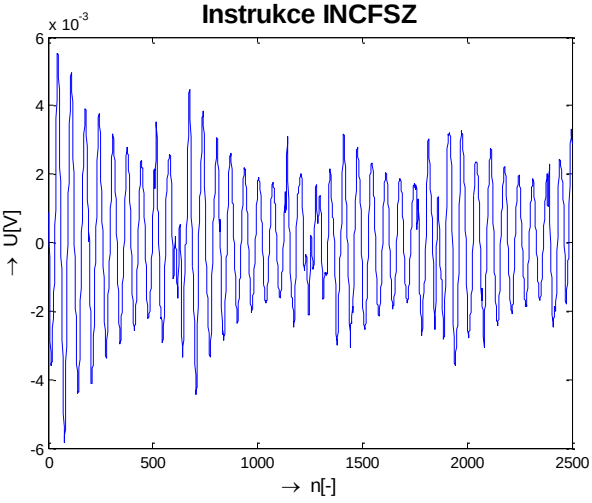

Instrukce CALL
x 10^-3
→ U[V]
→ n[-]

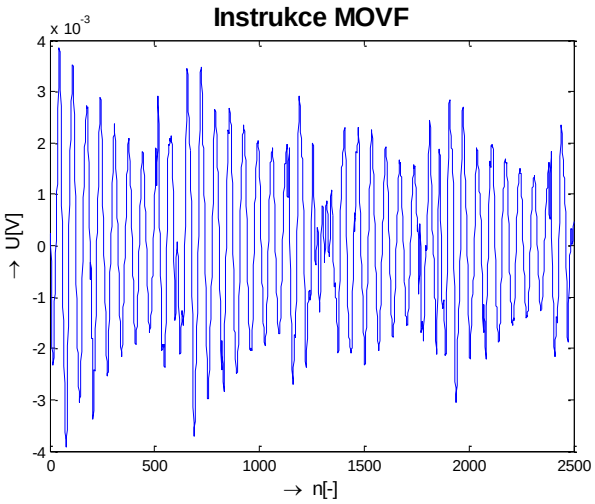

Instrukce RETURN
→ U[V]
→ n[-]

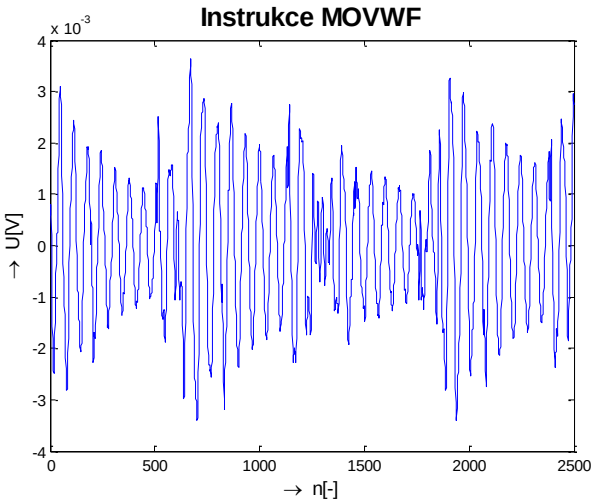

Instrukce DECF
x 10^-3
→ U[V]
→ n[-]

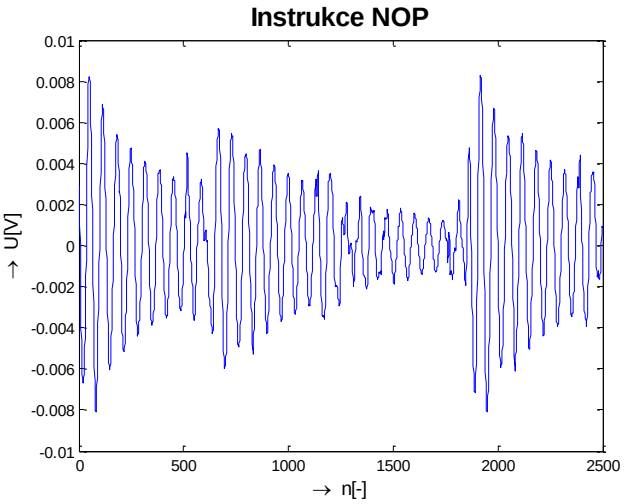

Instrukce INCF
x 10^-3
→ U[V]
→ n[-]

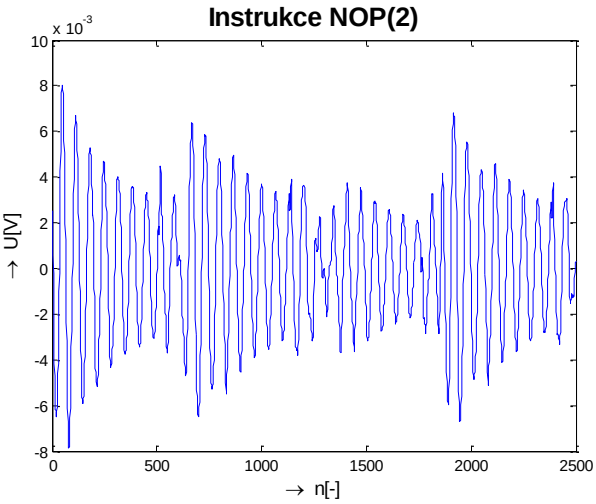

Instrukce DECFSZ
x 10^-3
→ U[V]
→ n[-]

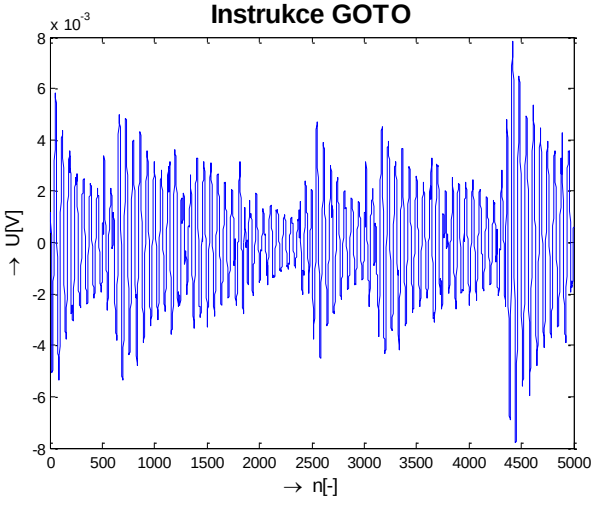

Instrukce INCFSZ
x 10^-3
→ U[V]
→ n[-]

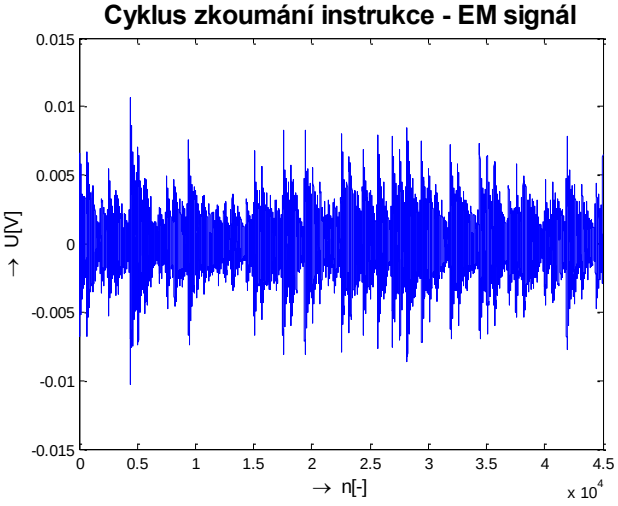

Instrukce MOVF
x 10^-3
→ U[V]
→ n[-]


Instrukce MOVWF
x 10^-3
→ U[V]
→ n[-]


Instrukce NOP
→ U[V]
→ n[-]


Instrukce NOP(2)
x 10^-3
→ U[V]
→ n[-]


Instrukce GOTO
x 10^-3
→ U[V]
→ n[-]


Cyklus zkoumání instrukce - EM signál
→ U[V]
→ n[-]
x 10^4

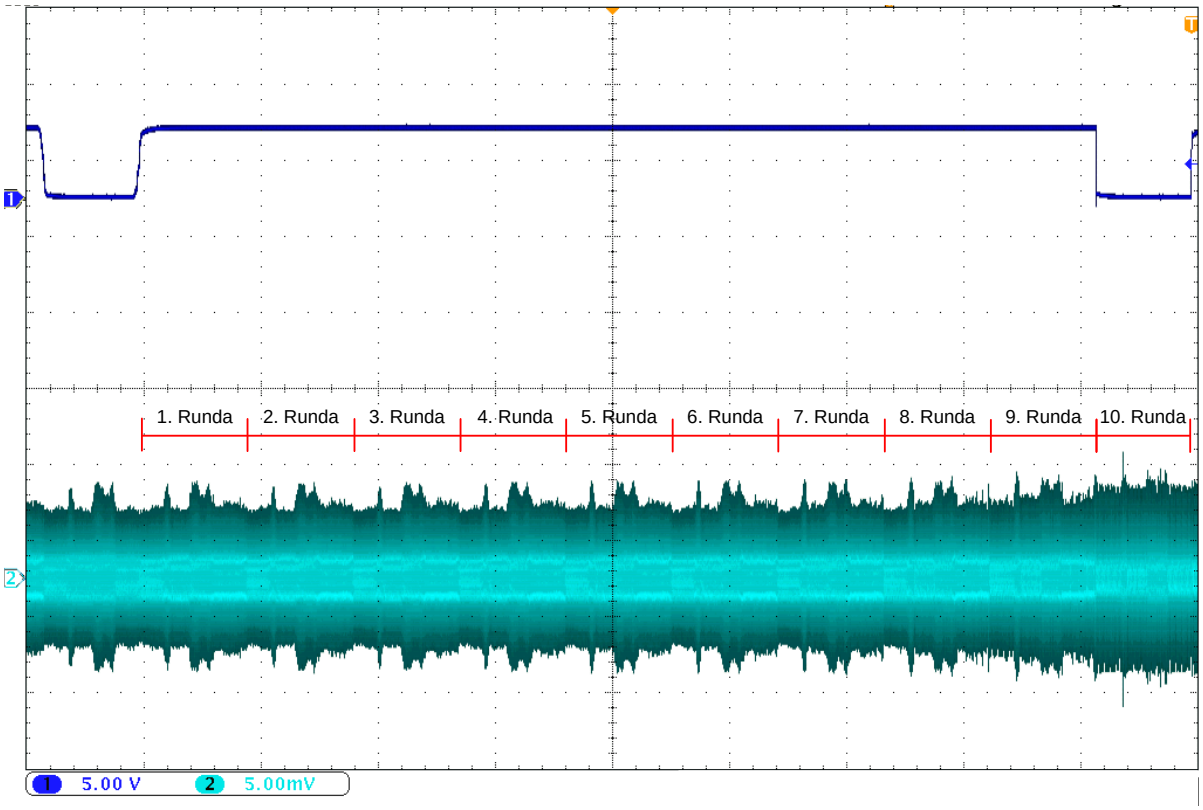
Jednotlivé instrukce jsou zobrazeny vždy pro jeden instrukční cyklus na ose x (ve vzorcích), kdy 2500 vzorků odpovídá časovému intervalu 1 µs. Všechny instrukce jsou jednocyklové s výjimkou instrukcí `Call`, `Return` a `Goto`, které jsou dvoucyklové. Při zobrazení jednotlivých instrukcí v čase, lze pozorovat rozdíly mezi jednotlivými instrukcemi, ale některé instrukce jsou v časové i ve frekvenční oblasti velmi podobné. Zároveň je z naměřených průběhů na první pohled patrné, ve kterých okamžicích nastává změna jednotlivých fází Q1 ÷ Q4. Nevýhodou je, že díky zřetězení instrukcí je poslední část aktuálně prováděné instrukce částečně ovlivněna i první části následující instrukce, což analýzu a rozpoznání jednotlivých instrukcí ztěžuje. K zpětné identifikaci jednotlivých instrukcí by bylo vhodné využít například neuronové sítě, která by se podle předložených vzorů naučila podobu jednotlivých instrukcí. Tato problematika však není cílem této práce.

5.3 Analýza EM průběhu AES

Tato kapitola se zaměřuje na popsání chování šifrovacího algoritmu AES-128 jako celku a také se zaměřuje na jeho jednotlivé rundy a části rund popsaných v kapitole 3.2. Program na šifrování a dešifrování AES, který je uveden v elektronické příloze, byl vytvořen Edim Permadim [30]. Tento program byl pouze upraven do takové podoby, že do něho byly vloženy synchronizační informace umožňující snadnější zobrazení EM průběhu na osciloskopu.

Zkoumání šifrovacího algoritmu AES-128

Nejprve je na oscilogramu obr. 5.16 zobrazen celkový EM průběh algoritmu AES vytvořený osciloskopem. Tento průběh nebyl zpracován v programu Matlab, protože na zachycení celého časového intervalu algoritmu AES bylo potřeba odebrat 10^6 vzorků, což bylo na zpracování velmi náročné. Pro měření bylo použito funkce průměrování Averaging 256. Při menších počtech průměrování docházelo k zhoršení rozlišovací schopnosti jednotlivých rund. Sestupná hrana synchronizačního signálu – kanál 1 – tmavě modrá barva, odpovídá začátku finální 10. rundy šifrování AES, následující nástupná hrana označuje konec jednoho cyklu šifrování.

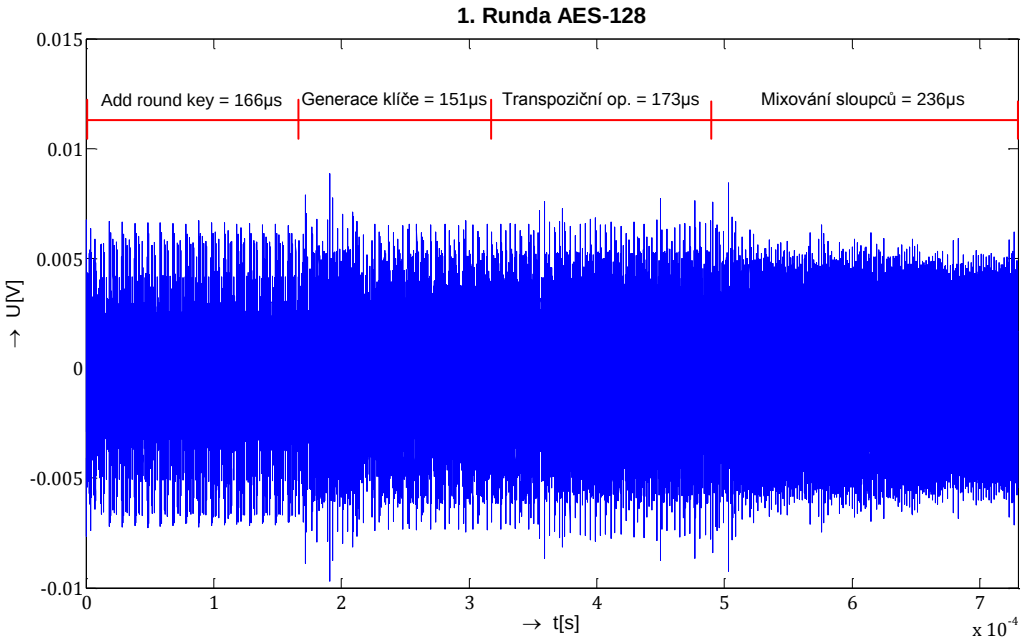


Obr. 5.16: EM průběh šifrovacího cyklu AES.

V obrázku 5.16, lze jednoznačně rozeznat jednotlivé rundy šifrovacího algoritmu AES. Dále je patrné, že finální desátá runda je o málo kratší, než předchozí rundy jedna až devět.

Analýza první rundy šifrovacího algoritmu AES-128

V první řadě je potřeba uvést, že pro potřeby měření bylo upraveno pořadí jednotlivých operací v rundách, oproti uspořádání podle obr. 3.4, uvedeného kapitole 3.2, kde je nejprve provedena inicializační operace Add Round Key a poté začíná první runda. V tomto měření byla inicializační Add Round Key považována za část první rundy, která končí s mixováním sloupců. V každé rundě byl ještě před transpozičními operacemi vypočítán klíč pro další rundu. Operace tedy byly v jednotlivých rundách prováděny v mírně pozměněném pořadí. V desáté rundě byla operace Add Round Key prováděna dvakrát. Jednou na začátku této rundy a podruhé na jejím konci. Žádný z výše uvedených faktů však neměl žádný vliv na správnou funkčnost šifrovacího algoritmu. Jednotlivé průběhy byly získávány se vzorkovacím kmitočtem 1,25 GSa/s.

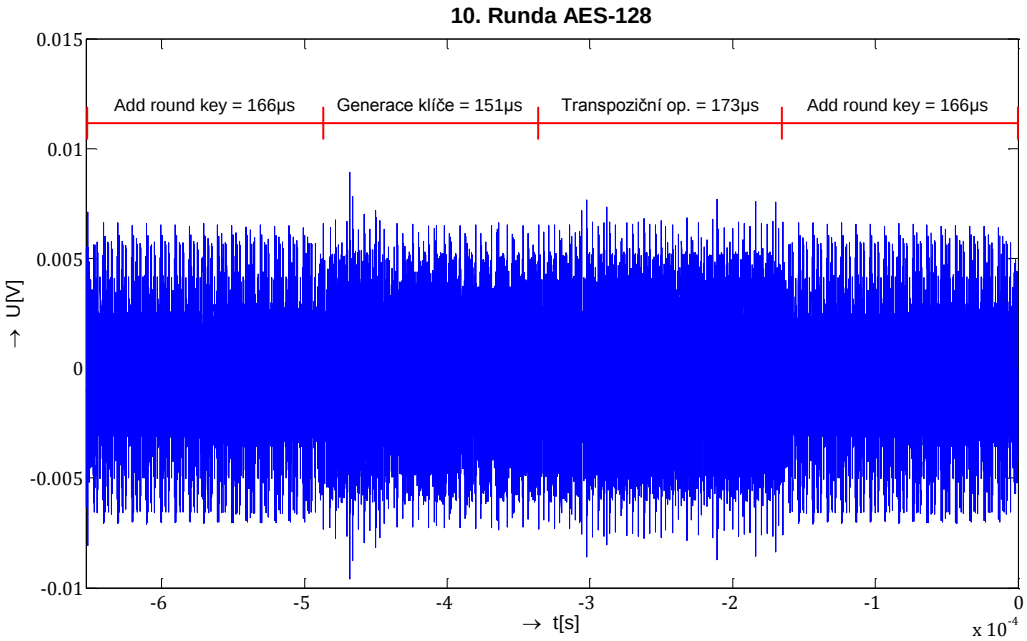


Obr. 5.17: EM průběh 1. rundy šifrování AES-128.

Na obr. 5.17 je vidět zobrazený průběh první rundy šifrovacího algoritmu AES. Hrubé obrysy jednotlivých fází jsou vidět i pouhým okem. Přesnější rozpoznání by však mělo proběhnout spíše na úrovni jednotlivých instrukcí. Jak bylo uvedeno výše v textu, první runda začíná operací xor klíče se stavy. Tato operace u této implementace šifrování AES trvá 166 µs. Následuje operace generace subklíče, která je kvůli nedostatku paměťového místa na mikroprocesoru prováděna v každém cyklu a nedochází k výpočtu všech rundovních subklíčů před začátkem, ale v průběhu jednotlivých rund šifrování. Tato fáze se může a nemusí v algoritmu takto objevit, záleží na konkrétní implementaci šifrovacího algoritmu. V tomto případě trvá generace klíče 151 µs. Následují transpoziční operace substituce bytů a posouvání bytů v řadě. Provádění transpozičních operací trvá 151 µs. Poslední operací je mixování sloupců, která je poměrně náročná a sama trvá 236 µs. Celková doba trvání jedné rundy této konkrétní implementace šifrovacího algoritmu AES-128 je 726 µs.

Analýza poslední rundy šifrovacího algoritmu AES-128

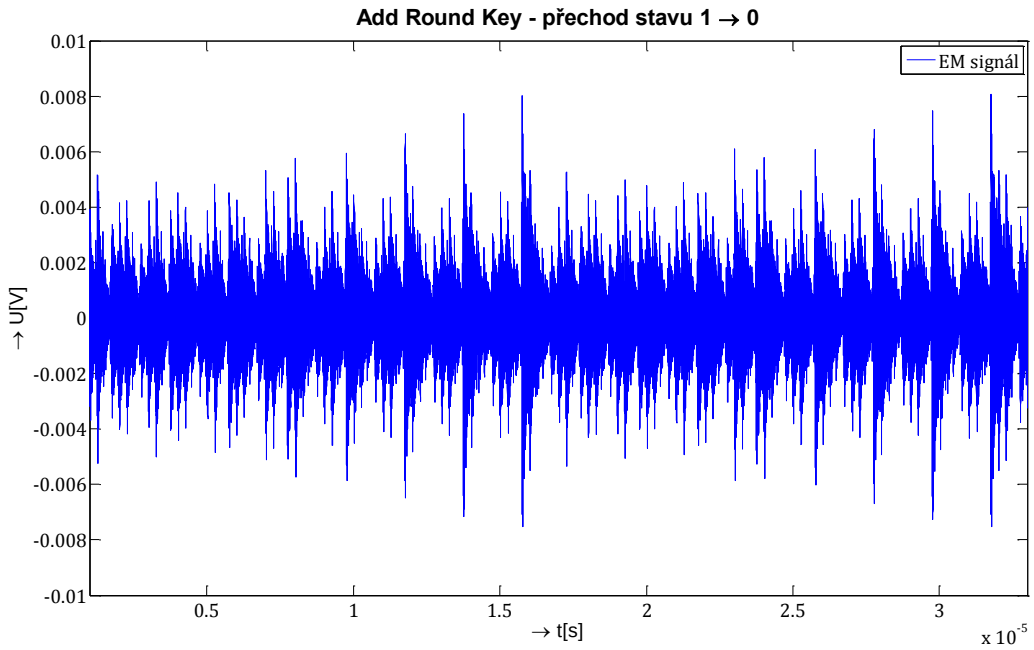
Poslední runda šifrovacího algoritmu AES-128 oproti předchozím nemá operaci mixování sloupců, proto je tato runda kratší, v této konkrétní implementaci však dochází ke dvojí operaci xor klíče a stavů. Celková doba trvání finální rundy je 656 µs viz obr. 5.18. Při porovnání fáze generace klíče i operací Add Round Key v první a poslední rundě, tedy v obr. 5.17 a obr. 5.18 jsou EM průběhy vzájemně velmi podobné.



Obr. 5.18: EM průběh 10. rundy šifrování AES-128.

5.4 Jednoduchá EM Analýza

Následující dvě kapitoly vycházejí z teoretického rozboru výkonové analýzy a EM analýzy uvedených v kapitolách 1.5, resp. 1.6. Cílem SEMA je vizuální analýza změřeného průběhu. Při dostatečných znalostech a zkušenostech s měřením EM pole u šifrovacích standardů a znalosti konkrétní implementace lze při pohledu na obr. 5.17 a obr. 5.18., na první pohled odhadnout, ve které fázi rundy se provádí operace xor klíče se stavy, popřípadě i další operace. Dále při roztažení časové osy lze podrobněji zobrazit i samotný průběh fáze Add Round Key viz obr. 5.19. V tomto průběhu je vidět, že napěťové špičky v místech, kde dochází ke změně více jak 4 bitů v stavovém bytu, jsou poměrně dosti zřetelné. Při změně menšího počtu bitů stavu však nelze určit přesný počet bitů, který se mění. Analyzovaná část průběhu je překrytá šumem. Z výše uvedeného vyplývá, že SEMA sice může posloužit jako dostačující analytický nástroj, ale pouze na úrovni pozorování a pro zběžný popis prováděné operace nebo instrukce. V případě potřeby přesnějšího popisu a podrobnější analýzy chování sledovaného systému je vhodnější zvolit analýzu diferenciální.



Obr. 5.19: SEMA operace Add Round Key.

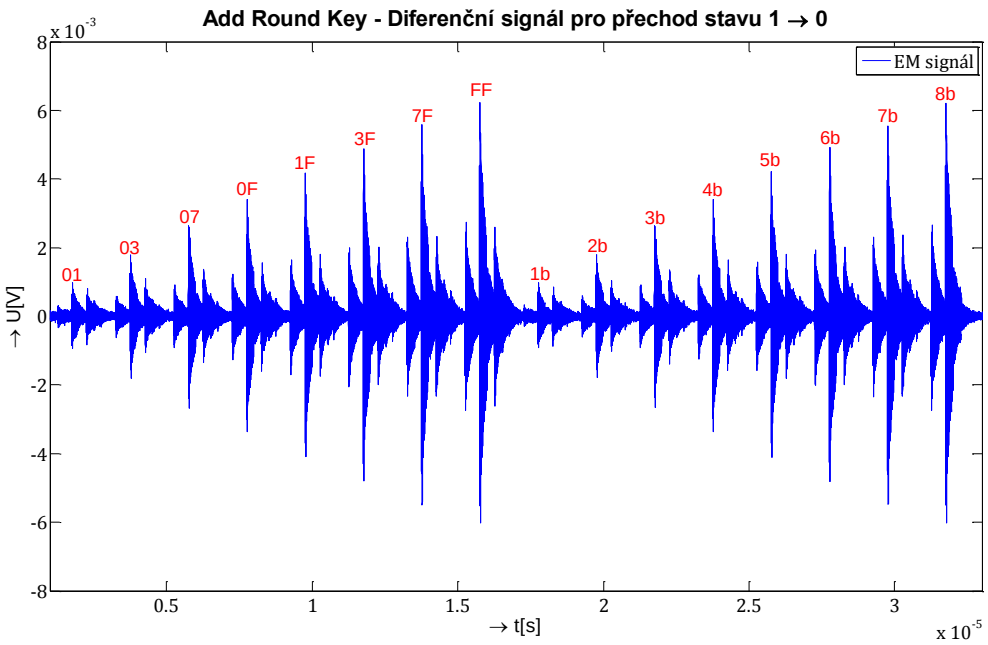
5.5 Diferenciální EM Analýza

K provedení DEMA (popř. i DPA), bylo potřeba průběžně sledovat úroveň EM záření v okolí zařízení a následně statisticky analyzovat sesbíraná data za účelem odhalení klíče. V kapitole 3.2.1 je teoreticky popsán model Hammingovy váhy klíče. V této kapitole byla realizována diferenciální elektromagnetická analýza funkce xor klíče $k_0 \div k_{15}$ se stavy $s_0 \div s_{15}$. Program s níže nastavenými hodnotami klíče a stavů, byl v předchozích měřeních prováděn jako demonstrační, nyní bude vysvětlen jeho praktický význam pro EM analýzu. Hodnoty klíče a stavů jsou vyjádřeny hexadecimálně, výsledek funkce xor klíče se stavy je na třetím řádku.

Klíč:	01 03 07 0F	1F 3F 7F FF	01 03 07 0F	1F 3F 7F FF
Stavy:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF
XOR:	FE FC F8 F0	E0 C0 80 00	FE FC F8 F0	E0 C0 80 00

Při operaci xor se změní tolik stavových bitů, kolik má klíč bitů rovných jedné[5]. Tomu odpovídá počet tranzistorů, které jsou sepnuty nebo rozepnuty pro uložení nového výsledku. V tomto případě má klíč Hammingovu váhu 72. Nejprve byla změřena EM trasa pro uvedené stavy a rostoucí klíč. Následně byla změřena EM trasa pro stejné počáteční stavy, ale nulový klíč. Po odečtení těchto dvou průběhů, byl vytvořen diferenční průběh, viz obr. 5.20.

[5] Platí pro situaci, kdy jsou všechny stavy nastaveny buďto na 0 nebo na 1



Obr. 5.20: DEMA operace Add Round Key.

Na obr. 5.20 je patrné rostoucí napětí indukované v měřicí cívce. Toto napětí je přímo úměrné počtu bitů klíče, které mají hodnotu 1. Následně bylo provedeno obdobné měření, s hodnotami uvedenými níže. Tento klíč je zajímavý v tom, že se sice od předchozího klíče hodnotami liší, výsledek funkce xor se liší, ale Hammingova váha klíče je stejná. Stejně tak i rozložení počtu jedniček v jednotlivých bytech je stejné jako u předchozího klíče, proto jeho diferenční průběh byl shodný s průběhem na obr. 5.20.

Klíč:	80 C0 E0 F0	F8 FC FE FF	80 C0 E0 F0	F8 FC FE FF
Stavy:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF
XOR:	7F 3F 10 0F	07 03 01 00	7F 3F 10 0F	07 03 01 00

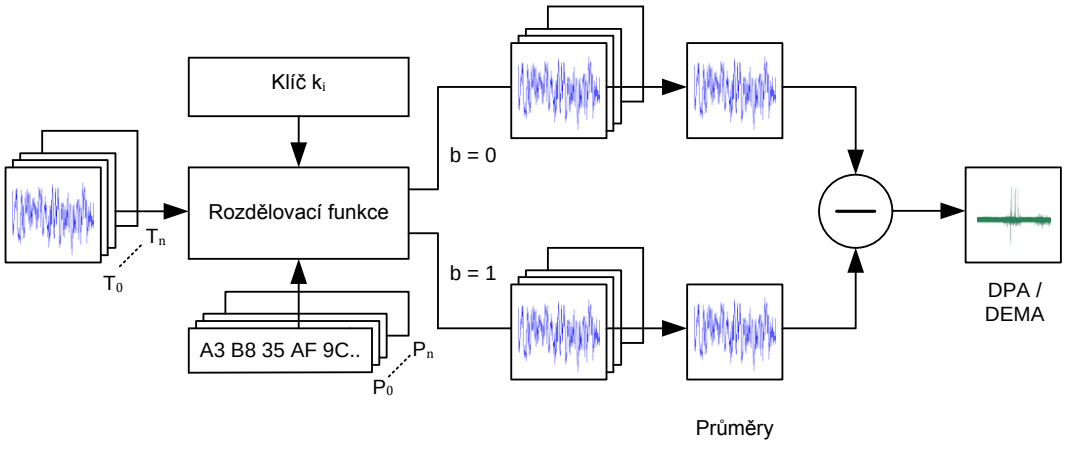
Nyní, pokud známe Hammingovu váhu klíče, je možné si vygenerovat všechny možné klíče pro daný počet jedniček a zkusit zprávu prolomit pomocí bruteforce útoku.

Pokud vyjdeme ze statistiky, tak celkový počet možných klíčů pro AES–128 je 2^{128}, což je přibližně 3,403 x 10^{38}. Pro toto konkrétní uspořádání, kdy víme, že v prvním bytu klíče je pouze jeden bit rovný 1, ve druhém bytu jsou dva bity rovné 1 atd., je možné vytvořit 5,975 x 10^{23} klíčů, což je o téměř 15 řádů méně.

Sofistikovanější metoda DEMA

Matematický základ této sofistikovanější metody DEMA je popsán v kapitole 1.5, resp. 1.6.. V této kapitole je vysvětlena její praktická realizace na standardu AES podrobněji.

Uvažujme následující situaci: Chceme zjistit první byte klíče AES-128. Jelikož víme, že klíč je před provedením první rundy nejprve xorován s prvním bytem stavu, zaměříme se právě na operaci xor, která odpovídá fázi Add Round Key. Sadu otevřených textů, které jsou vyjádřeny počátečními stavy upravíme tak, aby měly pro první stavový byte náhodný charakter a zbylých 120 bitů stavu ponecháme. Toto uspořádání zaručuje, že diferenční průběhy, které budou vytvářeny, budou vykazovat diferenci pouze v místech, kde bude pracováno právě s prvními osmi bity stavu (které se náhodně mění) a klíče (který je po celou dobu konstantní). Otevřené texty, které budou použity, uchováme pro pozdější zpracování. Následně změříme EM trasu na zařízení provádějící operaci Add Round Key v první rundě šifrování AES s připravenými otevřenými texty pro několik stovek až tisícovek opakování. Následně přistoupíme k zpracování naměřeného signálu. Nejdříve si EM průběh rozdělíme na jednotlivé části, prováděné pro jednotlivé otevřené texty. Tyto EM průběhy změřené pro konkrétní stavy, rozdělíme podle rozdělovací funkce zobrazené na obr. 5.21. A to tak, že podle odhadu klíče[6] K a osmi bitů otevřeného textu P určíme výstup funkce xor. Tento výstup vstupuje do substituční tabulky S-BOX, na jejímž výstupu dostáváme jinou osmibitovou kombinaci. Libovolný bit na výstupu substituční tabulky poslouží jako rozdělovací bit b, který je důležitou částí rozdělovací funkce. Podle hodnoty tohoto bitu rozdělíme naměřené EM průběhy do dvou skupin – pro bit b = 0 do podskupiny 0 a pro bit b = 1 do podskupiny 1. Toto rozdělení EM tras je potřeba provést pro všechny odhady klíče, u osmibitového klíče tedy 256krát. Poté již stačí obě vytvořené podskupiny pro jednotlivé odhady klíče zprůměrovat a průměry odečíst. V případě správného měření a zpracování, by u správného odhadu klíče měla mít diferenční špička nejvyšší hodnotu.

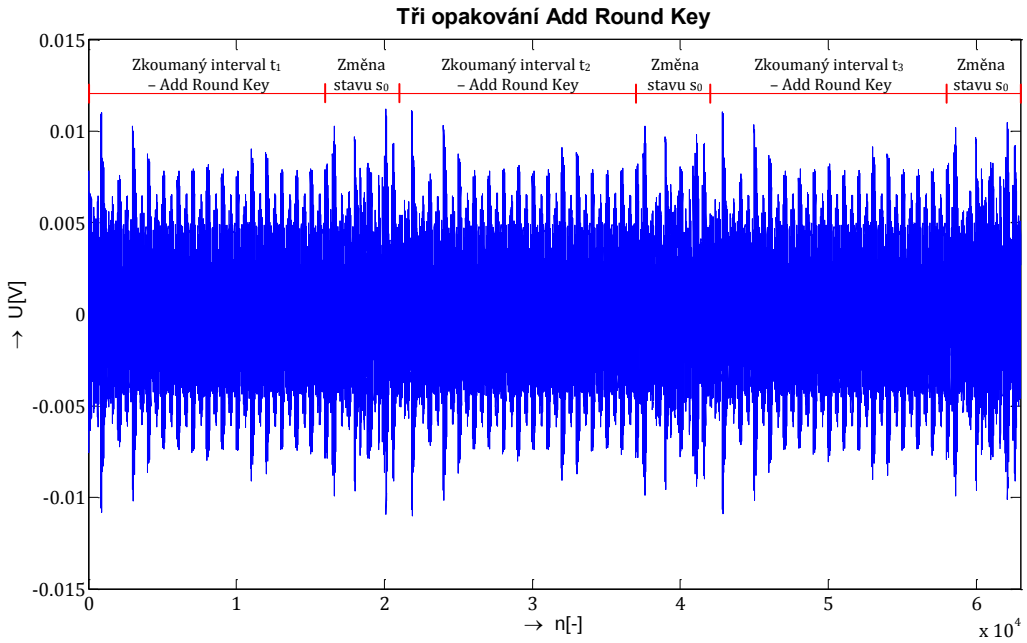


Obr. 5.21: Základní princip DEMA / DPA na standardu AES.

Program, který prováděl cyklické opakování operace Add Round Key, s prvním bytem klíče $F3_{hex}$ a ostatními bity klíče nulovými a s prvním stavovým bytem postupně

[6] Odhad klíče vyjadřuje vždy jeden konkrétní klíč, se kterým je aktuálně pracováno, v praxi je potřeba rozdělit průběhy pro všechny možnosti hodnot klíče, tedy pro klíč 00 až po klíč FF_{hex}

se měnícím od 00 $_{hex}$ do FF $_{hex}$ je uveden v příloze A.3 pod názvem *Program DEMA*. Princip, jakým má být signál zpracován, je zobrazen na obr. 5.22.



Obr. 5.22: Princip extrakce užitečných dat z cyklu.

Cílem je uložení a zpracování dat, která jsou pro náš cíl relevantní. Proto je v cyklu, který provádí 256 krát operaci xor, postupně pro měnící se stavy v rozsahu 00 ÷ FF$_{hex}$, důležitá fáze Add Round Key. Proto je praktické extrahovat data pouze ze zkoumaných intervalů a průběhy v intervalech odpovídající změnám stavů lze ignorovat. Pokud známe taktovací, resp. vzorkovací frekvence, pak by tento úkol neměl být příliš složitý. Ovšem realita je o mnoho složitější. Při tomto "sériovém" přístupu k věci, kdy jsou jednotlivé operace prováděny po sobě, dochází k postupné časové desynchronizaci jednotlivých průběhů, kdy jsou jednotlivé zkoumané intervaly díky nepřesné taktovací frekvenci oscilátoru vzájemně časově posunuty. Tento posuv není nijak výrazný, ale jak je popsáno v kapitole 5.1, i malý rozdíl v časovém posunu má na výsledek diferenční analýzy velmi velký dopad. Toto měření bylo provedeno celkem 2x, jednou s oscilátorem, podruhé pak s funkčním generátorem signálu generující obdélníkový taktovací signál o frekvenci 4 MHz, bohužel ani jednou nebylo možné naměřený signál správně rozdělit. Lepší výsledky by bylo možné obdržet např. při provedení automatizovaného "paralelního" měření, u kterého by osciloskop vždy každý průběh pro jednotlivý stav ukládal zvlášť pokaždé se stejnou časovou osou. Díky tomu by nedocházelo k vzájemnému posuvu jednotlivých průběhů.

6 MOŽNÁ PROTIOPATŘENÍ

Protiopatření proti elektromagnetické a výkonové analýze mají za úkol ztížit útočníkovi získání užitečné informace. Obecně se protiopatření dělí do dvou skupin. První skupina jsou protokolová protiopatření, která mají za cíl utajit příslušný protokol a dále se snaží v čase měnit protokol takovým způsobem, aby útočník nemohl zachytit dostatečné množství informace k odhalení některých utajovaných dat. Druhá skupina jsou implementační protiopatření, které implementují protokol takovým způsobem, aby nedocházelo k úniku užitečně informace.

Jelikož teoreticky je možné každý systém zabezpečit dokonale, záleží pouze vždy na ceně, kterou by dané zabezpečení stálo. V praxi je proto potřeba nalézt vhodný mix protokolových a implementačních protiopatření, které budou vykazovat nejlepší poměr ochrana/cena pro danou aplikaci. Tuto situaci lze přirovnat například k výběru šifrovacího standardu AES, kdy z možných návrhů rovněž nebyl vybrán nejbezpečnější návrh, ale návrh, který nejlépe splňoval požadavky na výkonnost, bezpečnost, náročnost, rychlost apod. V této práci nejsou popsány protokolová protiopatření, protože tato tématika je velmi obsáhlá.

6.1 Implementační protiopatření

Jak už bylo uvedeno v úvodu této kapitoly, implementační protiopatření se snaží implementovat daný protokol tak, aby za daných podmínek neunikala z postranního kanálu žádná informace a nebo tak, aby z této uniklé informace nebylo možné vyvodit správné závěry. Implementační protiopatření lze obecně rozdělit do dvou skupin, první skupina má za cíl ukrývání signálu, druhá skupina se pak signál snaží určitým způsobem maskovat.

6.1.1 Metody ukrývání signálu

Metody ukrývání signálu nemají schopnost zabránit útočníkovi v útoku, jeho snahu však mohou významně znesnadnit. Základní myšlenkou metod ukrývání signálu je převýšení užitečného signálu šumem. Principiálně lze toto provést několika způsoby.

Snížení úrovně vyzářeného signálu

Nejzákladnější protiopatření proti EM útokům je redukce vyzařovaného elektromagnetického pole pomocí stínění. Proto některé procesory bývají stíněny vrstvami mědi nebo hliníku.

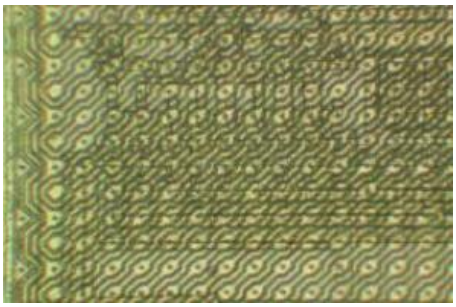
Dalším možným způsobem zamezení úniku EM záření je umístění sledovaného zařízení do Faradayovy klece. Toto řešení není z realizačního hlediska nejpraktičtější, navíc téměř každé zařízení vyžaduje externí napájení, popřípadě taktovací signál a další kontakty, takže činnost Faradayovy klece by v reálném případě nebyla ideální. Navíc lze

předpokládat, že by bylo nutné učinit rozsáhlé úpravy v procesu návrhu i výroby takovýchto zařízení. Toto protiopatření je vhodné zavést až v případě, kdy zpracovávané informace by měli skutečně klíčový význam.

Zvýšení úrovně vyzářeného neužitečného signálu

Opačným přístupem ke ztížení získání informace z postranního kanálu, ale se stejným cílem je zvýšení úrovně EM pole v okolí zařízení za pomocí vodivé mřížky, protékané proudem náhodné a nejlépe proměnné hodnoty. Velikost proudu protékající mřížkou by měla být vyšší než hodnota proudu v procesoru. Použití přídavné mřížky má za následek emitaci proměnného EM pole, které ztíží lokalizaci potenciálně užitečného signálu.

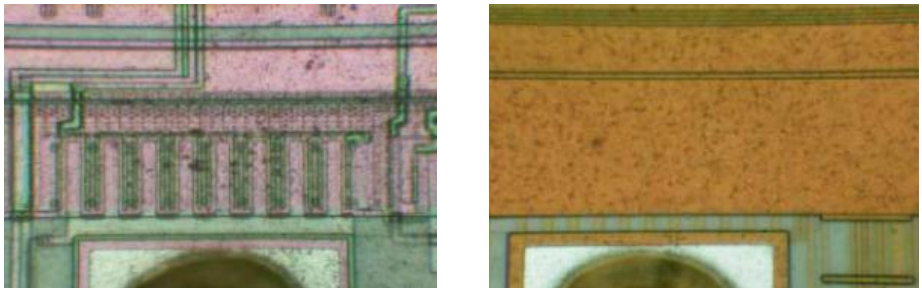
V praxi se využívá třeba mřížka implementovaná ve vrchní části mikroprocesoru, která se skládá z prokládaného vzoru zemnícího a napájecího přívodu. Výhodou je, že pokud je tato mřížka narušena, nebo nastane vodivé spojení země s napájecím přívodem, zařízení přestává fungovat. Tento způsob se využívá jako opatření proti invazivním útokům a v případech, kdy je vhodnější znehodnotit vlastní zařízení, než ztratit citlivá data.



Obr. 6.1: Mřížka složená z napájecích a zemnících vodičů.

Použití moderních výrobních technologií

Postupem času dochází k změnám výrobní technologie. V dřívějších dobách bylo relativně snadné vizuálně analyzovat povrch mikročipu a pomocí zpětného inženýrství zjistit jeho obvodové řešení. Příklad je uveden na obr. 6.2 a), kde je zobrazena druhá vrstva mikročipu, kterou lze snadno pozorovat po odstranění primární vrstvy. V moderních obvodech viz obr. 6.2 b), je každá vrstva vytvořena planárním nárůstem po chemicko-mechanickém leštění předchozí vrstvy. Proto je mnohem složitější odhalit obvodové řešení nižších vrstev. To totiž vyžaduje mechanické nebo chemické odstranění vyšších vrstev.



a) b)

Obr. 6.2: Porovnání výrobních technik mikroprocesorů PIC.

Návrh obvodů s nízkou spotřebou

Tento způsob protiopatření proti EM útokům vychází z myšlenky snížení výkonu, který zařízení spotřebovává při zpracovávání informace. Způsoby, kterými lze snižovat spotřebu zařízení je mnoho. Jednou z nich je například technika SOI (Silicon On Insulator) - Silikon na izolaci, která využívá k výrobě mikroprocesoru vrstvových silikon-izolátor-silikonových substrátů na rozdíl od klasických silikonových substrátů. Výsledkem je snížení vlivu parazitních kapacit s následným zvýšením výkonnosti polovodičového zařízení. Zvýšení výkonu zařízení má za následek snížení jeho spotřeby a snížení výkonu vyzářeného ve formě tepla i vyzářeného EM pole.

Desynchronizace

Tato metoda desynchronizuje jednotlivé prováděné instrukce. Synchronní procesory mají díky svému taktování v ohledu bezpečnosti nevýhodu. Jejich taktovací signál, který má tvar obdélníku, obsahuje velmi velké množství harmonických. Následně je díky tomu možné určit frekvenci, na které procesor pracuje a zasynchronizovat se na ni. V tomto směru mají asynchronní procesory velkou výhodu, protože nevyžadují vstup taktovacího signálu, jejich spektrum je výrazně jiné, než u synchronních procesorů a tím je velmi těžko analyzovatelné. Proto je výhodné softwarově zavádět různá zpoždění v době výpočtu, nebo v průběhu provádět různé cykly a instrukce, které nemají se zpracovávanou informací žádnou spojitost. Tato protiopatření jsou podrobněji popsána v pracích [30,31].

Zavedení duální logiky

Tato metoda spočívá ve snaze vyrovnávat jednotlivé přechody v zařízení nebo v přenosové cestě, což vede k nižší emisi EM pole. Každý drát je nahrazen dvoudrátovým spojem. Oba přenášejí informaci tak, že každý z nich má určitý stav. Pár vodičů musí být vyvážený. V praxi se často využívá například metod duální logiky SABL nebo WDDL. Největší potíží těchto metod je právě zajištění vyváženosti obou párů. K zajištění vyváženosti obou vodičů musejí být zachovány např. i kapacitní vazby mezi vodičem a

čipem. Proto nestačí, že jsou vodiče identické, ale identické musí být i jejich okolí – stínění apod. [32,33,34]

6.1.2 Metody maskování signálu

Maskování signálu se prakticky projevuje tak, že výkonová spotřeba zařízení je nezávislá na hodnotách citlivých dat, jelikož datům je před jejich zpracováním změněn charakter na náhodný. Příkladem maskování je právě provedení operace xor mezi stavy a klíčem, kdy s daty není pracováno přímo, ale je provedeno jejich kombinování s klíčem, který představuje masku. Pokud útočník následně zachytí unikající informace při zpracovávání dat, není tato informace pro něho čitelná, protože nezná příslušnou masku. Informace, která uniká z jednotlivě změřených tras při implementaci maskování, není výrazně jiná než u trasy bez maskování. Rozdíl je v tom, že každá trasa obsahuje informaci o maskované hodnotě a o její masce, přičemž jednu nelze odhalit bez znalosti té druhé. Některé nedokonalosti, ke kterým dochází při funkci mikroprocesoru a které mohou ohrozit bezpečnost systému, jsou popsány dále v textu.

Krátkodobé změny signálu

Standardní logické tranzistory mění své výstupy při každé změně vstupní hodnoty. V praxi tak některé tranzistory spínají několikrát během jednoho časového taktu. Příkladem může být, pokud je potřeba provést složitější operace, například násobení výsledku po operaci xor. V praxi tato operace bude prováděna v několika krocích, přičemž při jejím provádění se v průběhu výpočtu na výstupu budou zobrazovat i některé přechodné stavy, které mohou vést k úniku informace postranním kanálem.

Více informací a podrobností o moderních způsobech zaváděných protiopatření je uvedeno v literatuře [35,36,37].

7 ZÁVĚR

Cílem diplomové práce bylo navrhnout a sestavit pracoviště pro měření nežádoucího elektromagnetického záření z mikročipu PIC. Dále pak navrhnout a zhotovit měřicí sondu a otestovat její vlastnosti. Pomocí této sondy následně prozkoumat vliv odstranění pouzdra čipu na úroveň vyzařování. Další část práce se měla zabývat analýzou jednotlivých instrukcí a analýzou chování čipu při provádění vybraného šifrovacího standardu.

Ke správnému navržení měřicího pracoviště a ostatních aspektů nutných, k úspěšné realizaci útoku postranním elektromagnetickým kanálem bylo nejprve nutné prozkoumat teoretické základy elektromagnetické a výkonové analýzy a také principy vyzařování elektromagnetického pole v okolí zařízení protékaných elektrickým proudem. Stejně tak bylo nutné prostudovat základní vlastnosti mikroprocesorů PIC a také popsat chování standardu AES. Všechny tyto poznatky jsou uvedeny v teoretické části této práce.

Na základě těchto poznatků byly navrženy a realizovány 4 různé sondy pro měření magnetické složky elektromagnetického pole. Z těchto sond byla vybrána sonda s nejlepšími mechanickými a měřicími vlastnostmi. Zároveň bylo navrženo i samotné měřicí pracoviště pro měření přímé emise mikroprocesoru PIC16F84A.

V praktické části nejprve proběhla analýza vlivu polohy snímací cívky vůči mikroprocesoru. Posléze byla vybrán vhodný snímací mód osciloskopu. Následně byl zjištěn vliv odstranění pouzdra mikroprocesoru a také vliv vzdálenosti měřicí cívky od mikroprocesoru na úroveň napětí indukovaného v měřicí cívce. Bylo zjištěno, že úroveň napětí indukovaného v cívce s rostoucí vzdáleností klesá exponenciálně. Zároveň bylo provedeno orientační porovnání elektromagnetického a výkonového postranního kanálu.

Při měření vybraných instrukcí bylo zjištěno, že jednotlivé instrukce se v časové oblasti vzájemně liší. Jejich hlubší porovnání však provedeno nebylo, jelikož díky zpracovávání instrukcí pomocí jejich zřetězení, dochází k vzájemnému ovlivňování jednotlivých instrukcí. Navíc fakt, že jednotlivé instrukce jsou tvořené čtyřmi různými fázemi zpracování, jejich zpracování ještě ztěžuje. K rozpoznání jednotlivých instrukcí by bylo nejspíše nejvhodnější využít neuronových sítí, které by se mohli jednotlivé vzory naučit a následně i rozpoznat.

Dále byla provedena analýza chování šifrovacího algoritmu standardu AES, u něhož byl nejprve změřen jeho celkový průběh a posléze byly podrobněji změřeny a popsány i jednotlivé rundy šifrování. Konkrétně pak runda první, která je shodná s dalšími osmi rundami a také runda desátá, která je oproti předchozím rundám zkrácená.

Nakonec byla provedena jednoduchá EM analýza SEMA a také diferenciální EM analýza DEMA, která demonstrovala únik informace o klíči postranním kanálem tzv. modelem Hammingovy váhy. Prakticky byla zjištěna Hammingova váha použitého klíče. Zároveň byla v textu popsána i metoda pro realizaci sofistikovanější metody DEMA, která vede k odhalení celého klíče. Pro tuto metodu byl vytvořen program pro realizaci měření na mikroprocesoru PIC16F84A a samotné měření bylo rovněž provedeno. Bohužel postup, kdy EM průběhy pro jednotlivé stavy byly zpracovávány po sobě, vedl k tomu, že následně nebylo možné vytvořit diferenční průběhy, jelikož jednotlivé průběhy byly vzájemně časově posunuty. K úspěšné realizaci této sofistikovanější metody DEMA by bylo vhodné měření realizovat jako automatizované, kdy by byly průběhy měřeny jednotlivě pro odpovídající otevřené texty. Vzájemná desynchronizace jednotlivých by proto nebyla problémem.

V závěru bylo provedeno shrnutí moderních protiopatření, která se postupně zavádějí do výrobních procesů tak, aby byly znemožněny útoky elektromagnetickými a výkonovými postranními kanály.

Seznam použité literatury

[1] ZHOU, Yong Bin; FENG, Deng Guo. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing. In [online]. Beijing, China : [s.n.], 2005 [cit. 2010-10-05]. Dostupné z WWW: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.100.8856&rep=rep1&type=pdf>.

[2] HAGAI, Bar-El. Introduction to Side Channel Attacks. In [online]. [s.l.] : [s.n.], [2005] [cit. 2010-10-05]. Dostupné z WWW:<http://www.discretix.com/PDF/Introduction%20to%20Side%20Channel%20Attacks.pdf>.

[3] KOCHER, Paul C. Timing Attacks on Implementations of Diffie - Hellman, RSA, DSS, and Other Systems. In [online]. San Francisco, USA : [s.n.], [1996] [cit. 2010-10-07]. Dostupné z WWW: <http://www.cryptography.com/public/pdf/TimingAttacks.pdf>.

[4] BONEH, Dan; DEMILLO, Richard A.; LIPTON, Richard J. On the Inportance of Eliminating Errors in Cryptographic Computations. In [online]. [s.l.] : [s.n.], 1997 [cit. 2010-10-10]. Dostupné z WWW:<http://saluc.engr.uconn.edu/refs/dfa/boneh97ontheimportance.pdf>.

[5] KUHN, Markus G. Optical Time-Domain Eavesdropping Risks of CRT Displays. In [online]. Cambridge, UK : [s.n.], 2002 [cit. 2010-10-10]. Dostupné z WWW: <http://www.computer.org/portal/web/csdl/doi/10.1109/SECPRI.2002.1004358>.

[6] TSUNOO, Yukiyasu, et al Cryptanalysis of DES Implemented on Computers with Cache. In [online]. Japan : [s.n.], 2003 [cit. 2010-10-10]. Dostupné z WWW: <http://www.computer.org/portal/web/csdl/doi/10.1109/SECPRI.2002.1004358>.

[7] TIU, Chin Chi A New Frequency-Based Side Channel Attack for Embedded Systems. In [online]. Waterloo, Ontario, Canada : [s.n.], 2005 [cit. 2010-10-13]. Dostupné z WWW: <http://optimal.vlsi.uwaterloo.ca/NEW/thesis_AgnesTiu.pdf>.

[8] AGRAWAL, Mukesh; KARMAKAR, Sandip; MUKHOPADHYAY, Debdeep. Scan Based Side Channel Attacks on Stream Ciphers and Their Counter-Measures. *Progress in cryptology : Indocript* [online]. 2008, [cit. 2010-10-15]. Dostupný z WWW: <http://www.springerlink.com/content/501614h05w036w30/>.

[9] QUISQUATER, Jean-Jacques Side Channel Attack - State of the art. In [online]. [s.l.] : [s.n.], 2002 [cit. 2010-10-22]. Dostupné z WWW: <http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel_report.pdf>.

[10] DANEČEK, Petr; BŘEZINA, Milan. Útok výkonovým postranním kanálem na hardwarový kryptografický modul. *Elektrorevue* [online]. 14.8.2006, 2006, 31, [cit. 2010-11-01]. Dostupný z WWW: <http://www.elektrorevue.cz/clanky/06031/index.html#DPA>.

[11] MATTHEWS, Adam Low Cost Attacks on Smart Cards The Electromagnetic Side-Channel. In [online]. [s.l.] : [s.n.], 2006 [cit. 2010-11-05]. Dostupné z WWW: <http://www.ngssoftware.com/Libraries/Documents/09_06_Low_Cost_Attacks_on_Smart_Cards_-_The_Electromagnetic_Side-Channel.sflb.ashx>.

[12] MCNAMARA, Joel. *The Complete, Unofficial TEMPEST Information Page* [online]. 2004, 2004 [cit. 2010-11-07]. Dostupné z WWW: <http://www.eskimo.com/~joelm/tempest.html>.

[13] GANDOLFI, Karine; MOURTEL, Christophe; OLIVIER, Francis Electromagnetic Analysis: Concrete Results . In [online]. France : [s.n.], 2001 [cit. 2010-11-10]. Dostupné z WWW: <http://www.springerlink.com/content/ead10k34v7q36d3w/>.

[14] AGRAWAL, Dakshi; ARCHAMBEAULT, Bruce; RAO, Josyula R.; ROHATGI, Pankaj: The EM Side–Channel(s). *Computer Science : Cryptographic Hardware and Embedded Systems – CHES 2002* [online]. 2003, 2003, [cit. 2010-11-12]. Dostupný z WWW: <http://www.springerlink.com/content/mvtxbq9qa287g7c6/fulltext.pdf>.

[15] KOC, Cetin K., et al. *Cryptographic Engeneering*. [s.l.] : Springer, 2009. 517 s. ISBN 978-0-387-71816-3.

[16] KOC, Cetin K.; NACCACHE, David; PAAR, Christof. *Cryptographic Hardware and Embedded Systems - CHES 2001 : Third International Workshop*. Paris, France : [s.l.] : Springer, 2001. 411 s. ISBN 3-540-42521-7.

[17] ATTALI, Isabelle; JENSEN, Thomas. *Smart Card Programming and Security*. Cannes, France : [s.n.], 2001. 267 s. ISBN 0302-9743.

[18] QUISQUATER, Jean-Jacques; SAMYDE, David. *Computer Science : Smart Card Programming and Security* [online]. [s.l.] : [s.n.], 2001 [cit. 2010-11-15]. ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards , s. 200 – 210. Dostupné z WWW: <http://www.springerlink.com/content/chmydkq8x5tgdrce/>.

[19] SALEH, Baaha E.A.; TEICH, Malvin C. *Základy fotoniky*. 1. [s.l.] : [s.n.], 1994. 205 s. ISBN 80-85863-01-4.

[20] PEETERS, Eric; STANDAERT, Francoi-Xavier; QUISQUATER, Jena-Jacques Power and Electromagnetic Analysis: Improved Model, Consequences and Comparisons. In [online]. Belgium: [s.n.], 2006 [cit. 2010-11-20]. Dostupné z WWW: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.1619&rep=rep1&type=pdf>.

[21] DEUTSCHMANN, Bernd; PITSCH, Harald; LANGER, Gunter Near Field Measurements to Predict the Electromagnetic Emission of Integrated Circuits. In [online]. [s.l.] : [s.n.], [2007] [cit. 2010-11-20]. Dostupné z WWW: <http://www.langer-emv.de/fileadmin/website/dokumente/fachbibliothek/en_NFM-Emission-Integrated-Circuits.pdf>.

[22] A, MICROCHIP. 18-pin Flash/EEPROM 8-Bit Microcontrollers. In [online]. [s.l.] : [s.n.], 1998. Dostupné z WWW: <http://ww1.microchip.com/downloads/en/devicedoc/30430c.pdf>.

[23] PIC16F84A Data Sheet. *Microchip Technology Inc*. 2001, 1, s. 1-86. Dostupný také z WWW: <http://ww1.microchip.com/downloads/en/devicedoc/35007b.pdf>.

[24] JOAN, Daemen; VINCENT, Rijmen. AES Proposal: Rijndael. [online]. 1997, [cit. 2011-03-16]. Dostupný z WWW: <http://www.nist.gov/CryptoToolkit>.

[25] Federal Information Processing Standards Publication 197 : ADVANCED ENCRYPTION STANDARD (AES). *A* [online]. 26.11.2001, 1, [cit. 2011-03-16]. Dostupný z WWW: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

[26] ZABALA, Enrique. [online]. Montevideo, Uruguay : 2004 [cit. 2011-03-22]. RIJNDAEL CIPHER 128-bit version (data block and key) Encryption. Dostupné z WWW: <http://www.cs.bc.edu/~straubin/cs381-05/blockciphers/rijndael_ingles2004.swf>.

[27] CHOUINARD, Jean-Yves. Notes of the Advanced Encryption Standard (AES). *Design of Secure Computer Systems* [online]. 2002, [cit. 2011-03-22]. Dostupný z WWW: <http://www.site.uottawa.ca/~chouinar/Handout_CSI4138_AES_2002.pdf>.

[28] MICROCHIP. PICDEM™ 2 Plus Demonstration Board User's Guide. [online]. 2006, [cit. 2011-03-22]. Dostupný z WWW: <http://ww1.microchip.com/downloads/en/DeviceDoc/PICDEM_2_Plus_Users_Guide_51275c.pdf>.

[29] TEKTRONIX. DPO4032 Oscilloscope. *A* [online]. 2008, [cit. 2011-03-22]. Dostupný z WWW: <http://www2.tek.com/cmswpt/psdetails.lotr?ct=PS&cs=psu&ci=13408&lc=EN>.

[30] PIC MICROCONTROLLER MATH LIBRARY METHODS [online]. 2011 [cit. 2011-04-01]. PIC Microcontoller Math Library Methods. Dostupné z WWW: <http://www.piclist.com/techref/microchip/math/index.htm>

[31] DAEMEN, Joan; RIJMEN, Vincent. Resistance Against Implementation Attacks A Comparative Study of the AES proposal. [online]. 1999, [cit. 2011-04-08]. Dostupný z WWW: <http://cr.yp.to/bib/1999/daemen.pdf>.

[32] GEBOTYS, C.H.; TIU, C.C.; CHEN, X. A Countermeasure for EM Attack of a Wireless PDA. *IEEE Computer Society*. 2005, s. 1-6. Dostupný také z WWW: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1428519&tag=1>.

[33] QUISQUATER, Jean-Jacques; SAMYDE, David. ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards . *Computer Science : Smart Card Programming and Security* [online]. 2001, Volume 2140, [cit. 2011-04-02]. Dostupný z WWW: <http://www.springerlink.com/content/chmydkq8x5tgdrce/>.

[34] TUNSTALL, Michael. Attacks on Smart Cards. In [online]. [s.l.] : Gemplus, 2003 [cit. 2011-04-02]. Dostupný z WWW: <http://www.cs.bris.ac.uk/home/tunstall/presentation/AttacksonSmartCards.pdf>.

[35] MANGARD, Stefan. Side-Channel Attacks in the Presence of Countermeasures. *Chip Card, Security Innovation Group* [online]. 17.2.2010, [cit. 2011-04-05]. Dostupný z WWW: <http://www.lorentzcenter.nl/lc/web/2010/383/presentations/Mangard.pdf>.

[36] BUTTYÁN, Levente. Tamper resistant devices. [online]. 2010, [cit. 2011-04-05]. Dostupný z WWW: <http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/slides-hsm.pdf>.

[37] LOMNE, Victor. Power & Electro-Magnetic Side-Channel Attacks: Threats and Countermeasures. [online]. 7.7.2010, [cit. 2011-04-05]. Dostupný z WWW: <http://www.lirmm.fr/~lomne/slidesPhDdefenseVictorLomne.pdf>.

Seznam použitých zkratek

ADM – Amplitude Demodulator – amplitudový demodulátor

AES – Advanced Encryption Standard – pokročilý šifrovací standard

CLK – Clock – Hodinový signál

CMOS – Complemetary Metal-Oxide Semiconductor – nejrozšířenější současná technologie výroby polovodičů

CPU – Central Processing Unit – Centrální procesorová jednotka

CRT – Cathode Ray Tube – CRT monitor

DEMA – Differential Electromagnetic Analysis – diferenciální elektromagnetická analýza

DEMFA – Differential Electromagnetic-Frequency Analysis – diferenciální elektromagneticko - frekvenční analýza

DES – Data Encryption Standard – standard pro šifrování dat

DFA – Differential Frequency Analysis – diferenciální frekvenční analýza

DFT – Differential Design For Testability – návrhový vzor s možností testování sama sebe

DPA – Differential Power Analysis – diferenciální výkonová analýza

DPFA – Differential Power-Frequency Analysis – diferenciální výkonově – frekvenční analýza

DSA – Digital Signature Algorithm - šifrovací algoritmus pro digitální podpisy

EM pole – Electromagnetic field – elektromagnetické pole

FIB – Focused Ion Beam – fokzovaný iontový paprsek

HO-DPA – High Order Differential Power Analysis – diferenciální výkonová analýza vyššího řádu

IO – Integrovaný obvod

ISO – International Organization for Standardization – mezinárodní organizace pro standardizaci

LED – Light Emiting Diode – dioda emitující světlo

NIST – National Institute of Standards and Technology – národní institutu pro standardizaci a technologii

PA – Power Analysis – odběrová analýza

PC – Postition Counter – čítač pozice

PA – Personal Computer – osobní počítač

PDA – Personal Digital Assistant – osobní digitální pomocník

PDM – Phase Demodulator – úhlový demodulátor

PSD – Power Spectral Density – výkonová spektrální hustota

RSA - Rivest, Shamir, Adleman Cipher – asymetrický kryptografický algoritmus

SEMA – Simple Electromagnetic Analysis – jednoduchá elektromagnetická analýza

SCA – Side-Channel Attack – postranní kanálový útok

SCB – Side-Chain Based – postranní kanálový útok zkoumáním řetězce

SOI – Siilicon On Isolator – výrobní technika polovodičových součástek

SPA – Simple Power Analysis – jednoduchá výkonová analýza

TEMPEST – Transient Electromagnetic Pulse Emanation Standard – pracovní skupina vytvářející standardy a doporučení pro zařízení emitující EM pole

Seznam příloh