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

DIFERENCIÁLNÍ ELEKTROMAGNETICKÁ ANALÝZA

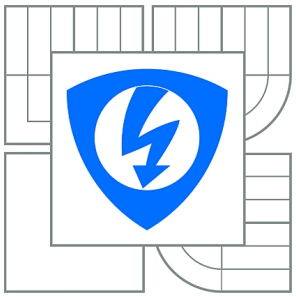
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. BOHUMIL NOVOTNÝ
AUTHOR

BRNO 2013

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

DIFERENCIÁLNÍ ELEKTROMAGNETICKÁ ANALÝZA

DIFFERENTIAL ELECTROMAGNETIC ANALYSIS

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

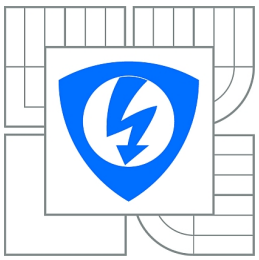
AUTOR PRÁCE — Bc. BOHUMIL NOVOTNÝ

AUTHOR

VEDOUCÍ PRÁCE — Ing. ZDENĚK MARTINÁSEK

SUPERVISOR

BRNO 2013



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Bohumil Novotný	***ID:***	119555
Ročník:	2	***Akademický rok:***	2012/2013

NÁZEV TÉMATU:

Diferenciální elektromagnetická analýza

POKYNY PRO VYPRACOVÁNÍ:

V rámci diplomové práce prostudujte problematiku elektromagnetického postranního kanálu. Pozorně prostudujte jednoduchou a diferenční elektromagnetickou analýzu. Realizujte experimentální pracoviště určené k analýze elektromagnetickým postranním kanálem. Pracoviště bude vybaveno vhodným vybavením umožňující přesné nastavení elektromagnetické sondy a mělo by být uzpůsobeno k automatizovanému měření (tzn. realizace požadovaných 1000 měření bez nutnosti obsluhy, vytvořený program bude umožňovat automatickou změnu vstupního textu popřípadě tajného klíče). K realizaci využijte vývojové sady pro procesory Atmel a PIC a měřicí techniku v laboratoři. Na pracovišti realizujte jednoduchou a diferenční elektromagnetickou analýzu pro zvolené kryptografické moduly a kryptografické algoritmy. Analyzujte vliv počtu naměřených proudových průběhů na výsledky analýzy. Implementujte softwarově některou z ochran (např. časová oblast) a diskutujte vliv na DEMA.

DOPORUČENÁ LITERATURA:

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

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

Termín zadání:	11.2.2013	***Termín odevzdání:***	29.5.2013

Vedoucí práce: Ing. Zdeněk Martinásek
Konzultanti diplomové práce:

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

ABSTRAKT

Tato diplomová práce se zabývá studiem teorie postranních kanálů, jednoduché a diferenciální analýzy a typy útoků na postranní kanál, které mohou proběhnout proti kryptografickému systému. V diplomové práci jsou vysvětleny principy jednotlivých útoku na postranní kanál a možná obrana proti nim.
Druhá část diplomové práce popisuje vytvořené experimentální pracoviště, jeho jednotlivé součásti a jejich funkce. Na tyto poznatky navazuje vlastní řešení útoku na elektromagnetický postranní kanál pomocí elektromagnetické sondy a příslušného vybavení pracoviště vytvořeného pro tuto úlohu.
Závěrečná část diplomové práce je věnována popisu implementovaného algoritmu, popisu měření, výsledkům měření a možným úpravám implementovaných algoritmů v mikrokontroléru pro plnou automatizaci útoku na zařízení, proti kterému byl útok veden.

KLÍČOVÁ SLOVA

postranní kanál, jednoduchá analýza, diferenciální analýza, měřicí metody, sonda

ABSTRACT

This diploma thesis studies the theory side channels, simple and differential analysis, and types of attacks on the side channel, which may be run against the cryptographic system. The thesis explains the principles of side channel attack on a possible defense against them.
The second part of the thesis describes experimental work created, its individual components and their functions. The findings builds custom solutions attack the electromagnetic side channel using electromagnetic probes and the workplace equipment developed for this task.
The final part of the thesis is devoted to the description of the implemented algorithm, a description of measurement, measurement results and possible modifications of algorithms implemented in the microcontroller for full automation of the attack on the device, against which the attack was conducted.

KEYWORDS

side channel, simple analysis, differential analysis, measurement methods, probe

NOVOTNÝ, Bohumil *Diferenciální elektromagnetická analýza*: diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2013. 52 s. Vedoucí práce byl Ing. Zdeněk Martinásek

PROHLÁŠENÍ

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

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

(podpis autora)

PODĚKOVÁNÍ

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

Brno ....

(podpis autora)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic

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

PODĚKOVÁNÍ

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

Brno . . . . . .

. . . . . .
(podpis autora)

OBSAH

Úvod **10**

1 Teorie postranního kanálu **11**
1.1 Jednoduchá analýza 12
1.2 Diferenciální analýza 12

2 Typy postranních kanálů **13**
2.1 Proudový postranní kanál 13
2.1.1 Statická spotřeba obvodu 14
2.1.2 Dynamická spotřeba obvodu 14
2.1.3 Parazitní kapacita 15
2.2 Elektromagnetický postranní kanál 16
2.3 Časový postranní kanál 17
2.4 Chybový postranní kanál 17
2.5 Ostatní postranní kanály 17

3 Typy útoků **19**
3.1 Aktivní a pasivní útok 19
3.2 Invazivní,neinvazivní a semi-invazivní útok 19

4 Obrana proti útokům **21**
4.1 Proudový postranní kanál 21
4.2 Elektromagnetický postranní kanál 21
4.3 Časový postranní kanál 21
4.4 Chybový postranní kanál 22
4.5 Ostatní postranní kanály 22

5 Vlastní řešení **23**
5.1 Experimentální pracoviště 23
5.2 Elektromagnetická sonda 24
5.3 Vývojový modul AVR STK500 24
5.4 Mikrokontrolér Atmega8515L 25
5.5 Digitální osciloskop 25
5.6 Zařízení pro uchycení 26
5.6.1 Neukotvená konstrukce 26
5.6.2 Uchycení šrouby 27
5.6.3 Nevodivá konstrukce s aretací 27
5.6.4 Finální řešení 27

6 Implementace kódu v prostředí AVR **29**
6.1 Sledování smyčky 29
6.2 Implementace vyčítání matic 34
6.2.1 Program terminal 34
6.2.2 Sériová komunikace 34
6.3 Výsledky měření a jejich zpracování 35
6.3.1 Synchronizované operace 35
6.3.2 Nesynchronizované operace 36
6.3.3 Možná řešení pokročilých metod měření 38
6.3.4 Měření a ukládání hodnot 40

7 Závěr **41**

Literatura **43**

Seznam symbolů, veličin a zkratek **45**

Seznam příloh **46**

A Příloha **47**
A.1 Naměřené rozměry testovacího kitu 47
A.2 Rozkreslení úchytného zařízení 48
A.3 Naměřené průběhy signálů 50

SEZNAM OBRÁZKŮ

1.1 Typy postranních kanálů a jejich analýzy 12
2.1 Zapojení CMOS invertoru převzatý z [13] 14
2.2 Proudová závislost na napěťových změnách invertoru CMOS. Převzato a upraveno podle [5] 15
2.3 Princip útoku elektromagnetickým postranním kanálem 16
5.1 Blokové schéma zapojení pracoviště 23
5.2 Typy sond pro měření 24
5.3 Funkční zapojení AVR STK500 25
5.4 Finální řešení konstrukce 28
5.5 Aplikované řešení konstrukce 28
6.1 Vývojový diagram smyčky while 30
6.2 Proudové průběhy operace XOR 32
6.3 Zpracovaný vzorek operace XOR matice 37
6.4 Zpracovaný vzorek operace XOR jednoho řádku 37
6.5 Řešení programu pomocí přetečení zásobníku 38
6.6 Řešení programu pomocí externího přerušení 39
A.1 Testovací kit 47
A.2 Jednotlivé pohledy na úchytné zařízení 48
A.3 Izometrické zobrazení úchytného zařízení 49
A.4 Reálné zapojení pinů na AVR STK500 49
A.5 Průběh operace XOR pro 5 výpočtů 50
A.6 Průběh operace XOR pro 25 výpočtů 50
A.7 Průběh operace XOR pro 50 výpočtů 51
A.8 Průběh operace XOR pro 100 výpočtů 51
A.9 Srovnání vzorků matic 1x0 s 1xdata 52

ÚVOD

V současné době šifrovací algoritmy dospěly do velmi vyspělé formy, která je již matematicky velmi špatně napadnutelná. Matematický útok na šifry se stal spíše polemickou otázkou, protože prolomení šifry touto metodou by bylo úkolem pro počítače s nejvyšším výpočetním výkonem na několik desítek let. Z těchto důvodů se začaly objevovat nové metody, které neútočí na matematickou implementaci, ale na implementaci hardwarovou. Tyto útoky se soustřeďují na základní stavební prvky kryptografických modulů. Útočník se při nich zaměřuje na únik informací postranním kanálem. Mezi první útoky se řadí útok, který využíval proudovou analýzu. Brzy poté se začaly zkoumat teorie o napadení kryptografického modulu analýzou elektromagnetickou a v návaznosti na úspěšné prolomení šifer pokračovali kryptoanalytici ve zkoumání nových metod prolomení šifry. Díky zjištěním, že tyto útoky jsou možné, se postupem času začaly implementovat do kryptografických modulů různé verze ochran. Základní ochranou se stalo elektromagnetické stínění, oddělení datové a paměťové části, psaní kódu v hůře sledovatelných kaskádách posloupností a mnoho dalších metod pro ochranu citlivých dat.

V teoretické části diplomové práce jsou vysvětleny základní principy napadení kryptografických modulů postranním kanálem, důvody vzniku postranního kanálu a typy útoků, pomocí kterých jsou proti zařízením útoky vedeny. Na proudovém postranním kanálu je detailněji vysvětlena problematika CMOS obvodů, která úzce souvisí s jednoduchou a diferenciální analýzou. Na základě poznatků z této problematiky jsou zpracovány kapitoly o možné obraně proti vyjmenovaným útokům.

Druhá část diplomové práce se zabývá vlastním řešením a je členěna na dva segmenty. V prvním segmentu je popsán postup při konstrukci mechanického zařízení pro měření a zapojení měřicího pracoviště určeného k měření. Druhý segment je věnován implementaci algoritmů, které byly použity pro vlastní měření, shrnutí naměřených výsledků a návrhu dalšího možného postupu při diferenciální analýze dat.

1 TEORIE POSTRANNÍHO KANÁLU

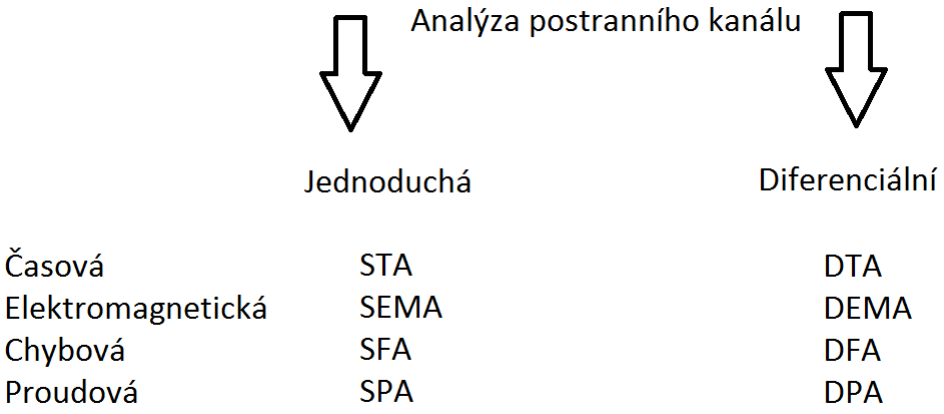
Ve světě informačních technologií jsou konstruována zařízení, která mají za úkol zpracovávat informace. V ideálním případě vstupuje do zařízení informace, zde je zpracována a vychází zpracovaná informace výstupní. Zařízení se z pohledu externího pozorovatele tváří jako takzvaný black-box neboli černá skříňka. Tento ideální model představuje zařízení, které je dokonale elektromagneticky stíněno, je napájeno konstantním elektrickým proudem a je vyrobeno zvukotěsně. Zařízení, které můžeme dnes prohlásit za bezpečný hardware již za krátkou dobu bezpečné být nemusí. V roce 1996 P.C. Kocher v [14] dokázal, že každé zařízení může mít nějakou slabinu, kterou může tajná informace uniknout.

Každé zařízení více či méně emituje do svého okolí informace. Tyto informace mohou být sledovány a zneužity ku prospěchu útočníka. Nežádoucí komunikaci s okolím označujeme jako postranní kanál.

Teorie postranního kanálu pojednává o metodách, které vedou k získání užitečných informací ze zařízení, které není možné napadnout jednoduchou matematickou metodou. Nežádoucí komunikace sledovaného zařízení s okolím může mít za následek monitorování informací v zařízení a případně následné dešifrování tajných dat. Nežádoucí komunikace zařízení s okolím může mít podstatu proudového, elektromagnetického, časového, optického a ostatního charakteru dle určení činnosti a chování napadeného zařízení. Útok postranním kanálem na zařízení se tedy může specializovat přímo na úkony, ke kterým bylo zařízení konstruováno. Výhodou útoku postranním kanálem oproti matematickým útokům na algoritmus je, že z velké části nebyla zařízení koncipována a připravena na typy útoků, které se nesoustředí přímo na informaci matematicky zašifrovanou, ale na únik citlivé informace při jejím zpracovávání z kryptografického modulu.

Díky moderním metodám zachycení citlivé informace se začaly zároveň s nimi tvořit matematické metody sloužící pro zpracování a vyhodnocení uniklých citlivých dat. Tyto metody se podle svého zaměření na rozkrývání informací dále rozdělují na jednoduchou analýzu a diferenciální analýzu.

Analýza postranního kanálu je typ neinvazivního nebo invazivního útoku, který má za úkol zjistit citlivá data z napadnutého zařízení. Jednoduchá analýza sestává z odchycení několika vzorků dat a jejich zpracování. Diferenciální analýza operuje s matematickými a statistickými výpočty stovek až tisíců vzorků. Přehledná tabulka typů analýz je na obr.1.1.



Obr. 1.1: Typy postranních kanálů a jejich analýzy

1.1 Jednoduchá analýza

Za jednoduchou analýzu postranního kanálu SPA považujeme takovou, která se zabývá přímým zpracováním dat uniklých ze sledovaného zařízení. Podle techniky odchycení dat ji můžeme dále rozdělit na útoky, které proběhnou pouze jednou a útoky, které proběhnou několikrát. U útoků, které probíhají jednou je zaznamenána pouze jedna trasa signálu, kdežto u vícenásobné analýzy je zaznamenáváno více tras signálu a může být zaznamenávána stejná část signálu vícekrát. Tím se dosáhne většího odkrytí volného textu.[5]

1.2 Diferenciální analýza

Zatímco SPA útoky identifikují relevantní výkonové změny, DPA útoky požívají statistickou analýzu a techniky pro korekci chyb, pomocí kterých se lze dopátrat zašifrovaného klíče. K takové analýze je třeba sesbírat mnohem více statistických dat, než u SPA. Díky faktu, že k provedení takového útoku nepotřebujeme znát detailní strukturu napadeného zařízení a k analýze nám stačí i zarušený signál, stal se tento typ útoku vhodným pro další zkoumání. Počty vzorků, které je třeba zachytit, se pohybují okolo tisíce kryptografických operací obsahujících soukromý klíč. DPA sestává ze dvou fází. První fází je shromáždění dat a druhou fází je jejich analýza. Shromáždění je provedeno vzorkováním příkonu zařízení během kryptografických operací a analýza je provedena matematickým zpracováním zachycených informací. DPA je tedy mnohem sofistikovanější a nebezpečnější pro kryptografický modul, než SPA. [6]

2 TYPY POSTRANNÍCH KANÁLŮ

Emise citlivých informací nemusí mít nutně povahu přímo závislou na konstrukci zařízení, ale i na faktorech, které nejsou zřejmé na první první pohled. Dle zdrojů informací unikajících postranním kanálem při zpracovávání algoritumu jsou to:

- proudová spotřeba
- elektromagnetické emise
- časové informace
- zavádění chyb do hardwaru
- ostatní typy emisí informace

2.1 Proudový postranní kanál

Proudová analýza využívá faktu, že proudová spotřeba zařízení je založena na hammingově váze právě zpracovávaných hodnot. Při zkoumání spotřeby proudového kanálu vycházíme ze skutečnosti, že procesor zpracováváním instrukcí spotřebovává proud rovný součtu statického a dynamického proudu mikrokontroléru. Proudová spotřeba je přímo úměrná počtu překlopených tranzistorů. V současných procesorech jsou využívány tranzistory založené na technologii CMOS. Jejich základním stavebním prvkem je invertor obr.2.1. Invertor je realizován dvěma tranzistory opačného typu vodivosti, které jsou řízeny napětím. Při klidovém stavu, kdy je invertor překlopen do stavu logické nuly nebo jedničky je proudová spotřeba minimální. Při konstantním napájecím napětí je tedy spotřeba udávána jako statický výkon P_{stat}. Výkonový skok ale představuje fáze překlopení. Při překlopení jsou v krátkém časovém úseku oba tranzistory otevřeny vůči zemi a vstupní svorky jsou proti zemi zkratovány. Při zkratu dochází k proudové špičce, která významně překračuje hodnotu statického proudu a stává se měřitelným ukazatelem překlopení invertoru. Zkratový proud při konstantním napájecím napětí nazýváme dynamickou spotřebou P_{dyn}. Celková spotřeba obvodu je dána těmito parametry:

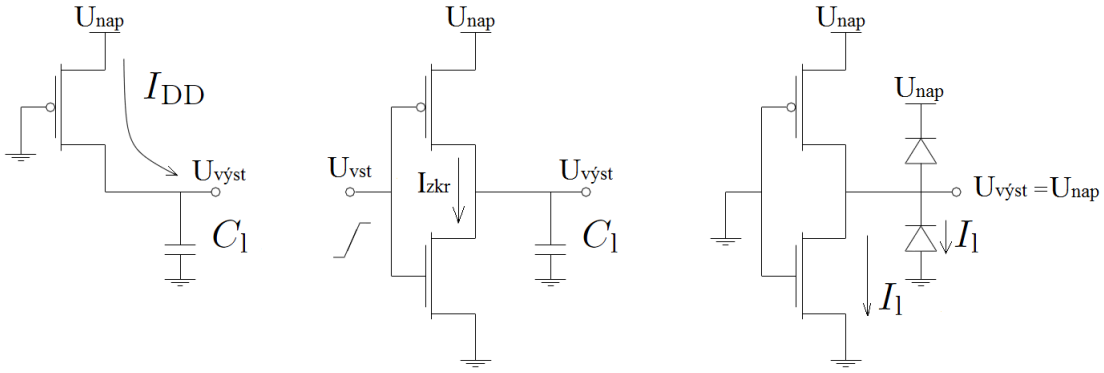
- Dynamická spotřeba
- Statická spotřeba
- Poruchová spotřeba

Celková spotřeba mikrokontroléru je dána vztahem:

$$P = P_{dyn} + P_{stat} + P_{glitch} \tag{2.1}$$

Průměrná spotřeba zařízení je rovna:

$$P_{ekv} = \frac{1}{T}\int_0^T p_{ekv}(t)dt = \frac{U_{nap}}{T}\int_0^T i_{DD}(t)dt \tag{2.2}$$



Obr. 2.1: Zapojení CMOS invertoru převzatý z [13]

2.1.1 Statická spotřeba obvodu

Statická spotřeba obvodu je přímo závislá na proudovém odběru CMOS invertorů při konstantním napájecím napětí. Proudový odběr při statické spotřebě je mnohem nižší, než u dynamické spotřeby. Statická spotřeba jednotlivých invertorů znamená, že je invertor CMOS v konstantním stavu logické nuly nebo logické jedničky. Statický proud je naznačen na obr2.1 vpravo jako I_l. Statická spotřeba je dána vztahem:

$$P_{stat} = I_l \times U_{nap} \tag{2.3}$$

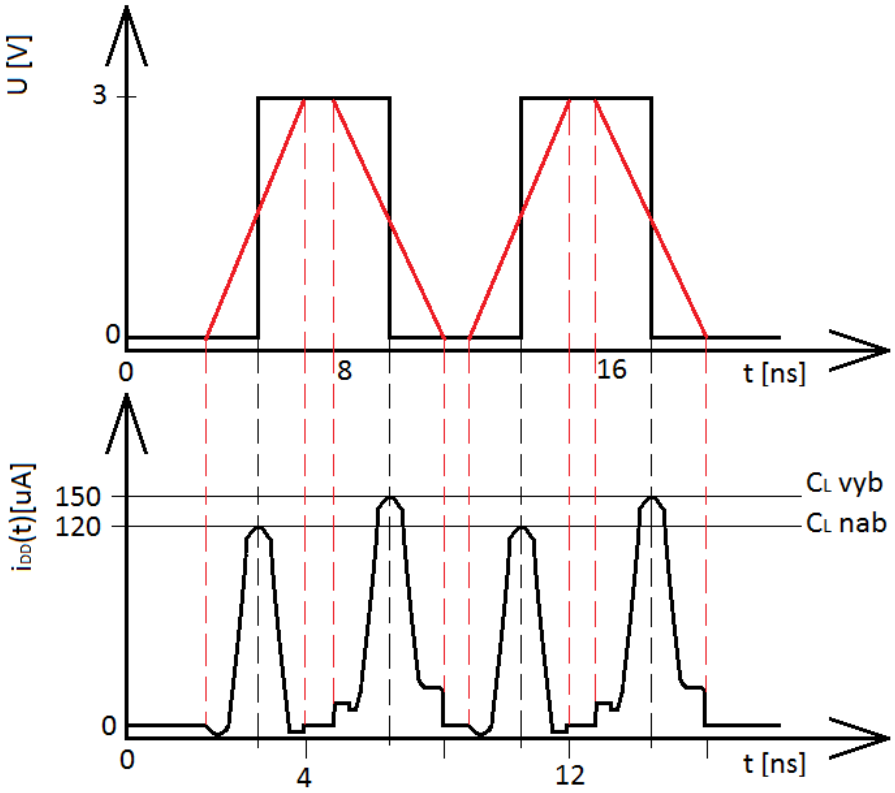
Kdy P_{stat} vyjadřuje statickou spotřebu jedné periody rovnu součinu ztrátového proudu I_l a napájecímu napětí U_{nap}.

2.1.2 Dynamická spotřeba obvodu

Dynamická spotřeba invertoru vzniká při překlopení logické úrovně z 0 do 1 a z 1 do 0. Hlavním důvodem vzniku dynamické spotřeby je proudová špička, která vznikne překlopením tranzistorů invertoru. Průběh proudu I_{DD} při překlopení je naznačený na levém obrázku 2.1. V ideálním případě by došlo pouze k překlopení logické úrovně. V reálné situaci se však při překlopení tranzistorů mezi nimi objeví krátký zkrat způsobující proudovou špičku. Tato situace je naznačena na prostředním obrázku, kde je zkratový proud naznačen jako I_{zkr}. Díky skutečnosti, že tato proudová špička vzniká pouze při změně logické úrovně tranzistoru se invertor stává datově závislým. Každý takto vytvořený proudový impulz vytváří elektromagnetické datově závislé pole, které dává možnost napadení zařízení elektromagnetickým postranním kanálem. Průběh proudové špičky při nabíjení a vybíjení je rozkreslen na obr2.2.

2.1.3 Parazitní kapacita

Pro úplné dokreslení situace při překlopení invertoru je možné si na obr2.2 všimnout mírných deformací proudové špičky. Tato deformace je dána parazitní kapacitou. Parazitní kapacitu C_l si lze představit jako kondenzátor paralelně připojený mezi oba tranzistory a zem, tedy výstup a zem. Tato kapacita má v reálném obvodu za následek mírný pokles proudové špičky při změně logické úrovně z 0 na 1 a nárůst proudové špičky průběhu při přechodu z logické 1 na 0. Tyto změny jsou způsobeny nabíjením a vybíjením kondenzátoru C_l naznačeného v obr.2.1. Lehká deformace před proudovou špičkou a za proudovou špičkou je dána ostatními parazitními kapacitami tranzistorů. V závislosti na počtu CMOS invertorů v zařízení poté tyto ostatní parazitní kapacity narůstají. [5]

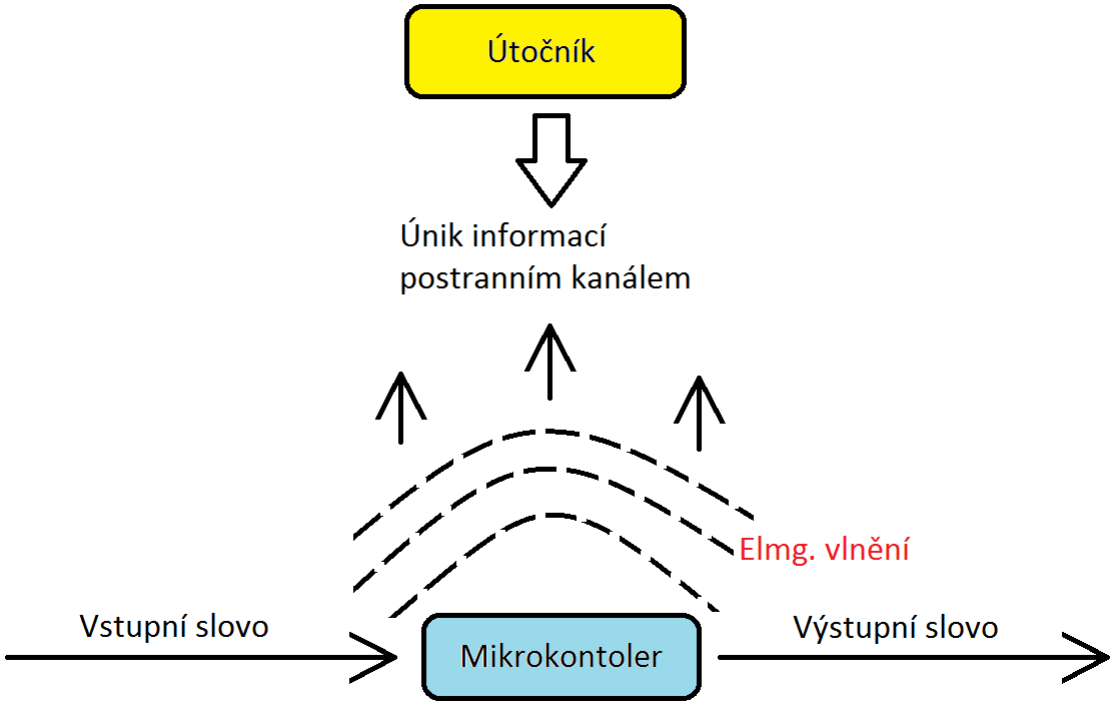


Obr. 2.2: Proudová závislost na napěťových změnách invertoru CMOS. Převzato a upraveno podle [5]

2.2 Elektromagnetický postranní kanál

Elektromagnetický postranní kanál vychází z proudového modelu popsaného v předešlé kapitole a pracuje se zákony elektromagnetického pole, které zformuloval James Clerk Maxwell. Na základě jím popsaných zákonů lze tvrdit, že každá změna proudu nebo napětí vyvolá změnu elektromagnetického pole. Jelikož zařízení odebírá elektrický proud, který je datově závislý, elektromagnetické pole je datově závislé taktéž. Díky těmto fyzikálním vlastnostem se každé zařízení emitující elektromagnetické pole stává slabé proti útoku na fyzickou konstrukci kryptografického systému. Emisi elektromagnetického pole lze měřit vložením cívky do jeho blízkosti obr. 2.3. Každou slabinu zařízení, kolem kterého vzniká elektromagnetické pole a zpracovávajícího tajnou informaci, nazýváme elektromagnetickým postranním kanálem.

Hlavním rozdílem mezi měřitelnou křivkou napájecího elektrického proudu, kterým je zařízení napájeno, a elektromagnetickým polem vytvořeným okolo napájecího konektoru je, že naměřená proudová křivka odpovídá jednoduchému amplitudovému průběhu, kdežto naměřená elektromagnetická křivka odpovídá trojdimenzionálnímu vektoru elektromagnetického pole měnícího se v čase. [13]



Obr. 2.3: Princip útoku elektromagnetickým postranním kanálem

2.3 Časový postranní kanál

Kryptosystémy často při zpracování informace potřebují jistou dávku času. Množství času potřebné pro zpracování informace závisí na několika parametrech, mezi které patří:

- Výkonnost zařízení
- Větvení programu
- Rychlost čtení RAM
- Zpracovávané operace

Časový postranní kanál tedy operuje s časovou náročností matematických operací při zpracování klíče. Aby bylo možné časový útok na postranní kanál provést, je třeba znát časovou závislost matematických operací zařízení a parametry zařízení. [14]

2.4 Chybový postranní kanál

Zavádění chyb do kryptosystému je způsob napadení chybovým postranním kanálem, který je zaměřený především na symetrické šifry. Úspěšný útok pomocí chybového postranního kanálu úspěšně provedli E.Biham a A.Shamir. Obecně je tento útok založen na zavádění chyb do kryptosystému a následné analýze pertubací chybových hlášení. Při útoku se předpokládá, že se může v registru vyskytnout chyba na základě chybového modelu. Na základě pravděpodobnosti chyby pro každý jednotlivý bit je možné zjistit celý šifrovací klíč. [15]

2.5 Ostatní postranní kanály

Při rozmachu pokusů o útoky na postranní kanál různých zařízení, především čipových karet se, se začalo uvažovat i o alternativních útocích. Oproti zažitým a mnohokrát popsaným útokům se začalo uvažovat i o útocích, které nesouvisí přímo s elektrickými vlastnostmi čipu nebo jejich měřením. Začalo se uvažovat o útocích, které by mohly přinést jakoukoliv informaci o vnitřní struktuře zařízení.

Jedním z představitelů ostatních postranních kanálů je kanál optický. Princip optického postranního kanálu popisují autoři [16]. Je založen na poznatku, že CMOS tranzistory při svém překlopení emitují malé množství fotonů. Příčinou této emise je velmi krátký intenzivní zkrat popsaný v kapitole proudového postranního kanálu. Zkratový proudu způsobuje opticky měřitelnou emisi fotonů. Díky tomuto zkratu je možné extrahovat informací z napadnutého zařízení. Pro zkvalitnění naměřených informací se tato technika kombinuje s invazivním zásahem do zařízení odbroušením

svrchní části čipu nebo jejím odleptáním. Protože jsou v současné době k dispozici mnohem sofistikovanější obrany jako jsou metalické vrstvy okolo čipu, je tato metoda čím dál méně využívána pro získání informací.

Útok na akustický postranní kanál byl realizován jako odposlech centrální procesorové jednotky pány A.Shamirem a E.Tromerem. Ti ověřili, že procesorová jednotka vytváří akustické vlnění, které je měřitelné. Výsledkem měření se stal report, ve kterém bylo, podle typu vydávaného zvuku, možné vysledovat, jak moc je procesor vytížený a podle toho určit, o jaký se jedná algoritmus. [10]

3 TYPY ÚTOKŮ

V současné době se využívá k útoku na postranní kanál několik metod. Jejich základní rozdělení je odvíjeno od typu útoku, jaký je na zařízení veden. Základní rozdělení takových útoků je popsáno v následujících kapitolách.

3.1 Aktivní a pasivní útok

Aktivní útok

Aktivní útok bývá mnohem sofistikovanější, než pasivní a je založen na manipulaci se vstupy sledovaného zařízení, změnou okolních podmínek sledovaného zařízení nebo kombinací obou možností. Taková manipulace má za následek změny chování zařízení. Změny chování zařízení pro útočníka znamenají cennou informaci o jeho chování při změnách z běžného pracovního prostředí do neobyčejného a ne zřídka se podaří změnit pomocí takto nastavených parametrů zařízení některou z rozhodovacích úrovní tranzistoru a tím vysledovat část nezašifrované paměti.

Pasivní útok

Pasivní útok spočívá v pozorování zařízení a snaze zjistit stěžejní informace k odhalení otevřeného textu, šifrovacího klíče nebo jejich částí. Princip takového útoku bývá spjat se sledováním času, který je potřeba ke zpracování informace nebo spotřeby, která je přímo úměrná množství a složitosti zpracovávaných dat.

3.2 Invazivní,neinvazivní a semi-invazivní útok

Invazivní útok

Je považován za nejsilnější a nejefektivnější typ útoku, který může být veden proti kryptografickému zařízení. Invazivní útok zpravidla spočívá ve fyzickém narušení zařízení, části zařízení nebo rozebrání na součásti, které jsou poté zkoumány nezávisle na sobě. Následkem takového zkoumání je například odstranění ochranných prvků zařízení od části, která data zpracovává, šifruje, či dešifruje nebo odbroušení některých vrstev zkoumaného čipu. Takovýto útok bývá většinou destruktivní a nadále se nepočítá s dalším použitím tohoto zařízení. Invazivní útok tedy přímo ovlivňuje elektrickou i fyzickou část zařízení.

Neinvazivní útok

Neinvazivním útokem je myšlen každý útok, který není prováděn hrubou silou a nijak hardwarově ani softwarově nenaruší integritu zkoumaného zařízení. Při tomto útoku nelze ze strany zařízení zjistit, zda útok proběhnul, či neproběhnul, a tím se stává nebezpečným, protože napadené zařízení nemá zpětnou vazbu o tom, že vůbec útok probíhá nebo proběhnul. Základní myšlenkou je pouhé měření fyzikálních veličin, které zařízení vyzařuje do okolí a je měřitelné externím přístrojem. Nejznámějšími metodami jsou proudová analýza, elektromagnetická analýza a časová analýza.

Semi-invazivní útok

Semi-invazivní útok spočívá v částečném odstranění redundantních částí zařízení, ale přímo nenarušuje elektrickou strukturu zařízení. Semi-invazivní útok může probíhat také pasivně nebo aktivně. Pasivní útok je například zaměřen na vyčítání dat z paměťových center zařízení. Opačným případem je aktivní semi-invazivní útok, při kterém se do zařízení zavádějí záměrně chyby a zkoumají se výstupní informace, které zařízení vysílá. Zavádění záměrných chyb poté může probíhat několika způsoby. Optickým osvětlováním čipu vysoce intenzivním světlem, které může na bázích tranzistorů změnit rozhodovací úrovně, rentgenovým paprskem zkoumajícím vnitřní strukturu čipu nebo silným elektromagnetickým polem.

4 OBRANA PROTI ÚTOKŮM

V dnešní době existuje mnoho typů útoků na postranní kanály a žádné zařízení, které je chráněno a zabezpečeno dnes, nemusí být bezpečné za několik let. Na základě typu útoku můžeme obecně specifikovat druhy ochran kryptografických systémů.

4.1 Proudový postranní kanál

Jak bylo již zmíněno v předešlých kapitolách, proudový postranní kanál bude existovat v každém kryptografickém systému nebo zařízení zpracovávající citlivé informace, ve kterém bude napájecí proud nebo napětí datově závislý na zpracovávaných datech. Možnou obranou proti takovému útoku je zajistit nezávislost napájecího proudu nebo napětí na datech zařazením ochranných prvků do elektrických obvodů zařízení a zajistit nepřístupnost napájecích obvodů kryptografického modulu. Tím je myšleno, že nebude možné, aby se útočník dostal k napájecímu pinu nebo konektoru zařízení, aniž by invazivně napadené zařízení narušil.

4.2 Elektromagnetický postranní kanál

Elektromagnetická analýza postranního kanálu je možná díky závislosti elektromagnetického pole na právě zpracovávaných datech podobně jako u proudové závislosti. Hlavním cílem obrany proti útoku by mělo být co nejefektivnější zamezení jeho emise z kryptografického modulu například elektromagnetickým stíněním zařízení nebo zamaskování a zkreslení této emise.

Metodu zkreslení emise nazýváme jako skrývání. Je založena na vytvoření matoucí závislosti elektromagnetického pole na zpracovávaných datech. Matoucí emise elektromagnetického pole lze dosáhnout dvěma způsoby. Prvním způsobem je zavedení náhodné spotřeby zařízení v každém časovém intervalu. Druhou metodou je zkonstruovat zařízení tak, aby byla spotřeba zařízení ve všech časových intervalech stejná. Bohužel se zatím nepodařilo vytvořit žádné zařízení maximálně nezávislé na zpracovávaných datech. V současné době se zařízení pouze přibližují k tomuto ideálnímu stavu.

4.3 Časový postranní kanál

Obranou proti napadení zařízení pomocí časového postranního kanálu je dosažení časové nezávislosti na zpracování dat. Časová nezávislost dat může být dosažena

dvěma způsoby. Vytvořením stejných časových intervalů pro zpracování každé operace a nebo přidáním náhodného zpoždění u každé operace. V praxi jsou ovšem podmínky vedoucí k zamaskování času potřebného ke zpracování dat velmi často nedosažitelné z důvodu optimalizace kompilátoru, rychlosti vyčítání RAM, času pro provedení instrukce a kombinací mnoha jiných faktorů. Technika, která se zabývá problémem konkrétní obrany před napadením kryptografického modulu, se nazývá maskování. [14]

4.4 Chybový postranní kanál

Pokud útočník posílá do systému informace a zkoumá jeho odezvu, sleduje odezvu chybových hlášení a podle toho se učí, jak vnitřní struktura čipu funguje. Z těchto dat vyčítá správnost šifrovaného textu.

Jedním ze základních pravidel obrany proti takovému útoku je vyvarování se použití příkazů "stop"a "brake", psaní programů v co nejvíce spojité posloupnosti a ověřování délky dílčích výsledků.

Dalším řešením problému by bylo oddělení výpočtové části od datových vstupů. Tato metoda je již pokročilým řešením problému a vyžadovala by hlubší technologický zásah do konstrukce. [4]

4.5 Ostatní postranní kanály

Obrana před ostatními postranními kanály je závislá na typu vedeného útoku na zařízení. V současné době je diskutováno a zkoumáno mnoho nových metod napadení kryptografického zařízení.

Jedním z pomalu upadajících se stal útok na optický postranní kanál, který byl použit ke sledování emitovaných fotonů z čipu při překlápění logických úrovní CMOS tranzistorů v invertorech. V dnešní době jsou již čipy vybaveny metalickými vrstvami, které tyto emise fotonů pohlcují. V případě takto chráněných zařízení je již nutné využít invazivních metod útoku.

Mezi metody útoku na postranní kanál, které nejsou přímo vázány elektrickými vlastnostmi čipu, můžeme zařadit i kanál akustický. Odvětví akustických projevů zařízení zatím nebylo bráno jako přímá hrozba pro zařízení provádějící výpočty, ovšem každý projev zařízení, každá nežádoucí výměna jakékoliv informace s okolím se může stát v budoucnu nebezpečnou.

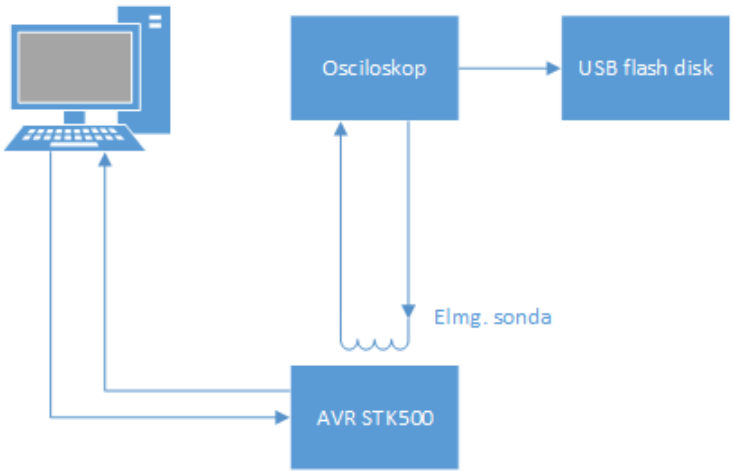
5 VLASTNÍ ŘEŠENÍ

Cílem vlastního řešení proudové analýzy bylo vytvoření experimentálního pracoviště vhodného pro měření, realizace zařízení pro uchycení včetně uchycovací soustavy pro předpřipravené sondy, implementace algoritmu části AES a změření elektromagnetického pole, pomocí kterého budou získány hodnoty pro SPA a DPA.

5.1 Experimentální pracoviště

Pro samotné zaměření postranního kanálu je nutné, abychom měli dostatečně vybavené pracoviště, které by bylo schopno zaměřit elektromagnetické změny způsobené překlápěním logických úrovní. Zkoumaným prvkem je mikrokontrolér Atmega8515L od společnosti Atmel. Pracoviště je zapojeno dle obr. 5.1. Mezi základní stavební prvky zapojeného pracoviště patří:

- Notebook MSI s nainstalovaných operačním systémem Windows 7 ultimate
- AVR studio verze 4.19.0.730
- Matlab verze 7.12.0.384
- Vývojová deska AVR STK500 s mikrokontrolérem Atmega8515L
- Převodník USB/RS-232 ASIX UCAB232
- Osciloskop Tektronix DPO 4032
- Elektromagnetická sonda
- Zařízení pro uchycení



Obr. 5.1: Blokové schéma zapojení pracoviště

5.2 Elektromagnetická sonda

Hlavním článkem experimentální měřicí soustavy je elektromagnetická sonda obr. 5.2, speciálně zkonstruovaná pro zaměření postranního kanálu. Tato sonda zachycuje blízké elektromagnetické pole vyzářené z převodní části mikrokontroléru a byla vyrobena pro dřívější diplomové práce na toto téma.[2]

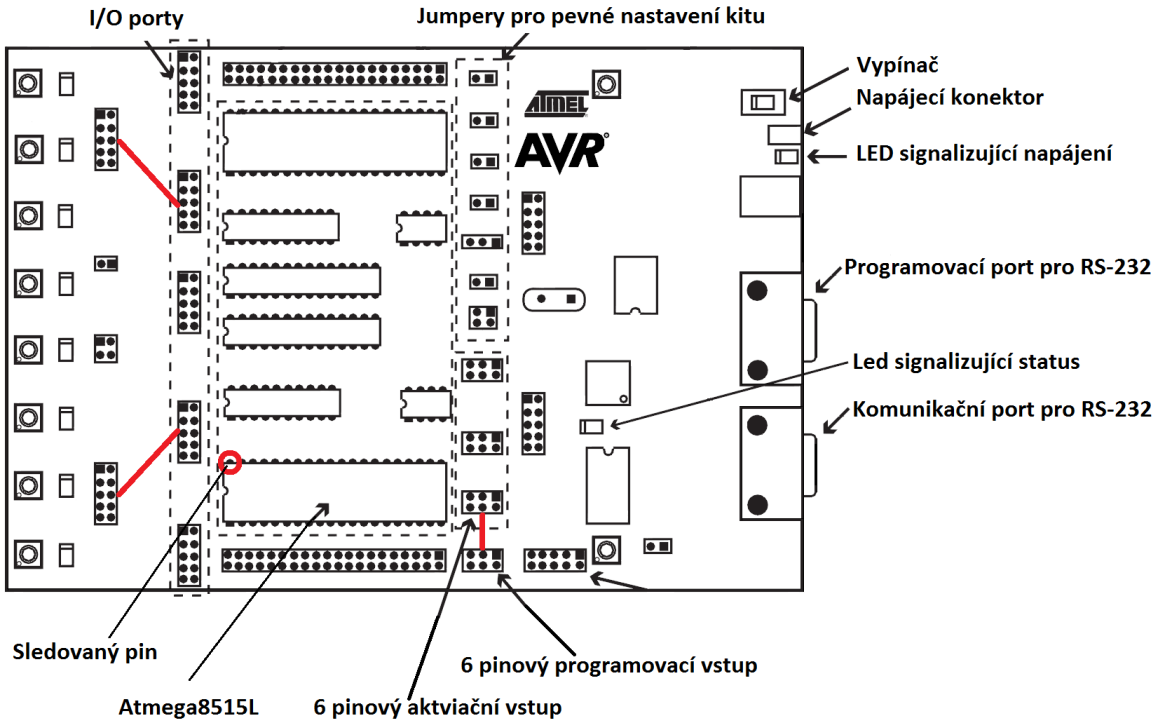
Hrot této sondy je zhotoven z měděného drátu o průměru d = 0,3mm, který je navinut jako cívka o jedenácti závitech ve tvaru solenoidu s vnitřním průměrem 0,7mm. Cívka je připojena ke koaxiálnímu kabelu o charakteristické impedanci 50Ω.

Obr. 5.2: Typy sond pro měření

5.3 Vývojový modul AVR STK500

Vývojový modul sestává z několika dílčích částí, které můžeme rozdělit na komunikační porty, část pro pevné nastavení vlastností kitu, paticovou část pro mikrokontroléry a vstupně/výstupní porty zařízení. Jak můžeme vidět na obr. 5.3, převzatého

z [3], je zde uvedeno zapojení pro náš případ zapnutí mikrokontroléru do aktivního stavu pro programování.



Obr. 5.3: Funkční zapojení AVR STK500

5.4 Mikrokontrolér Atmega8515L

Atmega8515L je osmibitový CMOS mikrokontrolér postavený na rozšířené architektuře RISC. Jádro AVR obsahuje 32 registrů, které jsou přímo spojeny s ALU. Sestavení mikrokontroléru je provedeno na základě harvardské architektury, která odděluje paměť pro programovou a datovou část. Zpracování instrukcí je prováděno tak, že při zpracovávání první instrukce je načtena instrukce následující z programové flash paměti. Tento koncept umožňuje zpracovávání instrukcí v každém hodinovém signálu.

5.5 Digitální osciloskop

K získání signálu, který věrně kopíruje obálku elektromagnetického vyzařování z obvodu, využijeme elektromagnetickou sondu, která dodá do osciloskopu analogový signál odpovídající proudovému odběru na měřeném místě. Po změření analogového

signálu přivedeného na osciloskop je signál vzorkován a převeden na digitální. Posledním krokem je zapsání signálu do paměti osciloskopu. Převod z analogového signálu na digitální je dán třemi parametry, kterými jsou vstupní šířka pásma, vzorkovací frekvence a rozlišení osciloskopu.

5.6 Zařízení pro uchycení

Jedním z úkolů diplomové práce bylo sestavit vlastní měřicí pracoviště tak, aby bylo možné provést jedno měření u SPA nebo také tisíc měření v sérii u DPA. K tomuto účelu bylo vytvořeno zařízení pro přesné uchycení elektromagnetické sondy, jejíž zaaretování je neměnné po celou dobu měření a je možné měření znovu opakovat i po rozložení laboratorní úlohy a jejím opětovném složení. Zařízení je vybaveno vertikálním i horizontálním pohybem ve směrech os x, y a z. V předchozích projektech a pracích byly tyto skutečnosti vyřešeny podomácku vyrobenými zkroucenými silnými dráty, které byly upevněny k pevné podložce nebo stolu. Takové řešení bylo nevhodné z několika hledisek.

Prvním problémem takového měření byla nemožnost opakovat stejné měření po rozebrání a znovusložení měřícího stanoviště. Tímto faktorem bylo měření výrazně ovlivněno hned v prvním okamžiku. Dalším faktorem ovlivňujícím výsledky byla možnost libovolného posunutí, zavadění o měřený čip nebo vibrace podložky. Při takovém nepatrnému posunutí mohlo kdykoliv dojít ke zkreslení výsledku a takový výsledek mohl vést k mnohem delšímu dešifrovacímu cyklu nebo celkovému zkreslení výsledku. Z tohoto důvodu bylo nutné vymyslet soustavu, ve které byly parametry zaaretování neměnné při jakékoliv manipulaci, čímž by bylo možno dosáhnout mnohem lepších výsledků měření a následného dešifrování posílané zprávy.

5.6.1 Neukotvená konstrukce

Z několika řešení se jako první naskytlo vyrobit jednoduchou klec z naohýbaných litinových hranolů, která by byla připevněna k měřené desce čtyřmi ocelovými svěrkami. Z důvodu rozložení součástek po obvodu měřené desky však nebylo technicky možné upevnit takové svěrky tak, aby nepoškodily měřenou desku v případě silného upevnění a aby v případě slabšího upevnění svorky neuhýbaly z původního nastavení při manipulaci. K tomuto systému by bylo nutné zkonstruovat ještě podstavec, aby nebyla soustava položena přímo na svorkách. Takové řešení však zcela nevyhovovalo požadavkům zadání.

5.6.2 Uchycení šrouby

Dalším řešením se zdál podobný princip konstrukce, ovšem s uchycením na šrouby. Opět jsme narazili na stejné konstrukční problémy zakoupeného kitu a desku nebylo možné provrtat na žádném vhodném bodě, který by zajistil pevné těžiště sondy, navíc by byla deska odkázána jen na jeden typ měření a zařízení jako takové by již nebylo možno využít pro jiné účely.

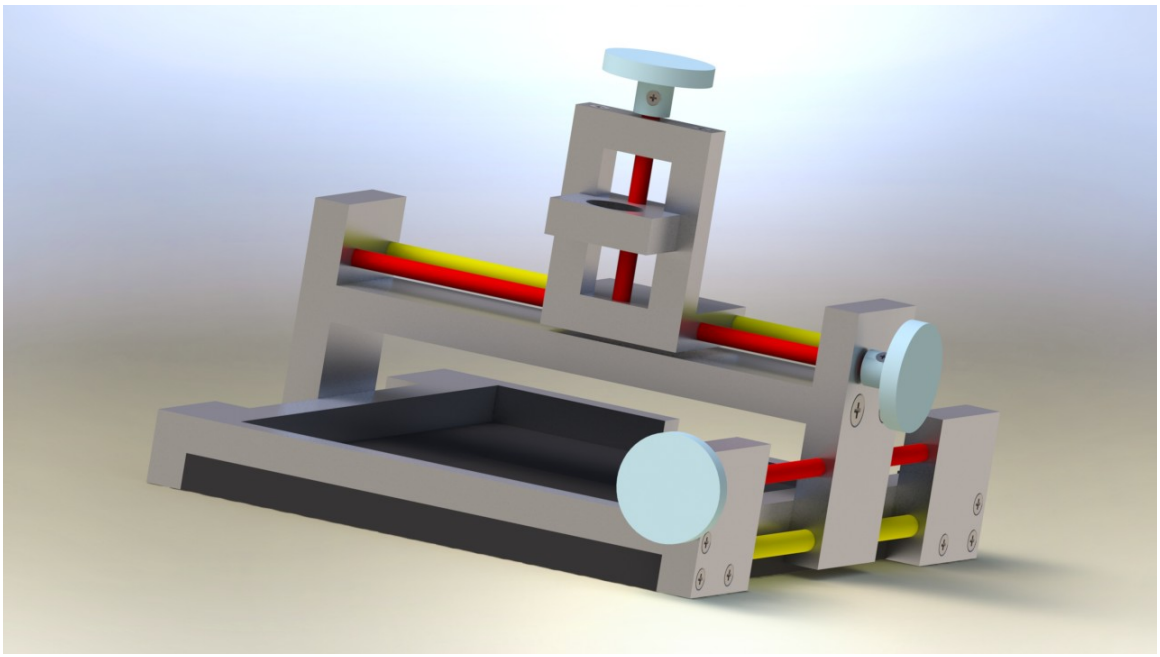
5.6.3 Nevodivá konstrukce s aretací

Třetím řešením se zdálo nalepení nevodivé konstrukce na kit a zajištění posuvu sondy po osách X a Y pomocí mikroareatčního zařízení. Takové zařízení je ale poměrně nákladné a pro náš účel není potřeba hodnoty přesné na setiny milimetru. Mikroaretační zařízení by bylo nutné ještě poupravit, aby se k němu dalo připevnit více druhů sond. Zařízení by bylo taktéž nepřenositelné na jiný druh testovacích plošných spojů. Rozměry testovacího kitu by nemusely rozměrově zapadnout a pevná konstrukce přilepená k testované desce by desku znehodnotila.

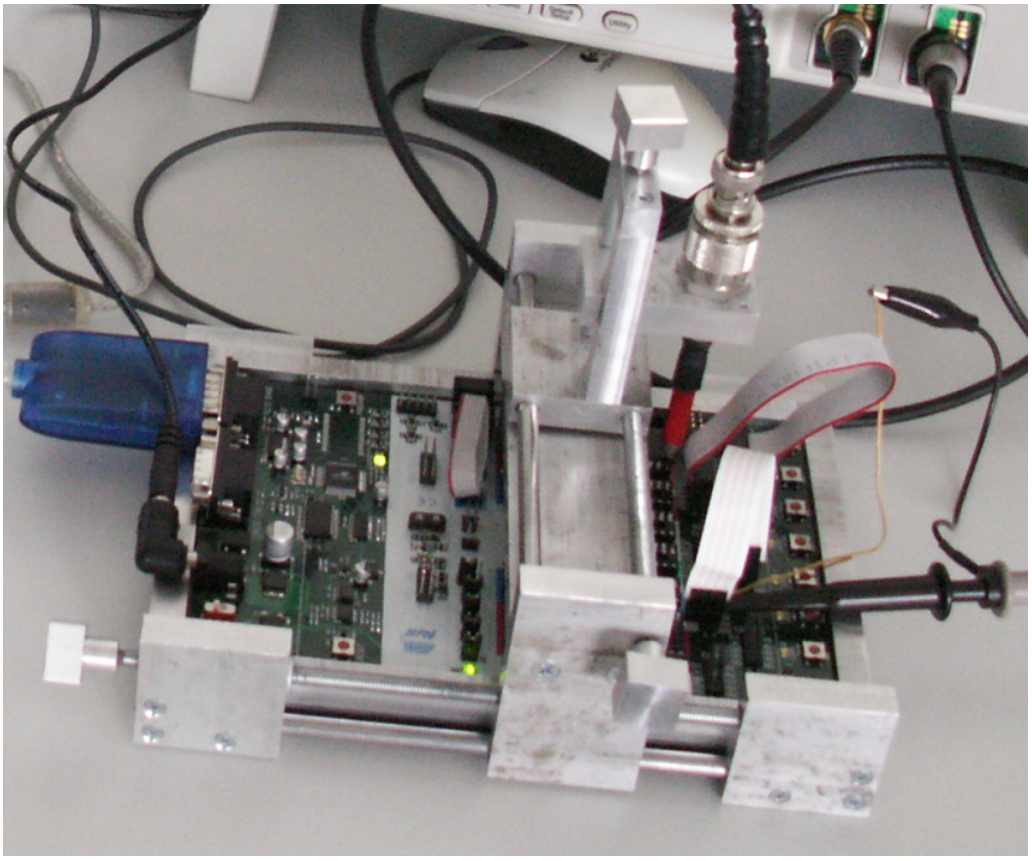
5.6.4 Finální řešení

Na základě předchozích řešení bylo navrženo zařízení obr. 5.4, které bylo kombinací všech předchozích návrhů. Zařízení má podstavec, ve kterém je přesně umístěn kit s měřeným čipem. Nad tímto kitem je zavěšena sonda na experimentálním závěsném zařízení s aretací. Aretace je řešena posuvnými hranoly se závity. Touto aretací je možno přesně zaměřit bod na měřeném zařízení. Zaměření je možné provést po celé délce i šířce části kitu, do kterého se dají umístit všechny mikrokontroléry, pro které je vývojový kit vytvořen. Aby bylo možné do zařízení umístit oba typy sond, je na výškově stavitelné části posuvu umístěn nástavec pro uchycení sond s větším i menším otvorem

Vlastní návrh byl vytvořen v programu solidworks, kde byly nejprve detailně zpracovány jednotlivé součásti zařízení a poté modelovány v 3D. Aby se předešlo problémům s montáží, byly jednotlivé součásti modelovány jednotlivě. Bylo zapotřebí, aby posuvy a na nich nasazené komponenty příliš netřely, což by mělo za následek špatnou manipulaci s aretací. Rozkreslení jednotlivých součástí však již není předmětem diplomové práce. Návrh celého zařízení je rozkreslen v příloze obr. A.2 z několika pohledů. Zkonstruované zařízení připojené přímo na pracovišti lze vidět na obr5.5.



Obr. 5.4: Finální řešení konstrukce



Obr. 5.5: Aplikované řešení konstrukce

6 IMPLEMENTACE KÓDU V PROSTŘEDÍ AVR

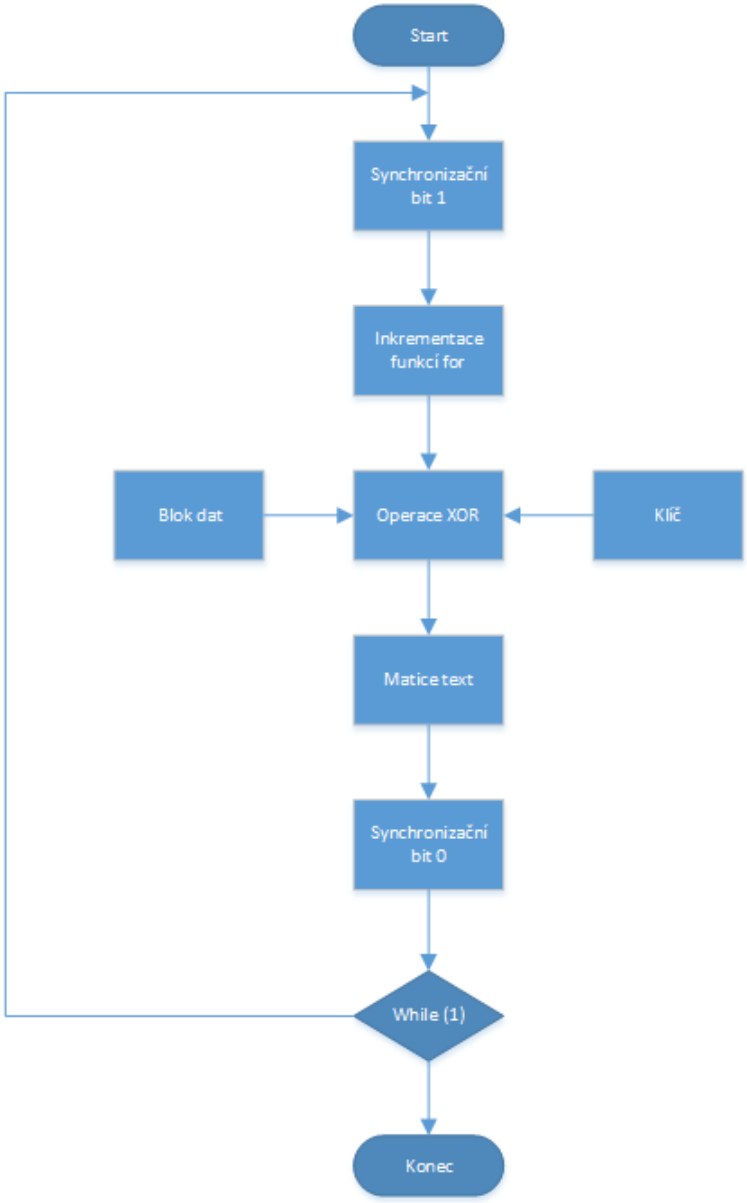
Pro zpracování dat a sledování šifrovacích algoritmů pomocí vytvořeného pracoviště a funkčního zapojení bylo třeba odesílat jakoukoliv informaci do paměti mikrokontroléru a sledovat zpracování informace v jeho vnitřní struktuře. V první části aplikace programu bylo vyzkoušeno, zda je možné vůbec na daném čipu vyzařování elektromagnetického pole měřit několika jednoduchými programy. Ve druhé fázi zpracování byla úloha rozvinuta o další možnosti programu i zadávání dat.

6.1 Sledování smyčky

Mezi první varianty odzkoušení funkčnosti fyzických parametrů patřilo ověření kompatibility zapojení. Ověřením kompatibility je myšleno samotné fyzické zapojení všech částí pro měření, implementace zdrojového kódu do mikrokontroléru a jeho správná funkce změřená osciloskopem. Fyzická struktura zapojení byla popsána v předchozích kapitolách. Zdrojový kód sloužící na odzkoušení měřitelnosti elektromagnetického pole byl použit program nightrider. Jeho princip spočíval v měření proudové spotřeby při zpracování dat v čipu. Pokud byl program ve stavu vykonávání procesu, bylo měřeno elektromagnetické pole okolo napájecího pinu větší, než u ostatních pinů.

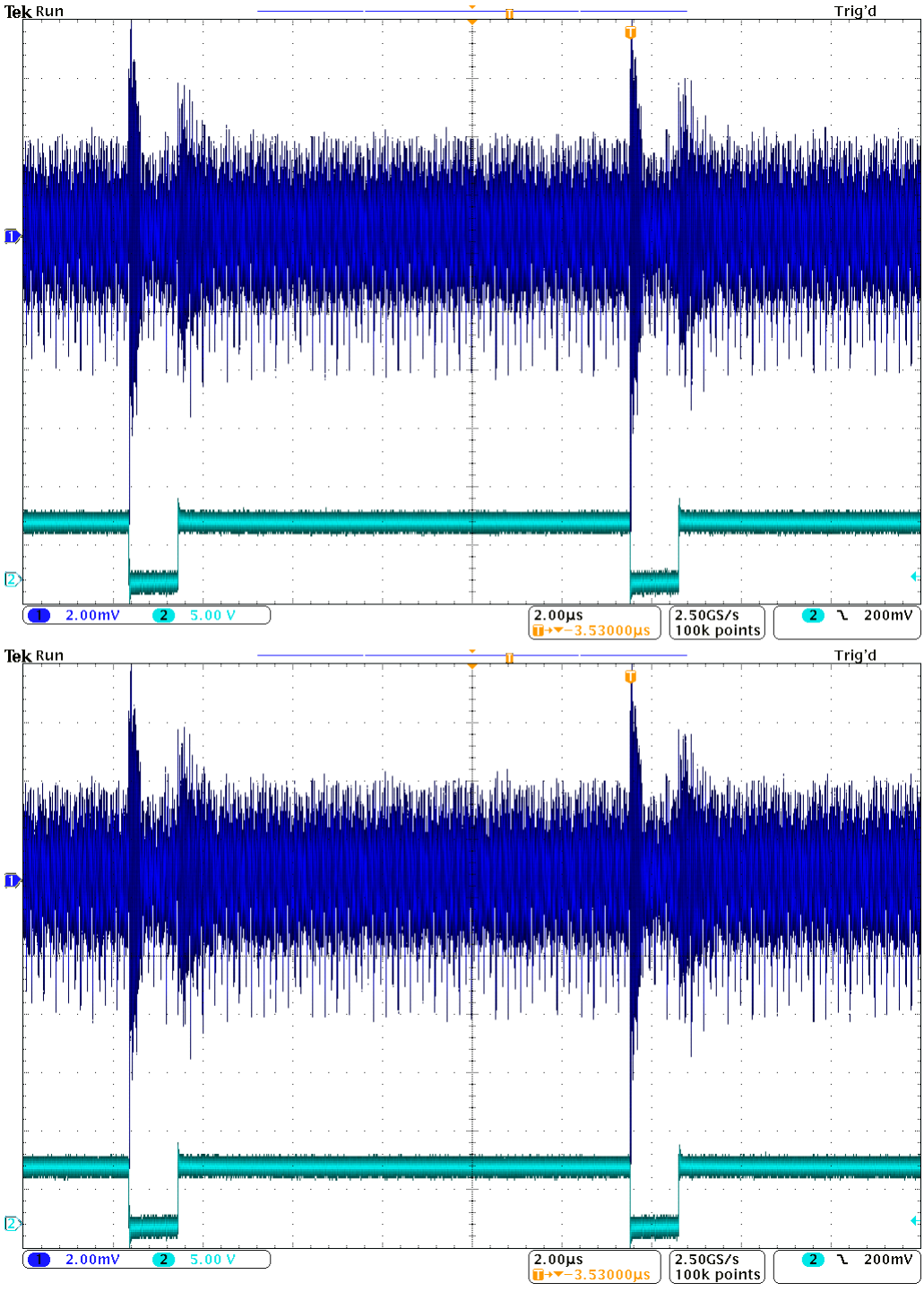
Po ověření funkčnosti celého systému bylo možné začít s jednoduchým implementováním funkcí, pomocí kterých byly sledovány na osciloskopu změny související s náročností prováděných matematických operací malých a velkých čísel. Úvodním pokusem bylo změření proudového průběhu při odeslané informaci 0b0000000, která znamenala logickou úroveň 0 na všech výstupech portu B. Zápisem této instrukce v každém cyklu smyčky bylo sledováno na průběhu proudové spotřeby, která vlna průběhu bude ovlivněna při inkrementaci odeslané informace v každé smyčce programu. Postupně byla přidávána na každý bit logická úroveň jedna a bylo sledováno, jak se projevuje změna na výsledném signálu. Bylo vycházeno z předpokladu, že čím vyšší matematicky zpracovávané číslo, tím větší amplituda sledované vlny na osciloskopu. Výsledné hodnoty byly zaznamenány osciloskopem, uloženy do tabulky a následně analyzovány v programu matlab. Výsledné odchylky byly téměř neznatelné i při maximálním rozdílu logických úrovní. Napěťová úroveň změřeného signálu kolísala okolo 2mV. Oproti proudové analýze při stejném principu měření se tato hodnota dá vyčíslit pouze jako dvě setiny signálu proudového. V případě násobení a následně výpočtů pomocí funkce XOR byly naměřené změny na osciloskopu rovněž zanedbatelné. Z důvodu velmi malého rozdílu proudových špiček nebylo možné tyto změny rozeznat ani po analýze v programu matlab.

Kvůli malým rozdílům proudových špiček byl program modifikován pro násobení matic o rozměrech 5x5 dle vývojového diagramu na obr6.1. Tyto matice byly uzavřeny ve smyčce while tak, aby operace XOR probíhala neustále. Aby bylo možné rozeznat operaci XOR a synchronizovat pouze násobení dvou matic, bylo do programu implementováno opakování operace desetkrát pomocí cyklu for v jedné smyčce. Na naměřených průbězích se cyklus for objevil jako první část signálu, následovaný provedením výpočtu.



Obr. 6.1: Vývojový diagram smyčky while

Protože má program AVR ještě svoji instrukční režii a také bylo nutné na osciloskopu přesně vymezit pouze matematické operace, byla zavedena do instrukčního cyklu synchronizace. Synchronizační cyklus byl realizován nastavením výstupu portu B0 na logickou úroveň 1 před začátkem operace XOR obou matic a jejím opětovném nastavení na logickou úroveň signálu 0 po ukončení funkce XOR. Následná synchronizace na osciloskopu byla provedena připojením druhého kanálu osciloskopu právě na pin B0. Na obr6.2 a je jasně parná synchronizace. Operace XOR jsou přesně vymezeny logickou úrovní 1. Obrázky jsou přímo vyexportovány z displeje osciloskopu. Na horním obrázku je znázorněno násobení matice naplněné hammingovou řadou násobenou maticí klíče naplněnou samými nulami. U této matice byl předpokládán výsledek shodný s násobenou maticí. Na spodním obrázku je výsledek měření pronásobení matice samých nul se stejným klíčem jako na horním obrázku. Výsledek těchto měření byl dále zpracováván v programu matlab jednoduchou analýzou, ovšem na výsledcích nebyl jasně patrný rozdíl mezi výsledky. Elektrický proud naindukovaný na měřicí cívce v podstatě odpovídal shodě.



Obr. 6.2: Proudové průběhy operace XOR

Pro přiblížení funkcionality je zde vložena hlavní část programu, která byla popsána výše a funguje podle popsaného vývojového diagramu. Je také hlavní částí dalšího postupu při programování složitější struktury programu, která bude popsána v následující části diplomové práce.

```
int main(void)
{



while(1)
    {

//aktivace portu B pro synchronizacni signal
DDRB = 0b00000001;
//_delay_ms(2);

//nastaveni synchronizacniho signalu na portu B na 1
PORTB = 0b11111111;

//smycka nacitani 10 cyklu
for(xor=0;xor<10;xor++){

/*postupne XORovani matice kazde hodnoty s kazdou,
kde I a J je poloha nasobeni v matici
*/
for(i=0;i<5;i++) {
for (j=0;j<5;j++) {
text[i][j] = klic[i][j]^text[i][j];
//text[i][j] =pole3[i][j];

}
}

}
//nastaveni synchronizacniho signalu na portu B na 0
//_delay_ms(2);
PORTB = 0b00000000;
}

}
```

6.2 Implementace vyčítání matic

V předešlém řešení bylo možné manipulovat s maticemi pouze přeprogramováním celé vnitřní paměti mikrokontroléru pomocí AVR studia. Dalšími velmi omezujícími faktory je samotné zadávání jediné matice pro výpočet XOR bloku matice a bloku šifrovacího klíče a zároveň získání výsledku. To nebylo možné bez použití dalších možností AVR studia. Splnění podmínky tisíce měření by bylo z tohoto hlediska velmi časově náročné. Automatizované měření by v tomto případě nebylo možné.

6.2.1 Program terminal

První variantou pro komunikaci po sériové lince se zdála komunikace pomocí programu terminal v1.9b. Jedná se o spustitelný soubor bez nutnosti instalace, který poskytuje rychlý přístup k sériovému rozhraní. Mezi jeho funkce, které mohly být využity je možnost odesílání a přijímaní dat v HEX nebo ASCII formátu a logování přijatých a odeslaných dat. Právě formát přenášených dat se stal hlavním úskalím odesílání a přijímání dat z programu AVR, který znaky neposílá v ASCII formátu, tedy bylo by nutné využít funkcí ATOI a ITOA pro převod číselných hodnot. Zadávání matic by nebylo možné provádět dávkou předepsaných nebo předem připravených matic bez jednoduché implementace zdrojového kódu.

6.2.2 Sériová komunikace

Nejvhodnější implementací sériové komunikace se stalo zadávání matic pro rozhraní RS-232 v programu Matlab verze 7.12.0.384. Tato verze programu je vybavena efektivním přístupem k sériové lince bez nutnosti řešení konverze datových formátů. V nové verzi zdrojového kódu upraveného k posílání a příjmu dat ze sériové sběrnice byl vytvořen skript, který obsahuje funkci načítání matice z předem připraveného externího souboru, následné odeslání matice po sériové sběrnici, zpětný příjem vypočtených dat z mikrokontroléru a jejich vypsání do konzole. Rozpoznání matice programem je inicializováno inicializační hlavičkou, která je přednastavena jako vektor deseti hodnot deset. Pro sériovou komunikaci byla zvolena přenosová rychlost 9600Bd, osm datových bitů a jeden stopbit. Parita nebyla nastavena žádná a vstupní buffer byl nastaven na 16 hodnot, které odpovídají matici o rozměru 4x4. Výpis konzole po zpracování operace XOR a příjmu obsahuje odeslaná data, přijatá data a informaci o správnosti proběhlého procesu výpočtu. Pokud by byl proces přerušen nebo jiným způsobem selhal výpočet, bylo nastaveno, aby program do konzole počítal počet neúspěšných výpočtů matic. Pokud by byl tento počet z jakéhokoliv důvodu překročil deset výpočtů, bylo by měření vyhodnoceno jako neúspěšné a proces odesílání dat by byl přerušen.

Stejným způsobem jako skript v programu matlab byl navržen program, který byl vytvořen v programu AVR a nahrán do mikrokontroléru ATmega8515. Program vychází z předchozích zkušeností s měřením proudových průběhů ve smyčce while. Při měření proudových průběhů opakovaného výpočtu stejných hodnot se podařilo přesně synchronizovat výpočetní smyčku funkce XOR, která byla složena z tajného klíče a bloku dat. Díky nemožnosti změny příchozí matice bez programování čipu bylo nutné vytvořit nástavbu programu v C tak, aby se dala data měnit pomocí sériové linky a vpisovat přímo do jeho paměti.

Implementace sériové komunikace proběhla úspěšně. Funkce programu byla změněna tak, aby již neprobíhala stále stejná operace XOR, ale aby mikrokontrolér čekal na vstupní blok dat, která má zpracovat. Hlavním smyslem této nástavby byla možnost měřit automatizovaně velké množství matic v sérii bez zásahu operátora. Tyto matice jsou načítány z externího souboru a odesílány ke zpracování do mikrokontroléru.

Při vlastním měření však bylo zjištěno, že při příjmu a odesílání dat vzniká časová prodleva, kterou nelze jednoduše zasynchronizovat a měřená data byla tímto zpožděním znehodnocována.

6.3 Výsledky měření a jejich zpracování

Při měření elektromagnetické závislosti na proudových špičkách byl kladen důraz na kvantum zpracovávaných číselných hodnot mikrokontrolérem a na počet cyklů v jedné synchronizované smyčce. Dle teorie elektromagnetického postranního kanálu bylo předpokládáno, že právě tyto faktory přímo ovlivňují tvar a amplitudu proudu naindukovaného na měřicí cívce. Měření bylo na základě těchto předpokladů rozvinuto o tyto poznatky.

6.3.1 Synchronizované operace

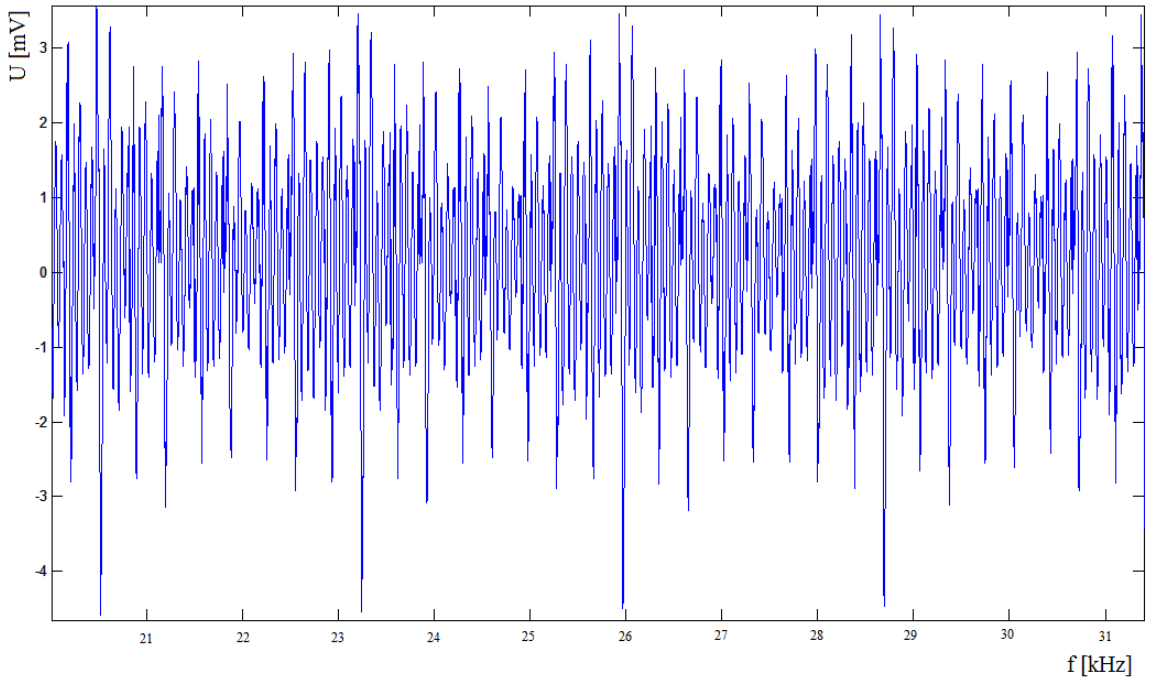
Na osciloskopu byl sledován proudový průběh zachycený elektromagnetickou sondou a po nalezení synchronizačního signálu na druhém kanálu bylo přesně určeno, která datově závislá část proudového průběhu jsou data vhodná k analýze. Z měření vyplynuly průběhy, které zobrazují časovou závislost na množství zpracovávaných dat. Závislost času na počtu provedených operací je patrná z obrA.5, obrA.6, obrA.7 a obrA.8. Při měření byly použity stejné číselné hodnoty matice klíče i matice šifrovaného textu o rozměru 5x5. V prvním průběhu bylo zpracováno celkem pět operací XOR. Z obrázku lze i pouhým okem rozeznat jednotlivé cykly násobení. V ostatních průbězích již byl měřen pětinásobek, desetinásobek a dvacetinásobek původní operace. Paralelně s grafickým snímáním displeje byly hodnoty exportovány do tabulky

v programu excel v množství 100 000 vzorků na zobrazený průběh. Tyto hodnoty byly zároveň zobrazeny v matlabu a dále analyzovány.

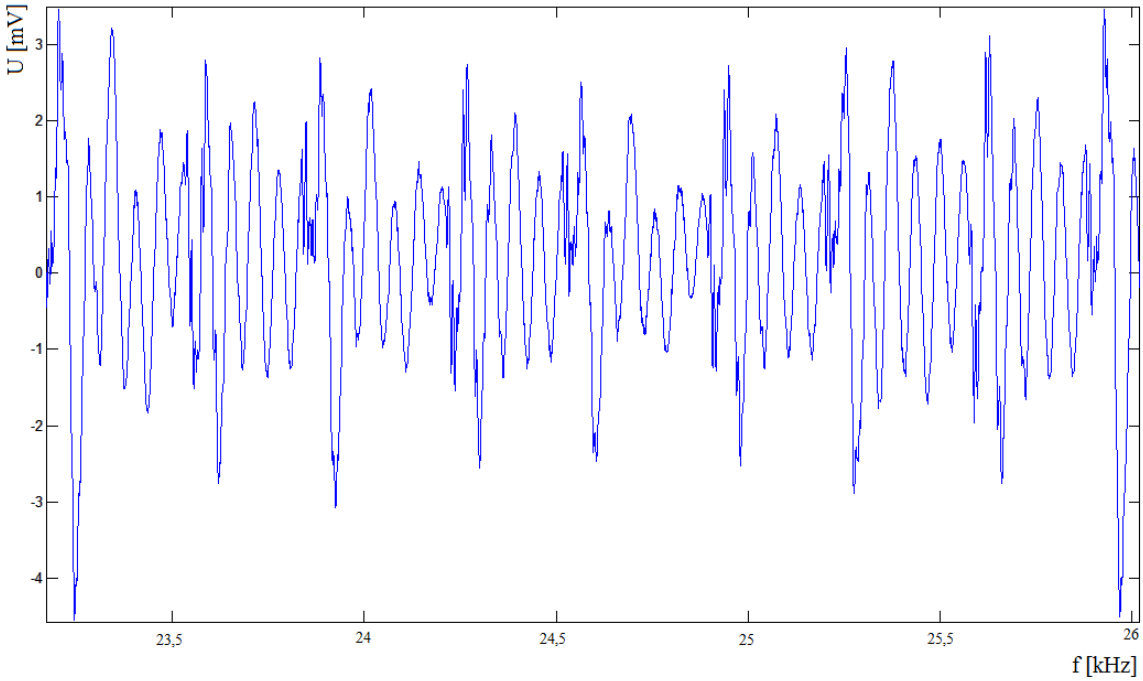
Další porovnání výsledků můžeme sledovat mezi průběhy na obrA.9, kde je zobrazeno porovnání průběhů pěti výpočtů XOR dvou matic,ovšem na horním obrázku jsou hodnoty s výsledkem matice samých jedniček, kdežto na spodním obrázku je zobrazen průběh náhodných čísel různých od nuly. Tyto dva průběhy byly odečítány v programu matlab, aby bylo zjištěno, zda a do jaké míry jsou průběhy odlišné v závislosti na vstupních datech. Výsledná analýza ale ukázala, že jsou naměřené rozdíly obou průběhů tak malé, že je nelze rozeznat.

6.3.2 Nesynchronizované operace

Pro zpracování části úlohy, která měla probíhat plně automatizovaně, byl vytvořen odesílací a přijímací algoritmus, který vyčítal předpřipravená data ze souboru a odesílal je do mikrokontroléru. Při následném měření se zjistilo, že data jsou zpracovávána tak rychle, že není možné je zachytit a jednoduše uložit. Z tohoto důvodu byly měřené průběhy pouze orientační a nebylo je možné použít pro diferenciální analýzu komunikace. Naměřená data byla zaznamenána a uložena pro jednoduchou analýzu v programu matlab. Tato data sebou nesla jedno hlavní úskalí. Průběhy, které byly naměřeny v synchronizační části, byly zobrazeny správně, ovšem nebylo možné s úplnou jistotou určit, které matici má být proudový průběh určen. Uvedené průběhy byly zpracovány skriptem v matlabu určeným pro zpracování naměřených dat z osciloskopu.[18] Zpracované průběhy jsou naznačeny na obr.6.3 a obr.6.4.



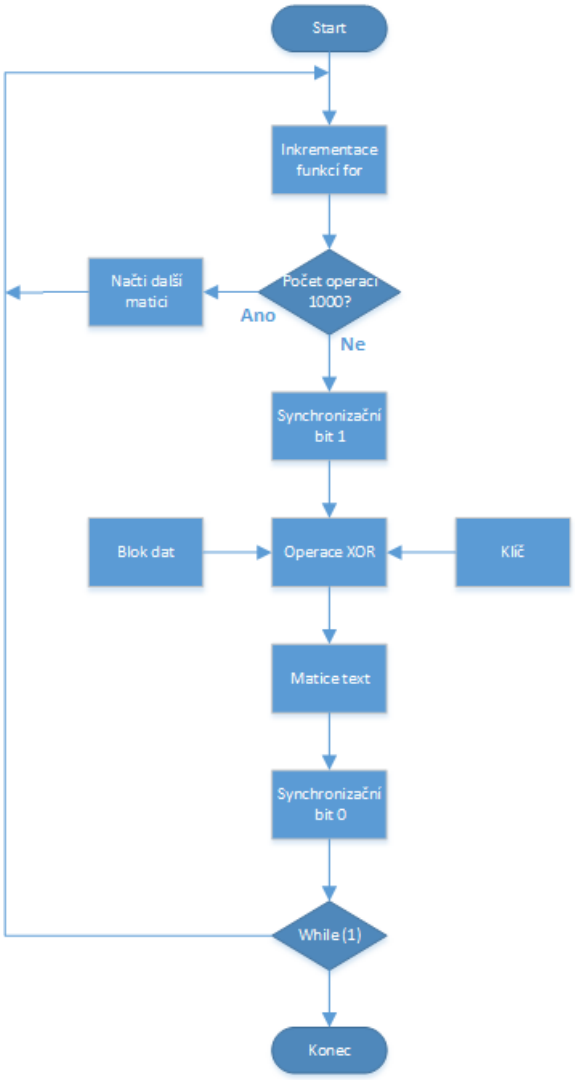
Obr. 6.3: Zpracovaný vzorek operace XOR matice



Obr. 6.4: Zpracovaný vzorek operace XOR jednoho řádku

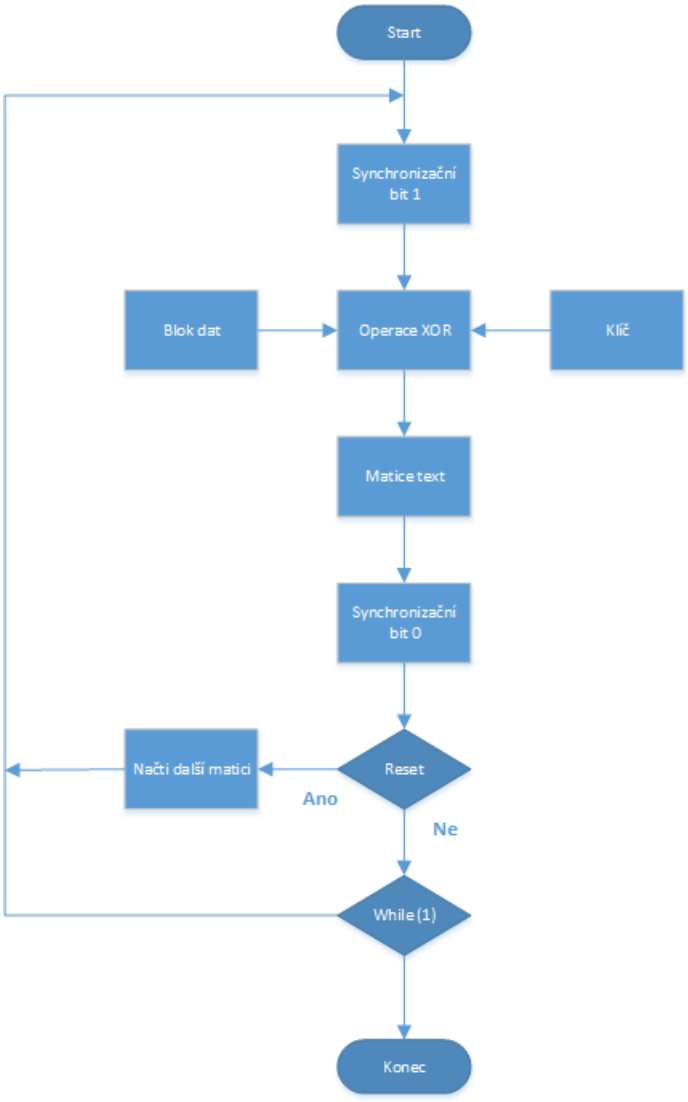
6.3.3 Možná řešení pokročilých metod měření

Pro řešení problémů s rozeznáním a přiřazením správných údajů k naměřeným křivkám se nabízejí dvě řešení. Prvním řešením by bylo opakovat měřicí smyčku každé matice po určitou dobu potřebnou pro její zaznamenání. Toho by bylo možné dosáhnout opakováním zpracování každé dvojice klíč a text pomocí operace XOR tisícinásobkem počtu stejných operací. Toto opakování by zaručilo určitou prodlevu mezi měřenými průběhy a poskytlo dostatek času pro synchronizaci a záznam průběhu jednotlivých výsledků. Vývojový diagram řešení lze vidět na obr6.5



Obr. 6.5: Řešení programu pomocí přetečení zásobníku

Druhým možným řešením je uvést do smyčky výpočtu požadavek na přerušení. Takové přerušení by reagovalo na vstupní impulz daný měřící osobou pomocí jednoho z přepínačů, které jsou součástí vývojové desky AVR STK500. Funkce tohoto přerušení by zajišťovala, že bude probíhat operace XOR matice klíče a matice dat, dokud nebude sepnut spínač. Po sepnutí spínače by byla zpracovávána matice následující v připraveném souboru. Tato metoda ovšem zcela nevyhovuje podmínce plně automatizovaného měření. Řešení je naznačeno na obr6.6



Obr. 6.6: Řešení programu pomocí externího přerušení

6.3.4 Měření a ukládání hodnot

Pro ukládání hodnot v diplomové práci bylo využito výstupního portu USB. V tomto portu byl připojen USB flash disk. Na flash disk byly exportovány naměřené hodnoty spolu s průběhy zobrazenými na displeji osciloskopu. Ke správnému zobrazení zasynchronizovaného signálu bylo využito funkce osciloskopu Trigger Holdoff, která umožnila zastavit a stabilizovat kontinuálně probíhající křivky podle nástupné nebo sestupné hrany synchronizačního signálu přivedeného na druhý kanál. [17] Pro rozšíření úlohy na plně automatizovanou by bylo třeba využít možnosti komunikace osciloskopu s počítačem po rozhraní SPI, USB nebo ethernet a příslušných ovladačů a software. Možnost využití připojení k PC nebyla využita z důvodu špatné synchronizace u pokročilé verze vytvořeného programu.

7 ZÁVĚR

Cílem diplomové práce bylo prostudovat problematiku elektromagnetického postranního kanálu a princip jednoduché a diferenční elektromagnetické analýzy. Mezi další cíle patřilo realizovat experimentální pracoviště, na kterém by bylo možné provést 1000 měření bez nutnosti obsluhy a vytvořit program, který umožní měnit automaticky zpracovávané informace. Na základě vytvořeného programu měla být uskutečněna jednoduchá a diferenční analýza na základě které mělo být diskutován vliv počtu naměřených výsledků na DEMA.

V diplomové práci byly prozkoumány metody jednoduché a diferenční analýzy. Na principu proudového postranního kanálu byla vysvětlena funkce elektromagnetického postranního kanálu, který s proudovým postranním kanálem úzce souvisí. Diplomová práce obsahuje k dokreslení situace i popis ostatních postranních kanálů a typy možných útoků prováděné na kryptografické systémy.

K prozkoumání poznatků o elektromagnetické analýze bylo v laboratorních podmínkách vytvořeno experimentální pracoviště vybavené odpovídajícími součástmi. Vybavení sestává z osciloskopu tektronix, elektromagnetické sondy, sériového převodníku USB/RS-232, vývojové sady pro procesory atmel a PIC a počítače s nainstalovaným softwarem AVR studio a matlab. K pracovišti bylo v rámci diplomové práce vytvořeno měřicí zařízení, které umožňuje přesné zaaretování sondy na cílový bod a zaručuje neměnnost polohy systému i při vibracích a lehké manipulaci.

Druhá polovina vlastního řešení byla věnována zprovoznění komunikace mezi PC a testovacím kitem. Tato část úkolu byla realizována úspěšně. Ověření funkce komunikace proběhlo na základě testovacího programu nightrider, na kterém byla ověřena teorie elektromagnetického kopírování obálky signálu vstupního proudu.

Hlavním úkolem byla realizace programu pro automatizované měření matematických operací bez zásahu operátora. Tento program byl vytvořen v programu AVR. Pro zadávání dávek matic pro výpočet byly vytvořeny soubory v programu matlab, které mají za úkol po sériové lince automaticky dopravit zadané matice do mikrokontroléru, který je následně zpracuje a výsledek opět vyšle sériovým rozhraním do PC. Právě zpracovávání odeslaných dat z PC mikrokontrolérem má za následek změny slabého elektromagnetického pole tvořícího se u jeho napájecího portu. Proudové změny na napájecím vstupu mikrokontroléru se měly stát předmětem jednoduché a diferenciální analýzy postranního kanálu. Při měření se vyskytly dosud nepředvídané problémy díky automatizaci měření. Problémy byly způsobeny desynchronizací měřicí smyčky při příjmu a odesílání matic do zařízení a jejich zpětném vyčítání. Následkem toho nebylo možné dokončit diferenční analýzu DEMA, která byla posledním bodem diplomové práce.

Z důvodů desynchronizace byly navrženy úpravy směřující k vyřešení problémů

s ní spojené. Ve vývojových diagramech byly doplněny možnosti úpravy zdrojového kódu nahraného v zařízení tak, aby byly vzniklé problémy eliminovány. V přílohách jsou uvedeny změřené průběhy u jednotlivých způsobů měření. Zpracování naměřených průběhů byo provedeno v programu matlab a jeho výstupy jsou také uvedeny v příloze.

LITERATURA

[1] Wobst, Reinhard *Cryptology unlocked* John Wiley and Sons,Ltd 2001, přeloženo Angelika Shafir 2007, ISBN 978-0-470-06064-3

[2] 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.

[3] Microchip, Atmega8515L *Data Sheet* [online]. 2012, [cit. 13. 11. 2012]. Dostupné z URL: <http://www.atmel.com/Images/doc2512.pdf>.

[4] V.Klíma, T.Rosa *O postranních kanálech, nové maskovací technice a jejím konkrétním využití proti Mangerovu útoku* [online]. 2001, [cit. 13. 11. 2012]. Dostupné z URL: <http://mkb.buslab.org/_archiv/2001/KlimaRosa.pdf>.

[5] S.Mangard, E.Oswald, T.Popp *Power Analysis Attack Revealing the Secrets of Smart Cards* Springer science+Business Media,LLC 2007, [cit. 13. 11. 2012]. ISBN-13: 978-0-387-30857-9

[6] Doc. Ing. Daniel Cvrček, Ph.D,. *Problémy odolných kryptografických zařízení* [online]. [cit. 13. 11. 2012]. Dostupný z WWW: <http://www.fit.vutbr.cz/~cvrcek/cards/karty.html.cs>.

[7] Doc. Ing. Karel BURDA, CSC., *Bezpečnost informačních systémů* Brno : [s.n.], 2005. 104 s

[8] Doc. Ing. Daniel Cvrček, Ph.D,. *Návrh digitálních integrovaných obvodů VLSI a jazyk VHDL* [online]. [cit. 13. 11. 2012]. Dostupný z WWW: <http://www.umel.feec.vutbr.cz/BNDI/skripta/Navrh_digitalnich_integrovanych_obvodu_a_jazyk_VHDL_S.pdf>.

[9] Z.Martinásek, O.Nečas, V.Zeman, J.Martinásek *Diferenciální elektromagnetická analýza* Brno : 2011/60, 28. 11. 2011

[10] Siddika Berna Ors Yalcin *SIDE CHANNEL ATTACKS ON HARDWARE IMPLEMENTATIONS OF CRYPTOGRAPHIC ALGORITHMS* [cit. 13. 11. 2012]. Dostupný z WWW: <http://web.itu.edu.tr/~orssi/dersler/cryptography/slides.pdf>.

[11] Z.Martinásek, V.Člupek, V.Zeman,P.Sysel *Základní metody diferenciální proudové analýzy* [cit. 10. 12. 2012]

[12] Federal Information Processing Standards Publication 197 *Announcing the advanced encryption standard (AES)* [cit. 13. 11. 2012]. Dostupný z WWW: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

[13] Elke de Mulder *Electromagnetic Techniques and Probes for Side-Channel Analysis on Cryptographic Devices* [cit. 10. 12. 2012] Arenberg Doctoral School of Science, Engineering and Technology, Faculty of Engineering, Department of Electrical Engineering (ESAT) November 24, 2010

[14] Kocher, Paul C. *Timing Attacks on Implementations of Diffie - Hellman, RSA, DSS, and Other Systems* [cit. 13. 11. 2012]. Dostupný z WWW: <http://www.cryptography.com/public/pdf/TimingAttacks.pdf>.

[15] Alexandre Berzati, Cécile Canovas, Jean-Guillaume Dumas,Louis Goubin *Fault Attacks on RSA Public Keys: Left-To-Right Implementations are also Vulnerable* [cit. 25. 5. 2013]. Dostupný z WWW: <http://hal.archives-ouvertes.fr/docs/00/56/09/31/PDF/rsa_laser.pdf>.

[16] Jerome Di-Battista, Jean-Christophe Courrege, Bruno Rouzeyre, Lionel Torres, Philippe Perdu *When Failure Analysis Meets Side-Channel Attacks* [cit. 25. 5. 2013]. Dostupný z WWW: <http://www.iacr.org/archive/ches2010/62250180/62250180.pdf>.

[17] Tektronix *DPO4000 Series Digital Phosphor Oscilloscopes* [cit. 25. 5. 2013]. Dostupný z WWW: <http://www.tequipment.net/pdf/tektronix/DPO4000_UserManual.pdf>.

[18] Elisabeth Oswald *Guided Analysis of WS1* [cit. 25. 5. 2013]. Dostupný z WWW: <http://www.dpabook.org/onlinematerial/matlabscripts/WS1-Guided-Exercise.pdf>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

AES Advanced encryption standard

$ASCII$ American Standard Code for Information Interchange

$CMOS$ Complementary Metal Oxide Semiductor

$DEMA$ Differential electromagnetic analysis

DFA Differential fault analysis

DPA Differential power analysis

DTA Differential time analysis

$NIST$ National Institute of Standard and Technology

SFA Simple fault analysis

SPA Simple power analysis

STA Simple time analysis

$SEMA$ Simple electromagnetic analysis

SEZNAM PŘÍLOH

A Příloha **47**

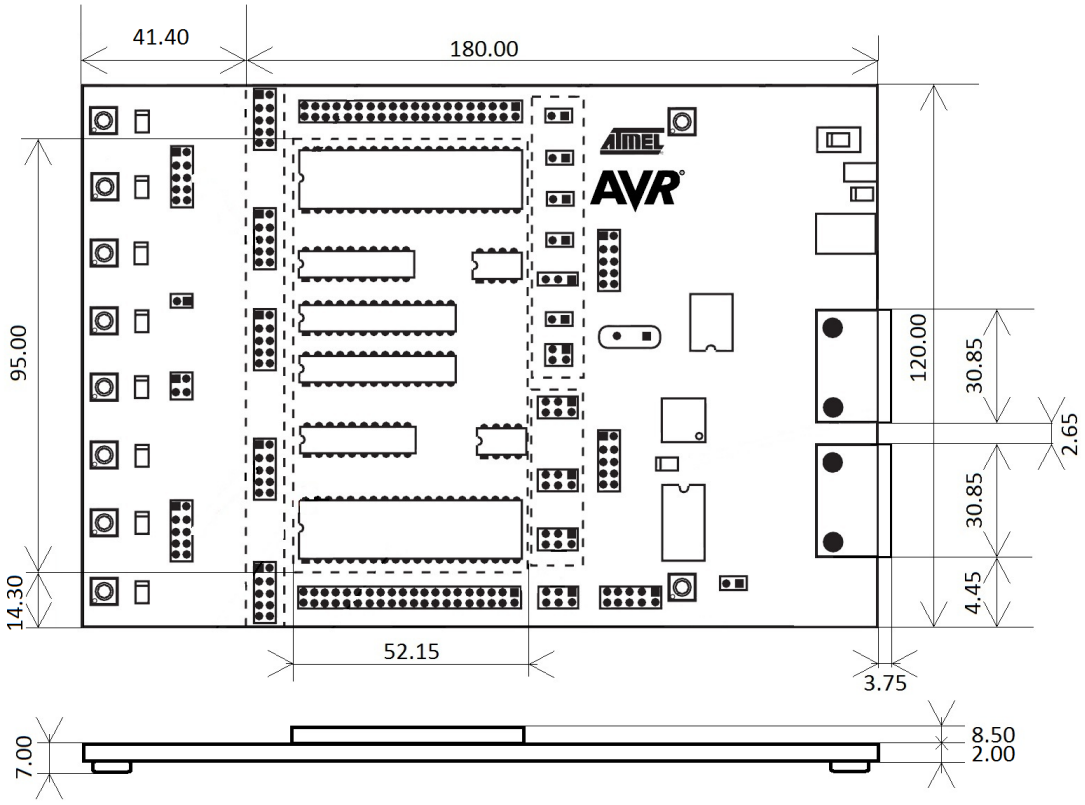
A.1 Naměřené rozměry testovacího kitu 47

A.2 Rozkreslení úchytného zařízení 48

A.3 Naměřené průběhy signálů 50

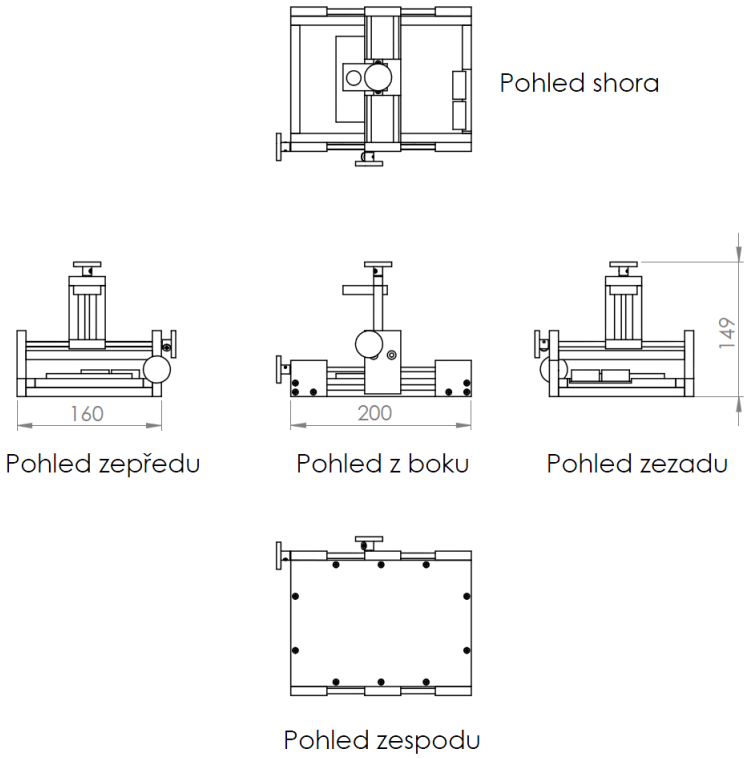
A PŘÍLOHA

A.1 Naměřené rozměry testovacího kitu

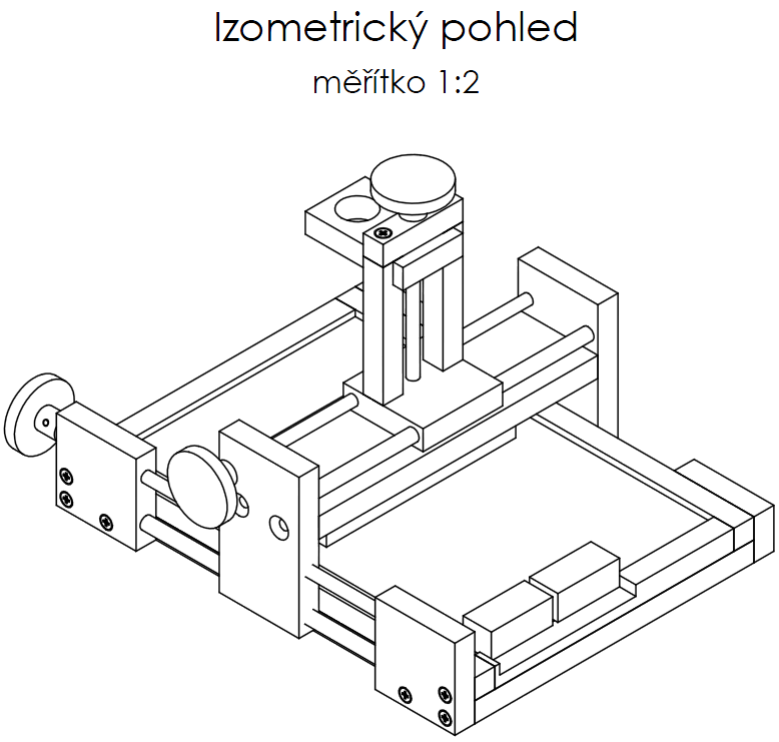


Obr. A.1: Testovací kit

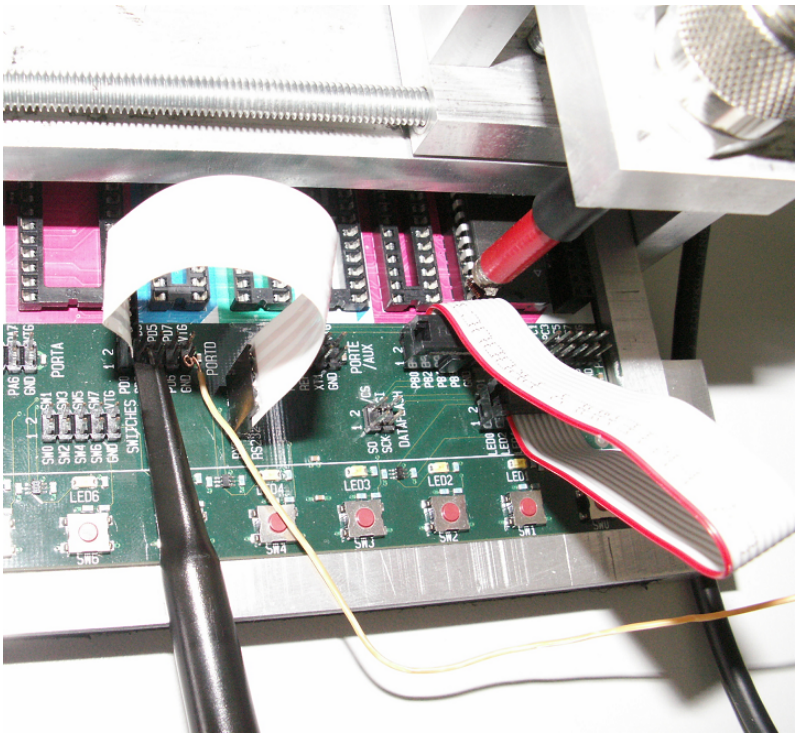
A.2 Rozkreslení úchytného zařízení



Obr. A.2: Jednotlivé pohledy na úchytné zařízení

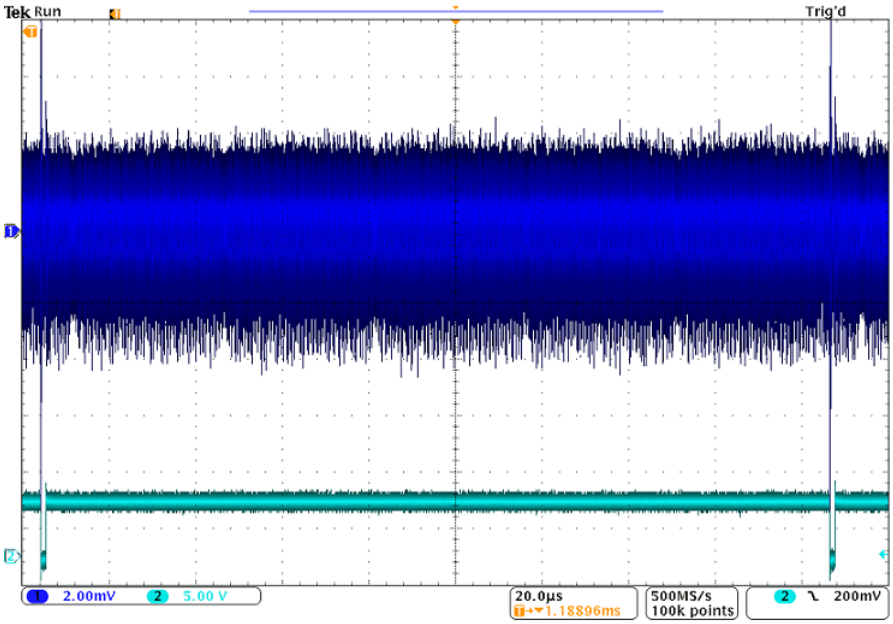


Obr. A.3: Izometrické zobrazení úchytného zařízení

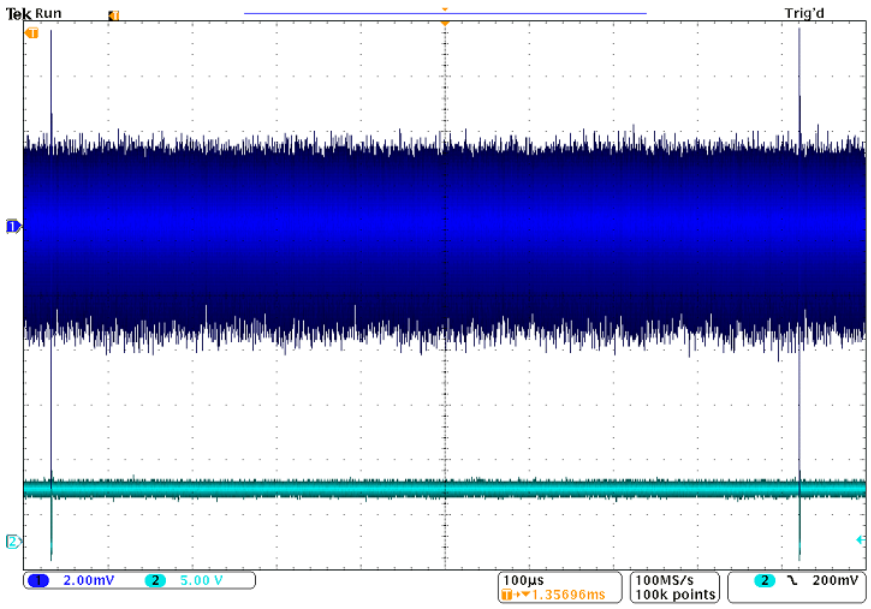


Obr. A.4: Reálné zapojení pinů na AVR STK500

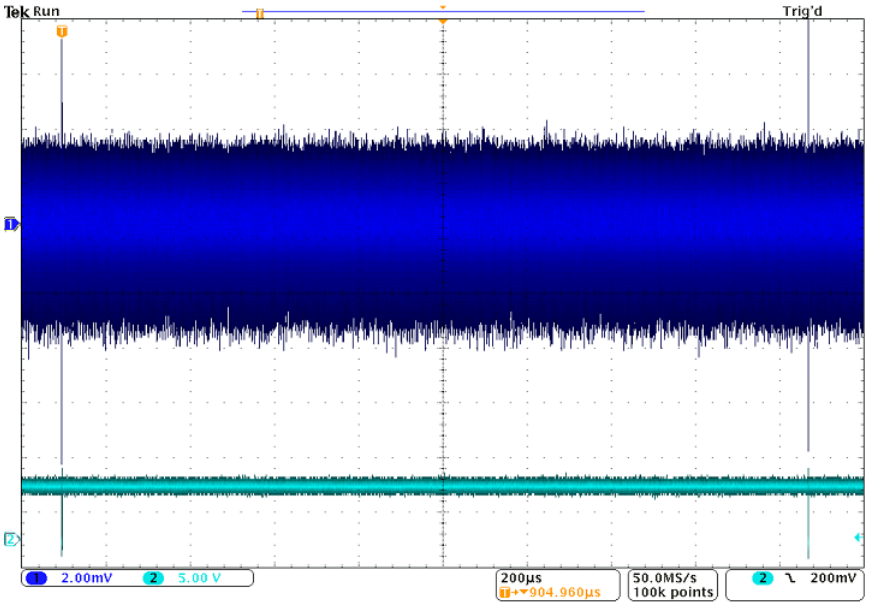
A.3 Naměřené průběhy signálů



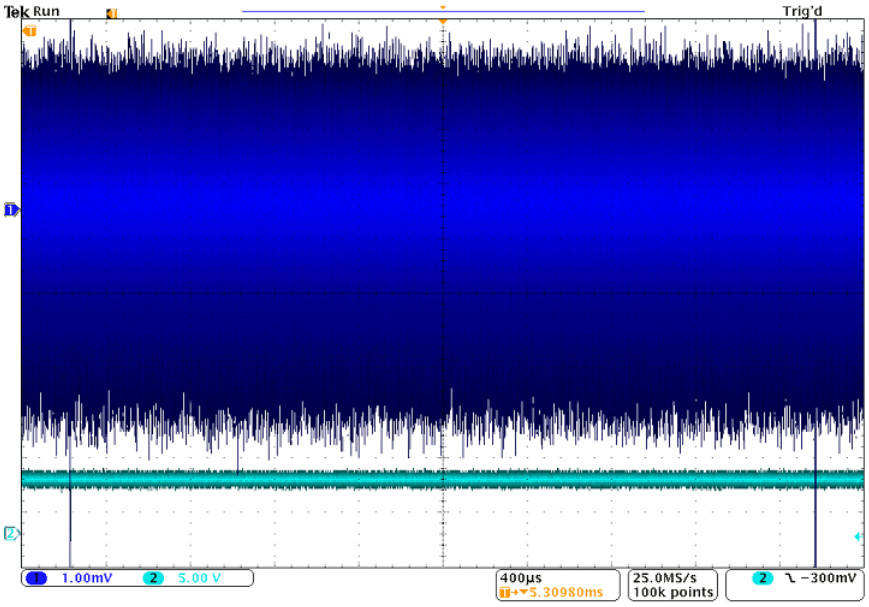
Obr. A.5: Průběh operace XOR pro 5 výpočtů



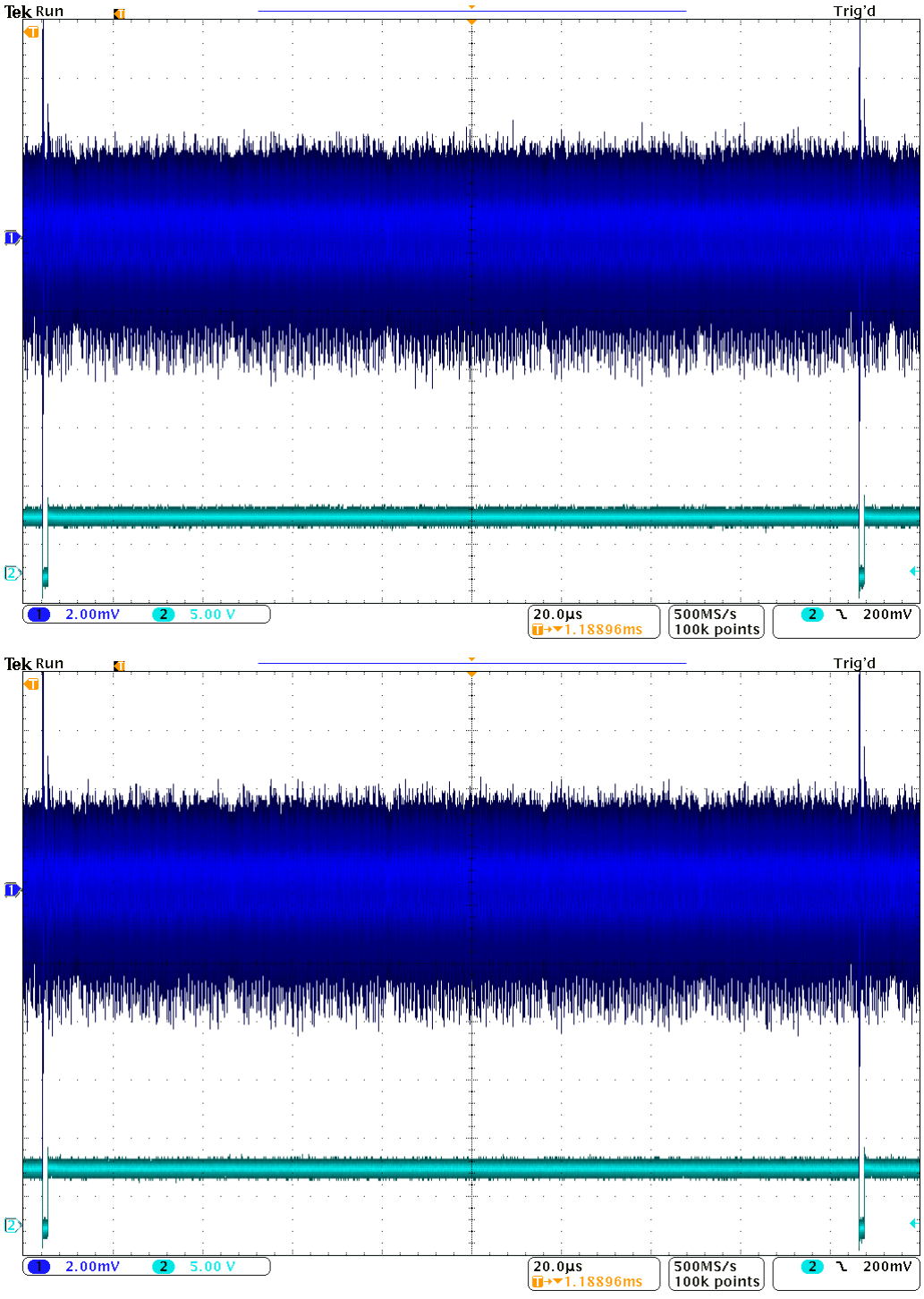
Obr. A.6: Průběh operace XOR pro 25 výpočtů



Obr. A.7: Průběh operace XOR pro 50 výpočtů



Obr. A.8: Průběh operace XOR pro 100 výpočtů



Obr. A.9: Srovnání vzorků matic 1x0 s 1xdata