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

OPTICKÝ POSTRANNÍ KANÁL

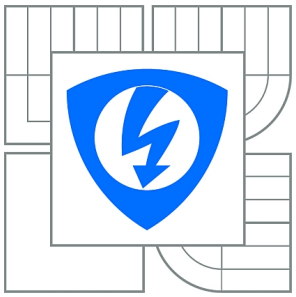
BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE JOSEF KOLOFÍK
AUTHOR

BRNO 2010

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

OPTICKÝ POSTRANNÍ KANÁL

OPTICAL SIDE CHANNEL

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

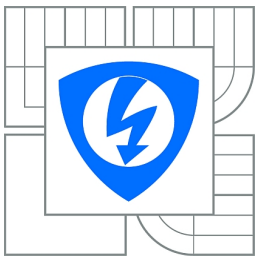
AUTOR PRÁCE — JOSEF KOLOFÍK

AUTHOR

VEDOUCÍ PRÁCE — Ing. ZDENĚK MARTINÁSEK

SUPERVISOR

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Josef Kolofík	***ID:***	112050
Ročník:	3	***Akademický rok:***	2009/2010

NÁZEV TÉMATU:

Optický postranní kanál

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte základní útoky postranními kanály na kryptografický modul. Z nastudovaných teoretických vědomostí vypracujte detailní přehled současného stavu problematiky. Zaměřte se na optický postranní kanál a na možné způsoby využití. Prostudujte vhodné odkrývací metody čipu a detekce fotonu. Z nastudovaných znalostí navrhněte a realizujte program analyzující data z vybraného postranního kanálu, který by bylo možné po modifikaci snímací části použít i pro analyzování dat z optického postranního kanálu.

DOPORUČENÁ LITERATURA:

[1] HLAVÁČ, M. FERRIGNO, J. When AES blinks: introducing optical side channel. In IET Information Security. 1st edition. [s.l.] : [s.n.], 2008. s. 5.
[2] KOCHER, P., JAFFE, J., JUN, B.: Introduction to Differential Power Analysis and Related Attacks, San Francisco, 1998.

Termín zadání:	29.1.2010	***Termín odevzdání:***	2.6.2010

Vedoucí práce: Ing. Zdeněk Martinásek

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

UPOZORNĚNÍ:

ABSTRAKT

Tato práce se zabývá problematikou optického postranního kanálu a využitím neuronové sítě jako klasifikátoru dat. První část práce se zabývá základy kryptografie a útoky na kryptografický modul. Druhá část práce se zabývá metodami odkrytování mikrokontroléru, technologickými postupy odkrytování a metodami detekce fotonu. Třetí část práce se zabývá využitím neuronové sítě jako základu softwaru pro rozpoznávání a klasifikaci dat. V závěru práce je popsán postup při vytváření tohoto softwaru, rozebrán zdrojový kód a otestována funkčnost celého řešení.

KLÍČOVÁ SLOVA

kryptografie, postranní kanál, optický postranní kanál, odkrytování mikrokontroléru, neuronová síť, klasifikátor

ABSTRACT

This thesis deals with the optical side channel and using a neural network as classifier of data. The first part deals with the basics of cryptography and attacks on the cryptographic module. The second part deals with methods of decapsulation the microcontroller, decapsulation technological processes and methods of detection of photons. The third part deals with the use of neural networks as the basis of recognition and data classification software. In conclusion, the thesis describes the procedure for creating this software, analyzes the source code and tests the functionality of this solution.

KEYWORDS

cryptography, side channel, optical side channel, decapsulation the microcontroller, neural network, classifier

KOLOFÍK, Josef *Optický postranní kanál*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2010. 51 s. Vedoucí práce byl Ing. Zdeněk Martinásek

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Optický postranní kanál“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

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

Brno ....

(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucímu práce Ing. Zdeňku Martináskovi za účinnou pedagogickou a odbornou pomoc a další cenné rady při zpracování mé bakalářské práce.

Brno ....

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Cílem práce je získání informací o novém optickém postranním kanálu a vytvoření souhrnného přehledu o jeho aplikaci. První část práce se bude zabývat funkcí kryptografického modulu a možnými typy útoků na tento modul.

Dále se práce bude zabývat vnitřním uspořádáním jednočipových integrovaných obvodů, které jsou často využívány právě ve funkci kryptografických modulů. Cílem této části je provedení několika experimentů k ověření informací uváděných výrobci a zjištění informací, které nejsou běžně uváděny v katalogových listech výrobků. Na základě získaných informací budou všeobecně rozebrány metody odkrytování čipu integrovaného obvodu. Pro některou metodu odkrytování proveditelnou v laboratorních podmínkách Ústavu telekomunikací FEKT VUT v Brně bude uveden podrobnější postup a tento bude prakticky ověřen. V další části práce bude rozebrán postup získávání informací pomocí optického postranního kanálu včetně základních principů detekce fotonů.

Poslední část práce se bude zabývat použitím neuronových sítí a bude tvořit stěžejní část praktické části práce. Na základě informací o neuronových sítích bude navržen program pro rozpoznávání a klasifikaci dat z postranních kanálů, který bude možné upravit i pro rozpoznávání dat z optického postranního kanálu.

1 ÚVOD DO KRYPTOGRAFIE

V současné době dospělo praktické využití elektronických obvodů do takové míry, že jsou využívány téměř v každém zařízení. S takovýmto rozvojem přišla také potřeba propojení jednotlivých zařízení za účelem vzájemné komunikace a výměny dat. Obecně lze takové spojení považovat za systém, konkrétněji za systém určený ke zpracování a přenosu dat.

Celková oblast využití těchto systémů zahrnuje i oblasti pracující s daty, jejichž únik či změny během přenosu by mohly znamenat vysoké bezpečnostní riziko různého charakteru. Aby bylo možné únikům a změnám dat zamezit, je třeba tyto systémy vhodně kryptograficky zabezpečit.

1.1 Požadavky na kryptograficky zabezpečený systém

Jako příklad oblastí pracujících s citlivými daty zde může posloužit uvedení některých konkrétních oblastí:

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

V návaznosti na příklad oblastí pracujícími s rizikovými daty je vhodné uvést také příklady spojení se základními kryptografickými požadavky.

V systémech využívaných armádou se nejvíce uplatní fakt, že přenášeným datům smí porozumět pouze jejich adresát. Může tím být tedy definován pojem důvěrnosti mezi odesilatelem a adresátem. Pokud tento pojem vztáhneme i na kryptografický systém, pak lze důvěrnost definovat jako jeden ze základních kryptografických požadavků na zabezpečený systém.

Jako další příklad poslouží oblast bankovnictví, kde je požadováno, aby byla zcela jednoznačně určena spojitost mezi autorem a daty a nebylo tedy možné zaměnit data od různých autorů. Konkrétněji může být tento princip znázorněn například při elektronické platbě, kdy musí být zcela jistě určeno, že příkaz k platbě pochází od majitele konta. Tento princip pak definuje autentičnost dat.

Posledním příkladem je oblast informačních technologií, která je v dnešní době prakticky nepostradatelná a využívají ji všechny již zmíněné oblasti. Komunikace prostřednictvím informačních technologií je prakticky ve všech případech zabezpečená.

Jedním ze základních principů zabezpečení byl v minulosti prostý kontrolní součet (v dnešní době se používají modernější metody, základem je např. hash funkce), kterým je prokazatelné a ověřitelné, že data nebyla během přenosu nijak změněna, což definuje pojem integrita dat.

Využití systémů pro zpracování a přenos dat v těchto oblastech vyžaduje kryptografické zabezpečení těchto systémů. Kryptograficky zabezpečený systém musí splňovat základní kryptografické požadavky vyplývající z výše uvedených příkladů: důvěrnost – přenášeným datům smí porozumět pouze jejich adresát, nikdo jiný, autentičnost – musí být jednoznačně prokazatelná spojitost mezi daty a jejich autorem, integrita dat – musí být prokazatelné a ověřitelné, že data nebyla při přenosu nijak změněna [1].

1.2 Kryptografický modul

Všechny výše uvedené služby zajišťuje kryptografický modul, jehož realizace může být hardwarová nebo softwarová. Kryptografický modul pracuje na základě využití kryptografických protokolů a kryptografických algoritmů. Hlavním úkolem kryptografického modulu je realizace resp. implementace konkrétního kryptografického řešení. Kryptografické moduly jsou zařazovány do všech systémů, u kterých je požadováno zabezpečení dat, zejména však tam, kde hrozí vysoké riziko útoku a únik tajných dat [1], [2].

1.3 Kryptografický algoritmus

Kryptografickým algoritmem se rozumí samotný princip zabezpečení dat. Velmi obecně lze tedy kryptografický algoritmus považovat za posloupnost operací v nakládání s daty při jejich cestě ze vstupu kryptografického bezpečnostního modulu na výstup kryptografického bezpečnostního modulu. Z matematického hlediska se jedná o funkci, která s použitím šifrovacího klíče transformuje data do podoby, ve které není možné původní data získat bez znalosti šifrovacího klíče. Cílem není utajit algoritmus šifrování, cílem je utajit šifrovací klíč. Z hlediska využití šifrovacího klíče jsou rozlišovány dva druhy šifrovacích algoritmů:

- symetrický algoritmus,
- asymetrický algoritmus.

Symetrický algoritmus využívá k šifrování i dešifrování informace shodný šifrovací klíč. U asymetrického algoritmu existují klíče dva, jeden sloužící k šifrování, druhý k dešifrování informace [1].

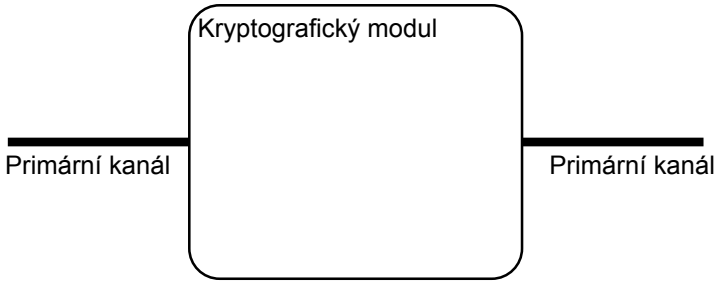
1.4 Kryptografický protokol

Kryptografickým protokolem je označován souhrn pravidel pro aplikaci kryptografického algoritmu, způsoby komunikace mezi jednotlivými moduly a implementaci v hardwarovém prostředí. Samotná hardwarová implementace mnohdy není jednoznačně definována, čímž pak dochází k nezávislosti protokolu na hardwaru a tím vzniká prostor pro útok na modul využitím postranních kanálů, které jsou mimo jiné založeny také na využití hardwarových nedostatků v zabezpečení [1], [2].

2 ÚTOKY NA KRYPTOGRAFICKÝ MODUL

2.1 Funkce kryptografického bezpečnostního modulu

Kryptografický bezpečnostní modul lze jednoduše znázornit jako systém se dvěma primárními kanály, kterými modul komunikuje s ostatními zařízeními, případně s dalšími moduly. Jednoduché grafické znázornění kryptografického bezpečnostního modulu uvádí obrázek 2.1.



Obr. 2.1: Kryptografický bezpečnostní modul.

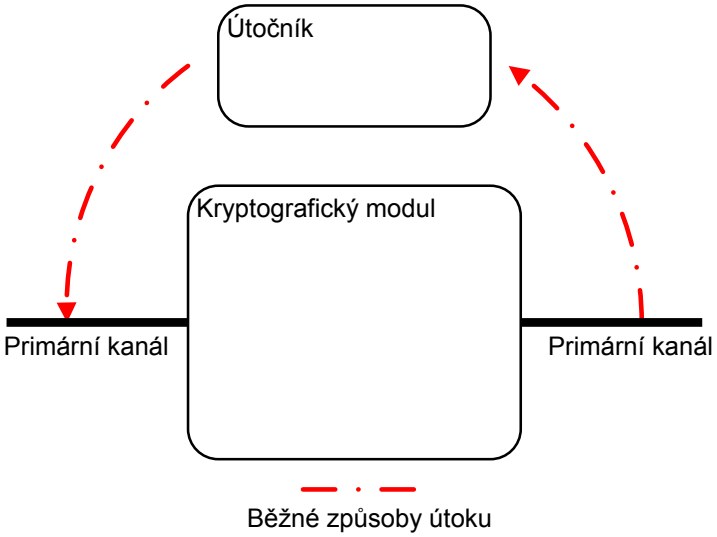
Jeden primární kanál slouží jako vstup, druhý primární kanál slouží jako výstup. Na vstup jsou zpravidla přiváděna data určená k šifrování. Uvnitř modulu dochází k aplikaci kryptografického algoritmu s použitím šifrovacího klíče a z výstupu jsou zpravidla odesílána šifrovaná data dále dalšímu zařízení nebo dalšímu kryptografickému bezpečnostnímu modulu [2].

2.2 Běžné útoky na kryptografický modul

Útoky na kryptografický modul byly dříve prováděny využitím primárních kanálů. Útočník na vstup zavedl vlastní datovou posloupnost a na základě analýzy výstupních dat byl schopen určit jakým způsobem kryptografický modul šifruje data a jaký k tomuto účelu využívá šifrovací klíč. Způsob využití znázorňuje obrázek 2.2.

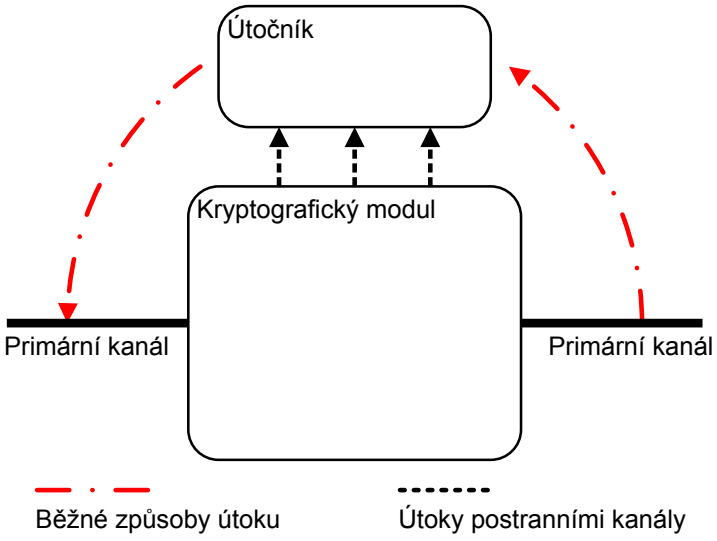
2.3 Útoky postranními kanály

Kryptografický modul při své činnosti spotřebovává elektrický proud, průchodem proudu vytváří ve svém okolí elektromagnetické pole, vyzařuje do okolí teplo a dále například vykazuje také zpoždění mezi primárním vstupem a výstupem. Souvislost



Obr. 2.2: Běžné útoky na kryptografický bezpečnostní modul.

mezi operacemi prováděnými uvnitř kryptografického modulu a uvedenými projevy jeho funkce vytváří postranní kanál, tedy nepřímý únik informací využitelných k prolomení šifrovacího klíče. Obrázek 2.3. znázorňuje využití všech útoků na kryptografický bezpečnostní modul [2], [3].



Obr. 2.3: Všechny útoky na kryptografický bezpečnostní modul.

2.3.1 Přehled využívaných postranních kanálů

Elektromagnetický postranní kanál

Elektromagnetický postranní kanál využívá skutečnosti, že při činnosti elektronického obvodu vzniká v důsledku průchodu elektrického proudu elektromagnetické pole. Jelikož prakticky všechny kryptografické moduly obsahují elektronické části, je možné u všech těchto modulů využít elektromagnetický postranní kanál, který je postaven na souvislosti velikosti elektromagnetického pole s operací prováděnou uvnitř kryptografického bezpečnostního modulu. Vhodnou analýzou elektromagnetického pole v okolí kryptografického bezpečnostního modulu je možné získat informace vedoucí k prolomení šifrovacího klíče.

Časový postranní kanál

Časový postranní kanál je založen na souvislosti mezi operací prováděnou uvnitř kryptografického bezpečnostního modulu a zpožděním mezi vstupem a výstupem kryptografického bezpečnostního modulu. Ze zjištěného zpoždění je možné zjistit, jak dlouhý klíč byl použit, protože doba zpracování dat je téměř ve všech případech úměrná délce klíče, případně u některých algoritmů lze takto přímo určit šifrovací klíč.

Výkonový postranní kanál

Výkonový postranní kanál je založen na spojitosti mezi operací prováděnou uvnitř kryptografického bezpečnostního modulu a jeho proudovým odběrem. Analýzou proudového odběru pak lze získat informace vedoucí k prolomení šifrovacího klíče.

Chybový postranní kanál

Chybový postranní kanál využívá spojitosti mezi uměle vytvořenou chybou a chybovým hlášením kryptografického bezpečnostního modulu. Útočník při vytvoření umělé chyby a následné analýzy takto vzniklého chybového hlášení může získat informace vedoucí k prolomení šifrovacího klíče.

Optický postranní kanál

Optický postranní kanál využívá fyzikální vlastnosti obvodu. Paměťová buňka při změně logického stavu emituje do svého okolí malé množství fotonů. Zachycením fotonů může útočník získat informace vedoucí k prolomení šifrovacího klíče. Více bude tato metoda rozebrána v následující kapitole.

3 OPTICKÝ POSTRANNÍ KANÁL

3.1 Základní princip

Jak již bylo zmíněno v předchozí kapitole, optický postranní kanál využívá fyzikální vlastnosti obvodu. Prvotní myšlenka jeho využití je velmi jednoduchá, spočívá ve skutečnosti, že při změně logické úrovně v základní paměťové buňce složené z tranzistorů jsou do okolí buňky emitovány fotony. Vhodným zachycením fotonů lze zjistit, které tranzistory změnily svůj stav. Z této informace je pak možné odvodit obsah paměti a tedy i tajná data [4].

Předpokladem pro úspěšnou aplikaci metody optického postranního kanálu je vhodné odkrytování čipu kryptografického modulu a využití vhodného detektoru fotonů, čímž se zabývají následující kapitoly.

3.2 Příprava vzorku pro analýzu

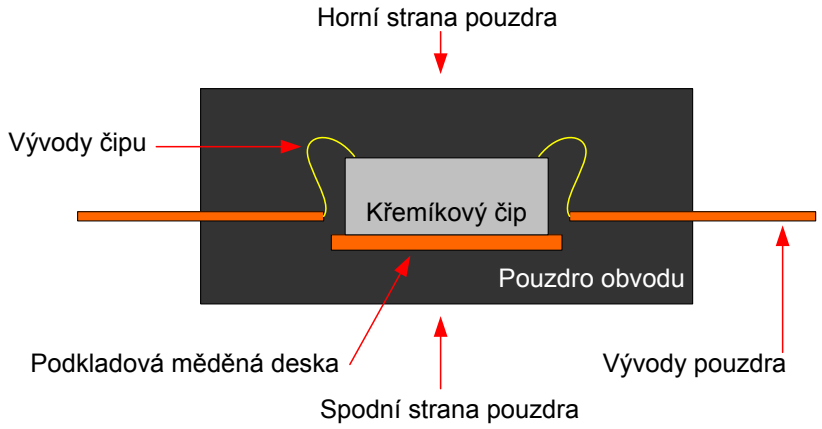
Počátkem přípravy vzorku vhodného k analýze pomocí optického postranního kanálu je odstranění části pouzdra obvodu. Pro efektivní přípravu je třeba znát postup výroby a uspořádání uvnitř pouzdra. Samotný obvod je vytvořen v křemíkové destičce, postup výroby samotného čipu není v tomto okamžiku stěžejní, postačí pouze fakt, že obvod jako takový je tvořen jednou křemíkovou destičkou s vhodně upravenými vývody.

Aby bylo možné takový obvod využít v praxi je třeba jej umístit do normalizovaného pouzdra opatřeného klasickými vývody (měděnými pásky nebo dráty). Běžným postupem při pouzdření čipu do pouzdra DIL (SIL a jiných) je výroba kovového rámečku, který obsahuje vývody a desku, která slouží jednak jako podklad pro čip a jednak napomáhá chlazení čipu. Čip je na desku nalepen pomocí pryskyřice s příměsí stříbra. Vývody čipu jsou s vývody budoucího pouzdra propojeny velmi tenkými vodiči. Takto připravený polotovar je následně zalit do plastu, čímž je proces výroby dokončen. Obrázek 3.1 znázorňuje vnitřní uspořádání pouzdra hotového integrovaného obvodu [5].

3.2.1 Základní metody odkrytování

Pro samotnou analýzu je třeba získat přístup k čipu, což lze provést postupem opačným k postupu výroby [13]. Základní obecné metody postupu odkrytování jsou dvě:

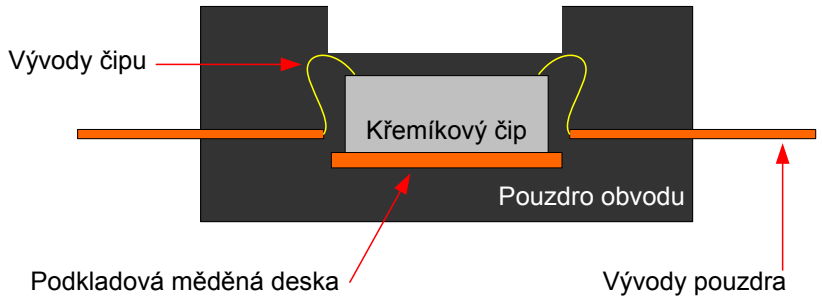
- horní stranou pouzdra,
- spodní stranou pouzdra.



Obr. 3.1: Řez pouzdrem hotového integrovaného obvodu.

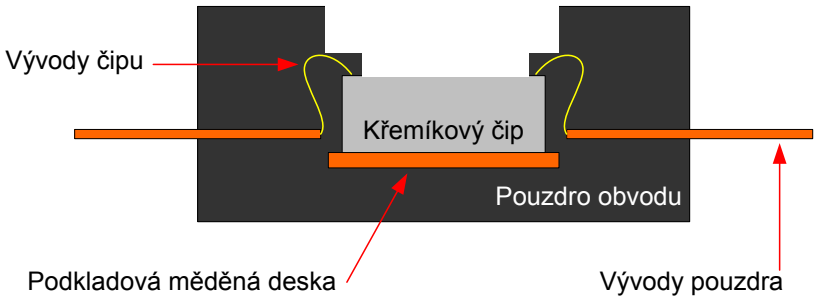
Metoda odkrytování horní stranou pouzdra

Prvním krokem této metody je odstranění části plastového pouzdra z horní strany. Krok číslo 1 je znázorněn na obrázku 3.2.



Obr. 3.2: Krok č. 1 - odkrytování horní stranou pouzdra.

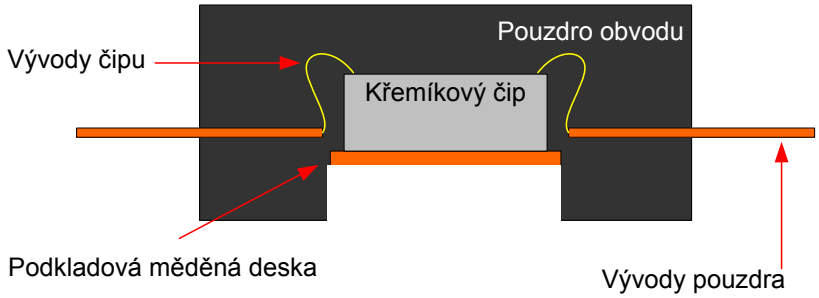
Jelikož jsou z horní strany čipu vyvedeny vodiče pro propojení čipu s vývody pouzdra, je nutné odstranit pouze menší část a zbytek odstranit až v dalším kroku [5]. Dalším krokem je odstranění části pouzdra přímo nad čipem mezi jeho vývody. Tato část je hlavní nevýhodou metody odkrytování horní stranou, riziko poškození vývodů čipu a čipu samotného je zde velmi vysoké. Krok č. 2 je znázorněn na obrázku 3.3.



Obr. 3.3: Krok č. 2 - odkrytování horní stranou pouzdra.

Metoda odkrytování spodní stranou pouzdra

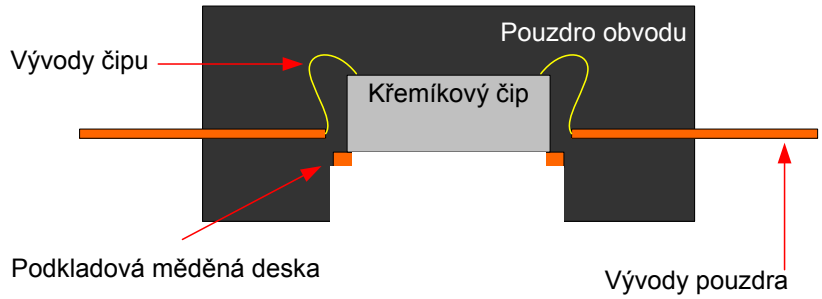
Prvním krokem této metody je odstranění části plastového pouzdra ze spodní strany. Jelikož ze spodní strany je umístěna podkladová měděná deska, na níž je umístěn čip, odstraňuje se plastové pouzdro pouze po tuto desku. V dalším kroku je pak nutné změnit technologii postupu, případně, pokud to daná technologie umožňuje, pouze změnit nástroj. Krok č. 1 je znázorněn na obrázku 3.4.



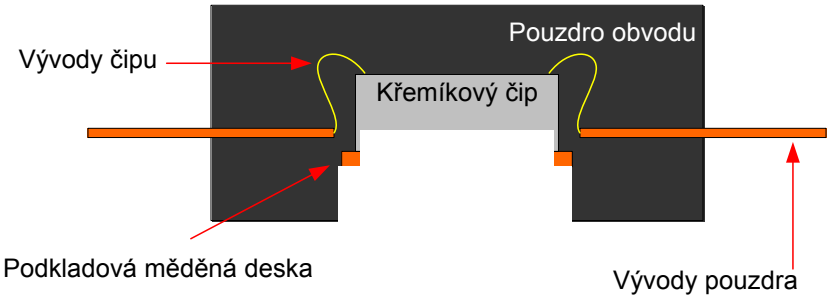
Obr. 3.4: Krok č. 1 - odkrytování spodní stranou pouzdra.

Po odstranění části pouzdra musí být odstraněna i podkladová měděná deska tak, aby byl odkryt i samotný čip. Tento krok je nevýhodou metody odkrytování spodní stranou, postupy pro odstranění plastového pouzdra a měděné desky jsou různé, v tomto okamžiku odkrytování je tedy třeba v některých případech změnit technologii postupu. Krok č. 2 je znázorněn na obrázku 3.5.

Narozdíl od metody odkrytování horní stranou je u této metody nutné provést třetí krok, kterým je ztenčení čipu. Ze spodní strany čipu se nachází poměrně velká vrstva substrátu, přes kterou nemohou projít emitované fotony. Tuto vrstvu je nutné ztenčit a následně vyleštit tak, aby byl umožněn průchod fotonů. Výsledný stav po tomto kroku znázorňuje obrázek 3.6.



Obr. 3.5: Krok č. 2 - odkrytování spodní stranou pouzdra.



Obr. 3.6: Krok č. 3 - odkrytování spodní stranou pouzdra.

3.2.2 Shrnutí výhod a nevýhod základních metod odkrytování

Z výše uvedeného vyplývá, že z horní strany čipu jsou vyvedeny vodiče pro propojení s vývody pouzdra [5]. Při odkrytování z horní strany je tedy třeba postupovat velmi opatrně, aby nebyly propojovací vodiče poškozeny a aby nebyl poškozen čip samotný. Tento fakt omezuje možnosti odkrytování čipu pouze na plochu mezi propojovacími body, nemůžeme tedy odkrýt celou plochu čipu. Výhodou této metody je využití jednotné technologie pro celý proces odkrytování.

Při analýze ze spodní strany pouzdra je třeba odstranit podkladovou měděnou desku pod čipem, což lze provést např. mikrofrézou. Nevýhodou této metody je nutnost změny technologie při odkrytování. Ze spodní strany nehrozí prakticky žádné nebezpečí poškození čipu. Jediným problémem je tedy odstranění desky. U výkonových čipů může mít odstranění desky vliv na chlazení čipu, je proto žádoucí vytvořit odvod tepla jinou cestou [12].

3.3 Technologie odkrytování

Výše uvedené metody odkrytování čipu integrovaného obvodu jsou obecnými postupy. Samotné technologie odkrytování mohou být různé, nejčastěji využívané technologie je možné rozdělit do čtyř skupin:

- mechanické odkrytování,
- chemické odkrytování,
- laserové odkrytování,
- plazmatické odkrytování.

Pro všechny zmíněné technologie odkrytování jsou komerčně vyráběny celé automatizované stanice, příkladem výrobce je ULTRATEC Mfg., Inc. Tento výrobce vyrábí jak automatizované stanice, tak i podpůrné nástroje k analýze.

3.3.1 Přehled jednotlivých technologií odkrytování

Mechanické odkrytování

Mechanické odkrytování je založeno na běžných metodách mechanické úpravy materiálů. Nástroje využívané při této metodě jsou zejména frézy a brusné nástroje. Tato metoda odkrytování patří mezi méně přesné metody, její přesnost je závislá zejména na použitých nástrojích. Využití této metody je často spojováno s ostatními metodami, metoda mechanického odkrytování tak slouží jako podpůrná metoda například pro metodu chemického odkrytování [6].

Chemické odkrytování

Pro chemické odkrytování se využívá kyselin a jejich směsí. Nejčastěji se pro chemické odkrytování využívá kyseliny sírové, kyseliny dusičné a směsí obou kyselin. Důvodem využití zmíněných kyselin jsou jejich typické vlastnosti využitelné při odkrytování. Kyselina sírová [8] je velmi silnou žíravinou, nereaguje však s ušlechtilými kovy (zlato, může být použito k pájení vývodu čipu k měděnému vývodu pouzdra) a její 20% vodný roztok nereaguje s mědí (nepoškodí vodiče čipu ani měděné vývody). Kyselina dusičná [9] nereaguje s křemíkem, při jejím použití dojde k rozleptání pouzdra obvodu, křemíkový čip však zůstane nepoškozen. Chemické odkrytování je v porovnání s ostatními uvedenými metodami nejméně přesné, nevhodným nastavením času působení kyselin nebo použitím nevhodné směsi může být vzorek poškozen.

Vylepšením této metody je již zmíněné spojení s metodou mechanického odkrytování, kdy je pro dosažení vyšší přesnosti mechanicky vytvořeno okénko v pouzdře, do kterého je pak přivedena směs kyselin. Tímto krokem je působení kyselin usměrněno pouze do vymezeného prostoru, což zvyšuje celkovou přesnost metody [7].

Laserové odkrytování

Přesným nastavením laserového paprsku může být zcela přesně odstraněn veškerý krycí materiál pouzdra, ovšem s rizikem poškození propojovacích vodičů čipu a čipu samotného. Tato metoda je srovnatelná s metodou mechanického odkrytování, dosahuje však mnohem vyšší přesnosti a rychlosti [10].

Plazmatické odkrytování

Plazmatické odkrytování využívá směs plynů uvedených do stavu plazmatu. Poměrem plynů vznikne plazma určitých vlastností, kterým je pak odstraňován materiál pouzdra. Vše se děje za přesné regulace teploty vzorku. Tato metoda je nejpomalejší ze všech uvedených metod, odkrytování vzorku trvá až 48 hodin. Tímto způsobem je možno odkrytovat čip do stavu, v jakém byl před zalitím do plastu, bez jeho poškození a bez poškození propojovacích vodičů. Tato metoda poskytuje jedny z nejlepších výsledků [11].

3.3.2 SAP

SAP je zkratkou anglický slov selected area polishing, jedná se o metodu leštění vybrané oblasti používanou při ztenčování křemíkového čipu pro potřeby analýzy.

Metoda SAP sdružuje několik postupů uvedených dříve v textu. K odkrytování je využito metody odkrytování spodní stranou technologií mechanického odkrytování. Dále je pomocí mikrofrézy odstraněna podkladová měděná deska a pomocí speciálních nástrojů je povrch čipu ztenčen a vyleštěn. Metoda SAP zahrnuje všechny kroky postupu pro úplné vytvoření vzorku vhodného pro analýzu. Komerčně je SAP používáno ve formě ASAP automatu vyvinutého firmou ULTRATEC Mfg., Inc. Více informací o SAP bude uvedeno v následujícím textu, který se týká přímo ASAP [12].

3.3.3 ASAP

Pro popis systému ASAP je využito sekce FAQ, často kladených otázek, které poskytuje přímo výrobce ve formě uceleného dokumentu [12]. Výběrem informací z tohoto dokumentu jsou níže popsány všechny důležité informace o ASAP.

Co je ASAP?

Automatic selected area polisher – automatický leštič vybrané oblasti – je nový komerčně dostupný systém vyvinutý společností ULTRATEC Mfg., Inc. pro provádění SAP pohodlným, snadno použitelným a cenově efektivním způsobem přinášejícím do aplikace SAP novou úroveň přesnosti a reprodukovatelnosti.

Jaké vlastnosti umožňují ASAP provedení úspěšné přípravy vzorku?

ASAP využívá vysoce přesného sklíčidla, které upíná množství různě velkých nástrojů, jejichž rychlost je možno přesně nastavovat. Nastavování je spojeno s pohybem na správném místě čipu nebo polovodičového plátku připravovaného vzorku.

Sklíčidlo se pohybuje po ose Z, je vedeno v lineárních ložiscích s přesně kontrolovanou silou přítlaku. Vzorek je upnut v pohyblivém držáku, který je umístěn pod sklíčidlem a pohybuje se v osách X a Y. Pohyblivý držák je nezávislý na systému sklíčidla a umožňuje tak uživateli kontrolou pohybu v osách X a Y vytvořit ve vzorku požadované okénko.

Jak jsou pomocí ASAP připravovány vzorky?

Klíčem úspěchu SAP je kontrola všech parametrů, které mohou ovlivnit broušení nebo leštění vzorku. Ty jsou rozděleny do následujících kategorií.

Výběr místa

ASAP zahrnuje prostředky pro nastavení středu, kolem něhož se pohybuje nástroj v ose X a Y, což znamená, že jedno nastavení na počátku je pak dostačující pro celou operaci. Reprodukovatelnost je lepší při použití standardních rozměrů nástrojů.

Kontrola tlaku

Zajištění plné kontroly zátěže systému znamená, že musí být možné zvolit správný tlak na nástroj, rozměr nástroje a typ brusiva.

Typ nástroje

Typ nástroje je zásadní pro vytvoření správného povrchu. Diamantové nástroje poskytují vynikající možnosti pro odstraňování obalových a podkladových materiálů. Mezi jednotlivými kroky použití diamantových nástrojů je třeba odstranit měděnou vrstvu. Diamantový nástroj je k tomu nevhodný, je tedy nutné zvolit metodu frézování, kterou je možno na přístroji použít, ovšem je nutné přepnutí do frézovacího režimu. Leštění se začíná použitím diamantového brusiva ve formě pasty. Mazání a chlazení probíhá působením přiváděné kapaliny. Nástroj XYLEM^{TM} zajišťuje dobrý povrch nástroje pro použití s brusnou pastou. Finální leštění se provádí pomocí koloidního křemíku a nástroje XYBOVE^{TM}.

Upnutí vzorku

Pro upnutí vzorku se využívá destičkových svorek, které s použitím distančních prvků mohou být použity k uchycení pouzder téměř každé velikosti, tvaru a orientace bez poškození elektrických kontaktů. Jelikož ASAP generuje pouze velmi

malé smykové napětí, často k upnutí postačí i obyčejná oboustranná lepicí páska. Pro větší série stejných pouzder je možno využít upravený testovací slot, případně modifikovat celou upínací desku ASAP přístroje.

Jaké informace je třeba znát předem, aby byl vzorek přesný?

Několikanásobným řezem lze určit pozici čipu v pouzdře. Pomocí řezů je možno také určit rozměry jednotlivých vrstev.

Z které strany je umístěn čip?

Tato informace se může zdát samozřejmou, ovšem v laboratoři, kde se pracuje s velkým množstvím různých vzorků z různých zdrojů, není tato informace často zcela jasná. Ke zjištění správné strany a umístění je vhodné mít několik vzorků pro provedení řezu.

Velikost čipu a jeho umístění?

Tuto informaci je možno získat z technických výkresů pouzdra. Případně je možno umístění zjistit pomocí rentgenového snímku nebo pomocí několika řezů na vyhrazeném vzorku.

Tloušťka měděné desky pod čipem?

Tloušťka měděné desky pod čipem může být velkým problémem v přípravě vzorku, nejlepší je znát tloušťku desky předem. Odstranění její části je pak mnohem snazší.

Náklon čipu?

Je běžné, že čip uvnitř pouzdra není umístěn zcela rovně, může být mírně nakloněn. Náklon je uváděn jako úhel odklonu čipu od roviny horní strany pouzdra. Náklon se pohybuje od několika mikronů až do 50 mikronů, tato hodnota je dána povolenou odchylkou při výrobě.

Malý náklon (o 5 až 10 mikrometrů) může být zobrazovacím NIR (infračerveným) systémem tolerován. Zvětšení mikroskopu je relativně malé, hloubka ostrosti je tedy velká. Nicméně větší odchylky mohou být během SAP přizpůsobeny. Před odstraněním pouzdra není zřejmé, jak velká je odchylka, ovšem po odstranění pouzdra, měděné desky pod čipem a stříbrem plněné epoxidové vrstvy je již možné zjistit přesnou hodnotu odchylky a jednoduše provést korekci úhlu náklonu. ASAP k tomuto účelu využívá tabulky korekcí, pomocí nichž lze kdykoliv během procesu provádět potřebné korekce.

Jaký je postup přípravy vzorku pomocí ASAP?

Přestože existuje velké množství odlišných pouzder, byly experimentálně určeny základní postupy přípravy pro dosažení požadovaných výsledků. Klíčovými kroky jsou postupy uvedené v tabulce níže, která uvádí detaily standardního postupu přípravy vzorku.

Tab. 3.1: Postup přípravy vzorku pomocí ASAP

Krok	**Operace**	**Typ nástroje**	**Mazivo**
1	Odstranění pouzdra	Hrubý diamant	Voda
2	Odstranění Cu desky	Frézovací nástroj	Olej
3	Ztenčení substrátu	Středně hrubý diamant	Voda
4	Prvotní leštění	XYLEM^{TM}	Olej, diamantová pasta
5	Pokročilé leštění	XYLEM^{TM}	Olej, diamantová pasta
6	Finální leštění	XYBOVE^{TM}	Koloidní křemík

Jak je postup přípravy vzorku a infračervená průhlednost kontrolována během SAP?

Během přípravy vzorku je důležité znát míru ztenčení, tedy kolik křemíku ze substrátu je již odstraněno a kolik je třeba ještě odstranit. Dále je vhodné mít zaznamenány údaje z postupu tak, aby bylo možné celý proces shodně opakovat. Tyto informace jsou stěžejní pro reprodukovatelnost SAP.

Důležité vzorky je nejlepší kontrolovat během celého procesu. To se provádí vždy přesunutím vzorku včetně držáku na PEM pracoviště. Jelikož je PEM velmi nákladné, je typicky z celého postupu přípravy vzorku vyjmuto. Ovšem z hlediska kvality přípravy vzorků je výhodné PEM zahrnout přímo do postupu SAP. Pro tyto účely ULTRATEC vyvinul systém INFRATEC. INFRATEC je zobrazovací systém, který je schopen vytvořit potřebné snímky přímo během SAP nebo při řezech pomocí ULTRASLICE. INFRATEC je umístěn přímo v ASAP přístroji pro své maximální využití a jednoduché použití.

Jsou nějaké další možnosti využití ASAP?

Existuje několik dalších laboratorních aplikací, kterým může být ASAP přínosem. Jedná se zejména o aplikace vyžadující použití přesného frézování.

SAP u hybridních nebo více-čipových modulů?

Mnoho společností vyrábí desky obsahující více čipů, které nemohou být ztenčeny jako celek. SAP poskytuje možnosti výběru jednotlivých čipů a ztenčení pouze vybrané oblasti nebo vybraného čipu.

SAP u složených polovodičů (GaAs atd.)?

Křemík dominuje na současném polovodičovém trhu jako podkladní materiál – substrát pro výrobu čipů. Výroba složených polovodičových prvků vyžaduje použití arsenidu galia jako substrátu. ASAP umožňuje kvalitní zpracování i těchto druhů materiálů.

Ostatní metody analýzy

Ostatní metody analýzy využívající odkrytování zadní strany čipu, jako jsou např. laserová mikrosondáž nebo změna tepelně indukovaného napětí, jsou o mnoho efektivnější při použití vzorku připraveného pomocí ASAP.

3.4 Detekce fotonu

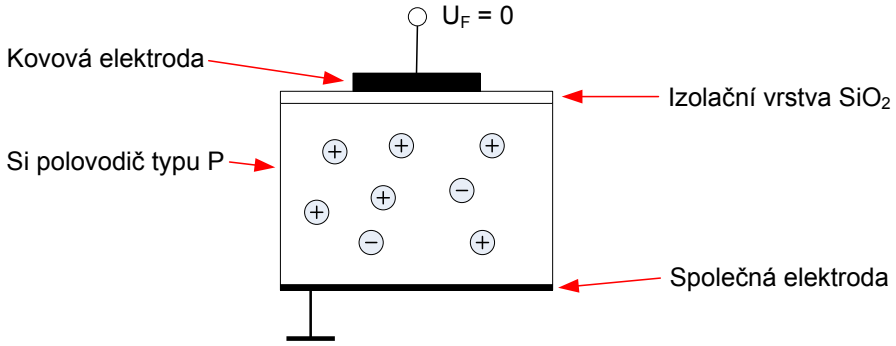
3.4.1 Základní metody detekce fotonu

Nejjednodušší metodou detekce fotonů je využití fotocitlivé desky nebo fotocitlivého filmu. V obou případech je na podkladní vrstvu nanesena fotocitlivá emulze, která je tvořena halogenidy stříbra vázanými ve velmi čistém a jemném klihu s rozdílnou velikostí krystalů. Právě velikostí krystalů je pak určeno celkové rozlišení desky nebo filmu. Dopadem světla nebo jiného elektromagnetického záření dochází ke změnám v halogenidech stříbra a vytváří se tak neviditelný obraz. Chemickým procesem je možné vytvořit z obrazu neviditelného obraz viditelný [14], [15].

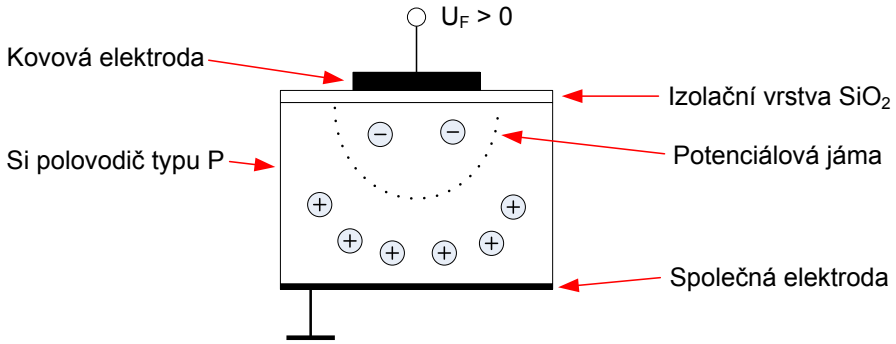
Další možnou metodou je využití CCD snímače, zařízení pracující s vázanými náboji. CCD snímací prvek využívá vlastnosti polovodiče, kdy vlivem dopadu světla (fotonů) dochází k vytvoření náboje. Na obrázku 3.7 je znázorněna základní buňka CCD snímače ve výchozím stavu, tedy bez napětí mezi elektrodami a bez osvětlení. V tomto stavu se v polovodiči nacházejí majoritní nosiče, díry, a minoritní nosiče, elektrony. Elektrony jsou v polovodiči obsaženy vlivem nečistot [16].

Při přivedení napětí na elektrodu dojde k vytvoření potenciálové jámy. Majoritní nosiče jsou od elektrody odpuzovány, minoritní jsou přitahovány pod elektrodu. Tento stav znázorňuje obrázek 3.8.

Při osvětlení buňky dochází vlivem předávání energie fotonů polovodiči ke generaci párů elektron-díra, vzniklé elektrony jsou přitahovány pod elektrodu, díry jsou

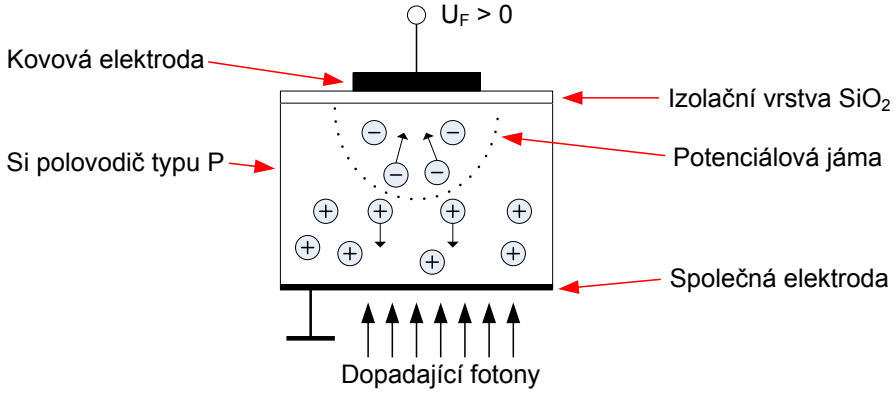


Obr. 3.7: Buňka CCD snímače ve výchozím stavu.



Obr. 3.8: Buňka CCD snímače s přivedeným napětím.

odpuzovány. Takto vzniká náboj, jehož velikost je úměrná velikosti a délce osvětlení. Tento stav zachycuje obrázek 3.9.

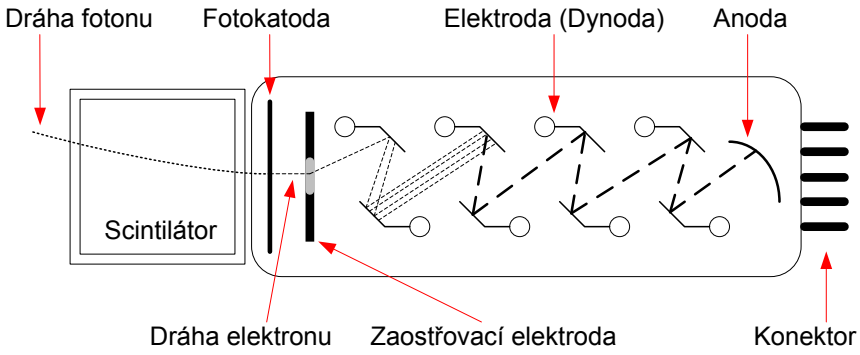


Obr. 3.9: Osvětlená buňka CCD snímače s přivedeným napětím.

Samotná buňka CCD snímače uvedená na obrázcích výše není schopna plnit požadovanou funkci detekce fotonů. Buňka musí být doplněna o transportní vedení,

které náboj odvádí k dalšímu zpracování, a tento celek musí být vhodně uspořádán např. do matice nebo do řádku tak, aby bylo možné určit polohu dopadajících fotonů. Podrobný popis a vysvětlení funkce celého CCD snímače uvádí pramen [16].

Pro aplikace vyžadující detekci jednotek fotonů nebo obecně velmi slabého světla byly vyvinuty fotonásobiče. Uspořádání fotonásobiče je uvedeno na obrázku 3.10.



Obr. 3.10: Uspořádání fotonásobiče.

Obalem fotonásobiče je skleněná baňka. Ve snímací části se nachází scintilátor, pomocí kterého je možné fotonásobičem detekovat i ionizující záření. Foton po průchodu scintilátorem naráží na fotokatodu, ze které se v důsledku fotoelektrického jevu (předáním energie) uvolní elektrony. Uvolněné elektrony jsou po průchodu zaostřovací elektrodou urychlovány napětím mezi elektrodami (dynodami), při každém dopadu elektronů na dynodu dochází k tzv. sekundární emisi, kdy je uvolněno větší množství elektronů, než dopadlo. Takto se postupně počet elektronů násobí. Po několikanásobném zesílení průchodem přes soustavu dynod dopadá proud elektronů na anodu. Celkové zesílení může dosáhnout hodnoty až 10^8, což umožní i detekci jednotlivých fotonů [17].

3.4.2 Výběr vhodné metody detekce fotonu

Předchozí kapitola zmiňuje 3 metody detekce fotonu. První metoda využívající fotocitlivé vrstvy na desce nebo filmu je uzpůsobena pro vytváření fotografických snímků, pro její použití je ovšem potřeba, aby na povrch světlocitlivé vrstvy dopadalo relativně velké množství fotonů (světla). Při detekci velmi malého množství fotonů nemusí být změna fotocitlivé vrstvy vůbec patrná, případně může dojít ke zkreslení vlivem zrnitosti podkladu. Velkým záporem této metody je také nevhodnost pro další elektronické zpracování. Z uvedených důvodů se tedy jedná o metodu nevhodnou k aplikaci optického postranního kanálu.

Metoda využívající CCD snímací prvek umožňuje elektronické zpracování získaných dat, to je velmi výhodné při dalším zpracování jako je např. porovnávání nebo rozpoznávání dat. Nevýhodou u CCD snímače je velikost šumu. Nečistoty v polovodiči způsobují výskyt nadbytečných elektronů, tyto pak vnáší chybu do výstupu. Zásadním problémem je také tepelná generace párů elektron-díra, páry pak nejsou generovány pouze v důsledku dopadu fotonů na buňku, ale také teplotními změnami v buňce. Při využití CCD snímače pro detekci jednotek fotonů může šum velmi zkreslit výsledné hodnoty, z tohoto důvodu není ani tato metoda vhodná k aplikaci optického postranního kanálu.

Poslední metoda detekce využívající fotonásobič netrpí žádným z výše uvedených nedostatků. Umožňuje elektronické zpracování změřených dat a hodnota šumu je velmi malá. Fotonásobiče jsou přímo určeny k zachytávání velmi malého množství fotonů, zesílení, které poskytují, je možné měnit změnou napětí mezi anodou a katodou a změnou napětí mezi jednotlivými dynodami. Změnami napětí je možné upravit také časové rozlišení snímání.

3.5 Současný stav problematiky

Jednou z aktuálně využívaných technik pro aplikaci optického postranního kanálu je pikosekundová zobrazovací obvodová analýza PICA. Pomocí tohoto druhu analýzy je možné s využitím patřičného zařízení detekovat a zobrazit emitované fotony. Přístroje pro aplikaci pikosekundové zobrazovací obvodové analýzy jsou schopny kromě samotné detekce emitovaných fotonů zaznamenávat také čas emise a polohu fotonu. Při provedení synchronizace PICA s algoritmem v analyzovaném obvodu je možné pomocí PICA zachytit tranzistory v paměti analyzovaného obvodu a tak úspěšně získat tajná data.

Několik experimentů využívajících právě PICA již bylo provedeno. Využití optického postranního kanálu bylo zdokumentováno panem Martinem Hlaváčem, doktorandem na katedře algebry MFF UK. Při své stáži ve Francii provedl v laboratoři CNES experimentální měření, které zdokumentoval článkem [4]. V tomto článku popisuje průběh experimentu, včetně využitých přístrojů.

Přístrojem pro provádění pikosekundové zobrazovací obvodové analýzy v laboratoři CNES byl přístroj s názvem Optica. Optica využívá jako detektor Mepsicron 2, který pracuje na principu fotonásobiče. Mepsicron 2 umožňuje zobrazovat fotony s prostorovým rozlišením 50μm a časovým rozlišením jednotlivých fotonů 100ps. Velkým kladem tohoto detektoru je vysoký odstup signálu a šumu, jak bylo zmíněno v kapitole 3.4.2.

Výše uvedená analýza byla provedena pomocí metody odkrytování spodní stra-

nou popsanou v kapitole 3.2.1, včetně potřebné ztenčení spodní vrstvy substrátu. Technologií odkrytování byla metoda mechanického odkrytování, která je blíže popsána v kapitole 3.3.1. Odkrytování společně se zbroušením a vyleštěním čipu bylo provedeno na automatu využívajícím ASAP, kterým se zabývají kapitoly 3.3.2 a 3.3.3.

Pro analýzu pomocí optického postranního kanálu byl zvolen mikrokontrolér PIC16F84A, tento obvod neobsahuje žádná opatření proti útokům postranními kanály a jeho využití je stále aktuální např. v kartách GoldCard, které jsou používány například k emulaci ISO7816 kompatibilních karet pro satelitní/kabelové televizní přijímače nebo předplacených telefonních karet, které se používaly v druhé polovině devadesátých let.

Analýzou obvodu PIC16F84A bylo zjištěno, že jsou detekovatelné přechody paměťových buněk jak z log. 1 na log. 0, tak opačně. Každou změnu v paměťové buňce lze tedy zachytit. Při aplikaci PICA na PIC16F84A pracující s částí AES algoritmu, kdy rundovní klíč xoruje s daty, byl zjištěn přímo šifrovací klíč. Analýzou PICA byl klíč doslova „vyblikán“, zobrazením paměťových buněk Opticou byly zachyceny informace v buňkách, které pak bylo možné jednoduše přečíst [4].

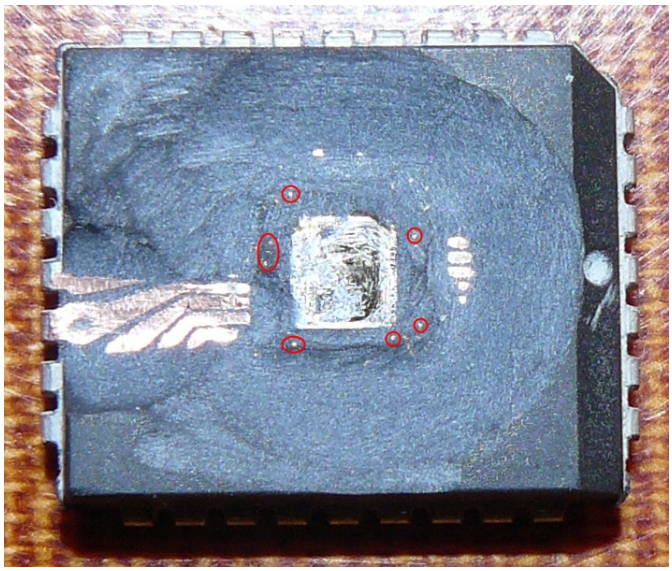
3.6 Experimentální ověření teoretických poznatků

Pro ověření teoretických informací o uspořádání uvnitř pouzdra integrovaného obvodu bylo provedeno několik experimentů, pomocí kterých bylo možné ověřit výhody a nevýhody základních metod odkrytování. Dále byla prakticky ověřena metoda mechanického odkrytování a její využití jako podpůrného nástroje k metodě chemického odkrytování. Pro experimenty byly využity různé integrované obvody, postup výroby je ve všech důležitých bodech shodný u všech typů pouzdra.

3.6.1 Odkrytování pouzdra

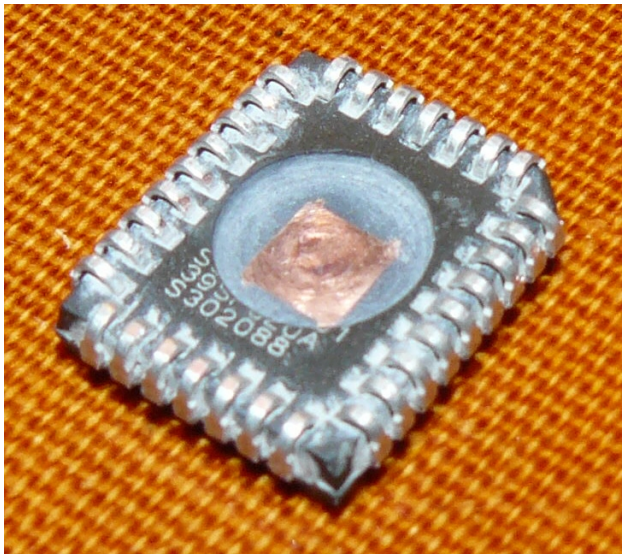
Na obrázku 3.11 je odkrytá horní strana pouzdra integrovaného obvodu. Červeně jsou označeny nejvíce patrné přerušené vodiče čipu. Zde je jasně patrné, že metoda odkrytování horní stranou je nevhodná pro technologii mechanického odkrytování. Vodiče čipu nejsou umístěny přesně, nýbrž volně, je tedy velmi obtížné předejít jejich poškození.

Na obrázku 3.12 je odkrytá spodní strana pouzdra, v kruhovém otvoru je zcela odkrytá podkladová měděná deska. Metoda odkrytování spodní stranou je vhodná i pro méně přesné mechanické odkrytování. Měděná deska zabrání poškození čipu i při hrubším odstraňování plastového pouzdra. Samotné odstranění desky je možné provést buď odfrézováním nebo zbroušením a následným stržením. Vrstva epoxidu pod deskou zabrání poškození čipu v případě frézování, v případě stržení zbroušené



Obr. 3.11: Odkrytá horní strana pouzdra.

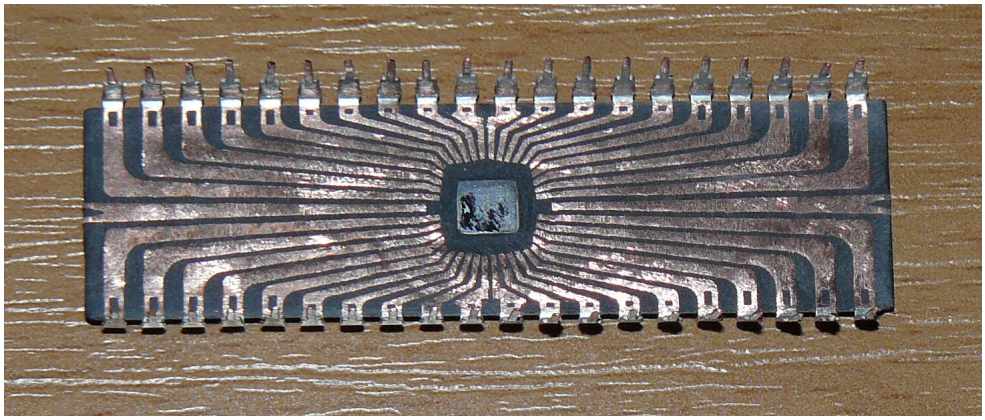
desky zůstává vrstva epoxidu nepoškozená a její odstranění je pak možné provést společně se ztenčováním čipu.



Obr. 3.12: Odkrytá spodní strana pouzdra.

Obrázek 3.13 zachycuje mikrokontrolér PIC odkrytovaný spodní stranou technologií mechanického odkrytování. Ze spodní strany mikrokontroléru byl zcela odstraněn plastový materiál pouzdra. Podkladová měděná deska byla nejdříve ztenčena a následně stržena. Na tomto vzorku byly testovány různé nástroje k mechanickému odstranění epoxidové vrstvy. Čip na fotografii má již částečně ztenčenu odkrytou

stranu. Dále je na fotografii zachycena celá struktura spojů mezi čipem a vývody pouzdra.



Obr. 3.13: Odkrytovaný mikrokontrolér PIC.

Odkrytováním mikrokontroléru PIC16F84A byly určeny údaje, které výrobce běžně v katalogovém listu výrobku neuvádí. Zjištěné údaje uvádí tabulka 3.2 Rozměry změřené po odkrytování jsou uvedeny tak, jak byly odměřeny a platí pouze pro jeden konkrétní vzorek. Odchylka nebyla stanovena, jelikož nebylo odkrytováno dostatečné množství obvodů pro její stanovení.

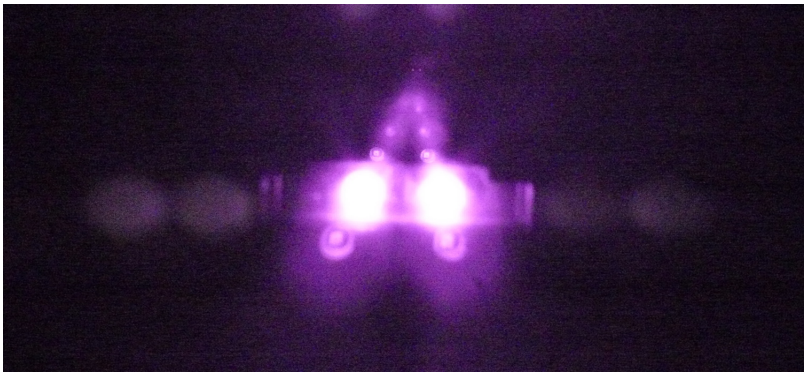
Tab. 3.2: Rozměry PIC16F84A důležité pro analýzu

Délka pouzdra	$22,61 \div 22,99$mm	Uvádí výrobce
Šířka pouzdra	$6,10 \div 6,6$mm	Uvádí výrobce
Výška pouzdra	$2,92 \div 3,68$mm	Uvádí výrobce
Tloušťka měděné desky	260µm	Zjištěno po odkrytování
Tloušťka čipu	300µm	Zjištěno po odkrytování

3.6.2 Zobrazení struktury čipu

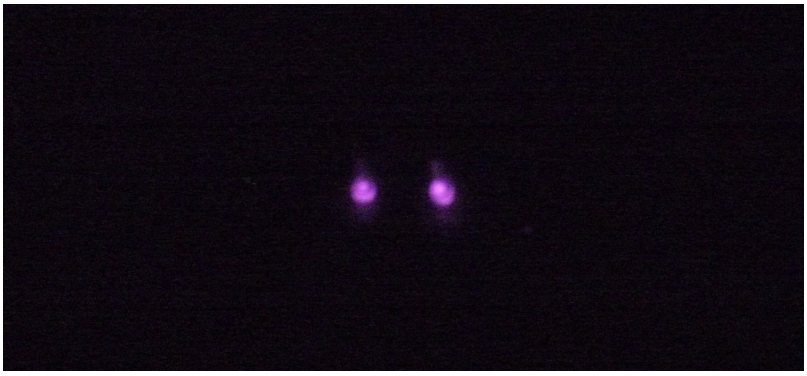
Na fotografiích uvedených výše se čip jeví jako zcela neprůhledný. Není tomu tak ve všech případech, křemík je pod infračerveným světlem průhledný. Průhlednost závisí úměrně na jeho tloušťce. Pro získání informací optickým postranním kanálem je třeba zajistit velmi dobrou průhlednost, aby emitované fotony pronikly skrze vrstvu substrátu a mohly být následně zachyceny. Pro ověření průhlednosti pod infračerveným světlem byl realizován primitivní experiment využívající křemíkovou desku tloušťky shodné s tloušťkou čipu, tedy 300µm. Povrch použité desky byl dokonale

vyleštěn, jednalo se o polotovar k výrobě křemíkových čipů. Jako snímač posloužil digitální fotoaparát s nastavenou citlivostí ISO 1250 a dobou expozice 13s, tyto hodnoty byly určeny experimentálně pro dosažení dobrých výsledků zobrazení. Jako zdroj infračerveného záření byl použit upravený dálkový ovladač se dvěma infračervenými diodami. Obrázek 3.14 zachycuje infračervený zdroj bez zakrytí deskou.



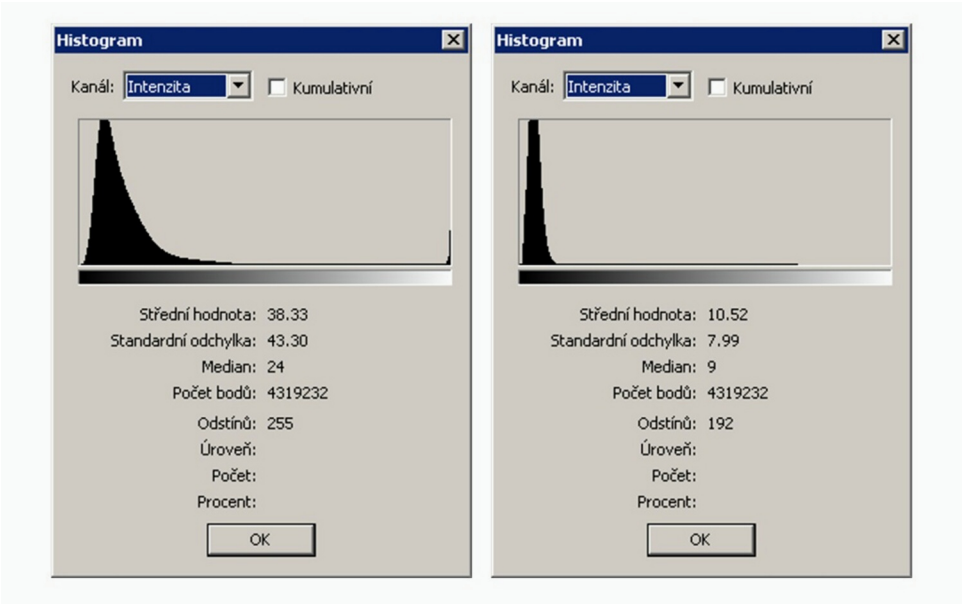
Obr. 3.14: Infračervený zdroj bez zakrytí.

Po zakrytí zdroje křemíkovou deskou intenzita zdroje silně poklesla. Obrázek 3.15 zachycuje infračervený zdroj po zakrytí deskou. Pro přibližné určení poklesu intenzity byly využity histogramy obou snímků. Porovnáním hodnot byl určen přibližný útlum intenzity a tím i potřebné ztenčení čipu. Oba histogramy jsou zachyceny na obrázku 3.16.



Obr. 3.15: Infračervený zdroj zakrytý křemíkovou deskou.

Porovnáním středních hodnot intenzity lze zhruba určit útlum intenzity způsobený zakrytím infračerveného zdroje křemíkovou deskou. Intenzita zakrytím klesla zhruba o 72%. Při předpokladu úměrnosti tloušťky a útlumu intenzity by bylo nutné ztenčit čip na tloušťku zhruba 84µm. Tato hodnota je velmi blízká hodnotě využité



Obr. 3.16: Histogramy snímků infračerveného zdroje, vlevo bez krytí, vpravo s krytím deskou.

při experimentu v [4], kde tloušťka ztenčeného čipu pro efektivní využití optického postranního kanálu činila zhruba 70µm.

4 ROZPOZNÁVÁNÍ DAT Z POSTRANNÍCH KANÁLŮ

4.1 Výběr metody rozpoznávání

K rozpoznávání dat existuje velké množství metod a prostředků založených ve většině případů na aplikaci matematického aparátu. V tomto konkrétním případě, kdy jde o rozpoznání dat z postranních kanálů, vystupuje požadavek univerzálnosti celého klasifikátoru. Cílem této části práce bude nalezení vhodné metody a vytvoření programu, pomocí kterého bude možné rozpoznávat data z více postranních kanálů jednoduchou modifikací vstupní části programu. Hlavní požadavky na program jsou následující:

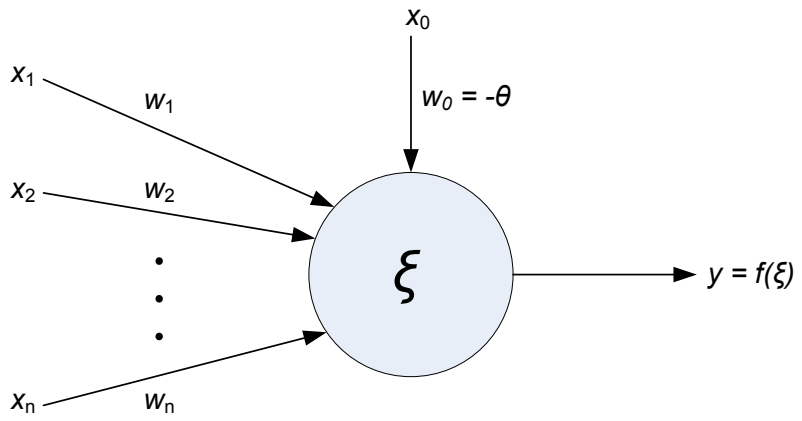
- možnost modifikace vstupu pro jiná data,
- rozpoznávání dle vzoru,
- přesnost výsledku,
- jednoduchá aplikace.

Vzhledem k požadavkům kladeným na program pro rozpoznávání dat byla jako základ programu zvolena umělá neuronová síť. Program s tímto základem umožňuje modifikovat vstup pro velké množství dat, poskytuje možnost rozpoznávání na základě předloženého vzoru a výstupem jsou vysoce přesné výsledky. Jednoduchost využití umělé neuronové sítě bude patrná v následujícím textu.

4.2 Charakteristika umělých neuronových sítí

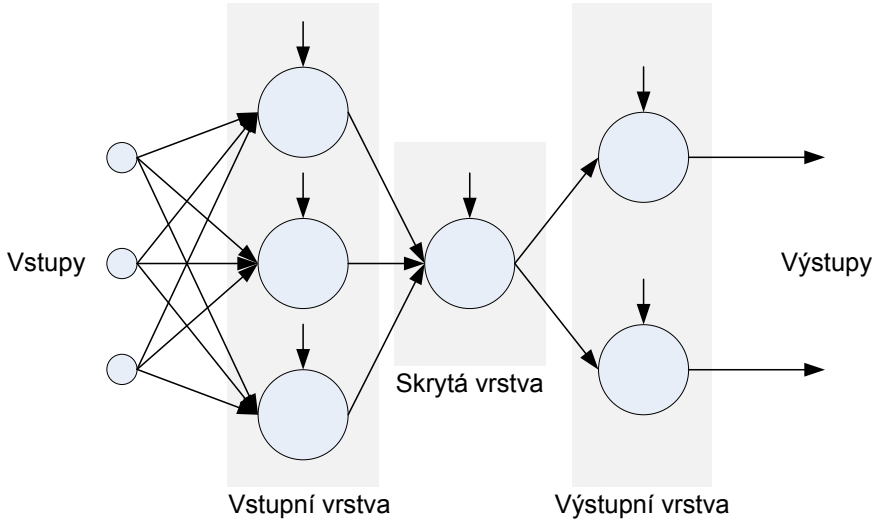
Umělá neuronová síť vychází z poznatků o biologické neuronové síti. Skládá se z propojených neuronů stejně jako biologická síť a i v postupu řešení problému je možné pozorovat stejné postupy jako u biologické neuronové sítě. Velmi jednoduše a zkráceně lze říci, že obě sítě mají shodný postup při řešení problému. Obecně je prvním krokem učení (obecně probíhá s učitelem nebo bez učitele) a teprve poté je možné přistoupit k řešení zadaného problému.

Základním prvkem umělé neuronové sítě je tzv. formální neuron, někdy též označovaný jako perceptron, znázorněný na obrázku 4.1. Každý formální neuron má x vstupů o váze w. Vstup x_0 s váhou $w_0 = -\theta$ znázorňuje prahovou hodnotu neuronu. Uvnitř neuronu probíhají dva výpočty. Prvním je výpočet post-synaptického potenciálu, který je definován jako vnitřní funkce neuronu $\xi = \sum_{i=1}^{n} x_i w_i - \theta$ a má nejčastěji sigmoidní průběh. Z výsledné funkce ξ je pak vypočtena výstupní hodnota neuronu $y = f(\xi)$. Z uvedených informací vyplývá, že každý neuron je možné popsat matematickým vztahem [18], [19].



Obr. 4.1: Formální neuron.

Samotný formální neuron není možné použít k řešení složitějších problémů. Z tohoto důvodu jsou neurony spojovány do celých sítí. Topologií sítě a počtem neuronů je pak síť předurčena k řešení určitého okruhu problémů, neboť na topologii a počtu neuronů je závislá vhodnost použití ke konkrétnímu účelu. Každá topologie poskytuje přesné výsledky pouze pro několik konkrétních okruhů problémů. Ukázku jednoduché topologie uvádí obrázek 4.2. První vrstva sítě je nazývána vstupní vrstvou, poslední vrstva sítě je nazývána výstupní vrstvou a všechny ostatní vrstvy jsou vrstvy skryté. Běžně jsou umělé neuronové sítě označovány ve formátu 3-1-2, což znamená, že takto označená síť má 3 neurony ve vstupní vrstvě, 1 neuron ve skryté vrstvě a 2 neurony ve výstupní vrstvě [19].



Obr. 4.2: Neuronová síť.

Činnost umělé neuronové sítě probíhá ve dvou fázích. Aby byly výsledky problémů řešených pomocí sítě správné, probíhá v první fázi učení sítě. Učení není nic jiného než porovnání výstupní hodnoty sítě se správným výsledkem a následná úprava funkce neuronu tak, aby byl výsledek co nejpřesnější. Na vstupy sítě jsou přivedeny určité hodnoty, na výstupu je pak očekáván konkrétní výsledek. Pokud se výsledek zpracování liší od správného výsledku, pak jsou upraveny váhy jednotlivých vstupů, případně počet neuronů nebo topologie sítě (topologii volí tvůrce sítě, váhy vstupů jsou upravovány automaticky během procesu učení). Proces učení se opakuje tak dlouho, dokud síť neposkytuje správné a přesné výsledky. Druhou fází je využití sítě k řešení problému.

Princip učení uvedený výše, kdy dochází k porovnávání výstupních hodnot se správnými hodnotami je nazýván jako proces učení s učitelem. Neuronové síti je předložen vzor, podle kterého je síť během učení modifikována. Vzor správných hodnot je nazýván trénovací množinou, v některých pramenech je pak proces učení nazýván též procesem trénování sítě [18].

4.3 Klasifikace dat pomocí neuronové sítě

Pro klasifikaci dat s využitím umělé neuronové sítě bylo zvoleno prostředí softwarového balíku MATLAB. Pro práci s umělou neuronovou sítí v prostředí MATLAB byl zvolen volně šiřitelný softwarový balík Free NN NETLAB Toolbox.

Jelikož reálná data z optického postranního kanálu nebyla během práce získána z důvodu nedostupnosti potřebného zařízení, budou pro rozpoznávání využita jiná data. Aby byly náležitě představeny všechny vlastnosti systémů postavených na umělých neuronových sítích, budou využita data z reálného měření při aplikaci výkonového postranního kanálu. Data výkonového postranního kanálu mají podobu proudového průběhu. Průběh je zapsán jako dvourozměrné pole hodnoty a času o 175 hodnotách. Pro experimentální účely budou využity 3 různé průběhy změřené při provádění funkcí XOR, AND a NOP na experimentálním přípravku s osazeným mikrokontrolérem PIC16F84A.

Požadovaným výstupem programu je přiřazení průběhu ke konkrétní funkci. Nejprve bude zvolen počet neuronů v síti a následně její topologie. Vzhledem k počtu vstupních hodnot bude ve vstupní vrstvě sítě 175 neuronů. Výstupní vrstva bude obsahovat 525 neuronů. Tento počet není standardní, běžně by k rozpoznávání 3 typů funkcí postačovaly 4 výstupní neurony (čtvrtý neuron by označoval neznámou funkci). Při tomto měření byly některé hodnoty zatíženy značně velkou chybou, která by se mohla projevit při rozpoznávání dat, z tohoto důvodu je pohled na síť a na data odlišný. Data jsou v tomto případě skupinou samostatných hodnot a celek

tvoří jako ucelená skupina. Pro experimentální účely bude síť naučena pouze na 3 různé funkce, tedy 3 krát 175 hodnot, z toho vyplývá výstupní počet neuronů 525. Počet neuronů ve skryté vrstvě bude určen experimentálně na základě výsledných hodnot a činnosti sítě.

4.4 Vlastní vytvoření klasifikátoru

Prvním krokem ve vytváření klasifikátoru je implementace v prostředí MATLAB. Výpis zdrojového kódu níže uvádí vytvoření nové funkce `klasifikace()` a inicializaci této funkce. V bloku inicializace je nejprve smazán obsah příkazového okna, přidána cesta k Free NN NETLAB Toolboxu, vypsána aktuální činnost skriptu do příkazového okna a vytvořeno pole `time`, které představuje časovou osu.

```
function klasifikace();
% Inicializace skriptu
%*************************************************************************
clc;
addpath('NETLAB')
disp('Inicializace skriptu');
time = [0:1:174];
%*************************************************************************
```

V bloku vzorových dat jsou připraveny hodnoty 3 konkrétních průběhů, které byly určeny jako vzory jednotlivých funkcí.

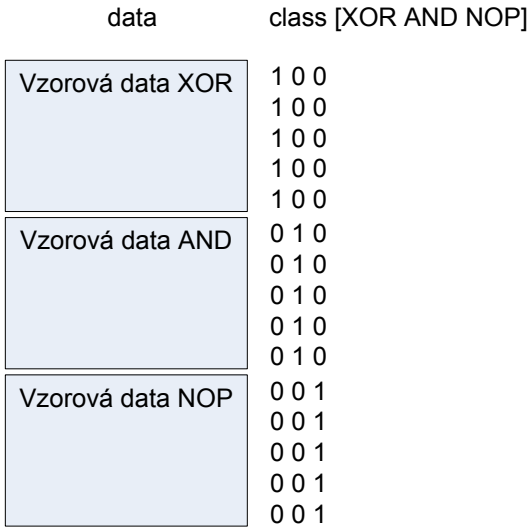
```
% Vzorová data
%*************************************************************************
xorvzor = [-0.0024 0 0.0032 0.0048 0.0072 0.012 0.016 0.0152 ...];
andvzor = [-0.004 -0.0016 0.0032 0.0072 0.0104 0.0136 0.016 ...];
nopvzor = [-0.0008 0.0032 0.008 0.0112 0.0128 0.0152 0.0168 ...];
%*************************************************************************
```

V další části jsou připraveny vzorky k rozpoznání. K základním funkcím vždy po dvou vzorcích, jeden vzorek průběhu jiné funkce.

```
% Vzorky k rozpoznání a klasifikaci
%*************************************************************************
% Vzorky funkce XOR
xor1 = [0.0008 0.0048 0.0088 0.0088 0.0088 0.0128 0.0168 0.012 ...];
xor2 = [-0.0024 0.0008 0.0032 0.0048 0.0072 0.012 0.0152 0.0144 ...];
```

```
% Vzorky funkce AND
and1 = [-0.0008 0.0008 0.0048 0.0088 0.012 0.0144 0.0144 0.0144 ...];
and2 = [-0.004 -0.0016 0.0032 0.0072 0.0104 0.0136 0.016 0.0168 ...];
% Vzorky funkce NOP
nop1 = [-0.0016 0.0032 0.008 0.0112 0.012 0.0144 0.0168 0.0144 ...];
nop2 = [-0.0008 0.004 0.0088 0.0112 0.012 0.0144 0.016 0.0144 ...];
% Jiný vzorek
swap1 = [0.008 0.0056 0.004 0.004 0.004 0.0032 0.0016 0.0024 ...];
%*****************************************************************
```

Před vytvořením sítě je nutné vytvořit tzv. trénovací data. Trénovací data obsahují vzory dat k rozpoznání a správný výsledek, tedy u každé hodnoty je vyznačeno, ke které konkrétní funkci patří. Množina vzorů je uložena jako pole `data`, množina správných výsledků jako pole `class`. Uspořádání obou množin hodnot ukazuje obrázek 4.3.



Obr. 4.3: Trénovací množina.

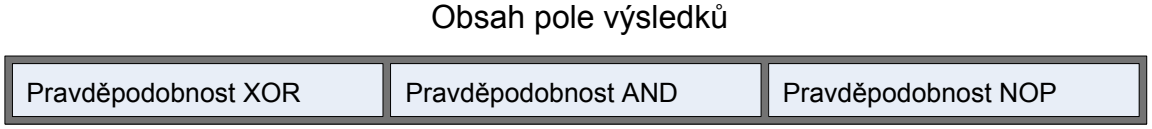
Samotné vytvoření neuronové sítě je v prostředí MATLAB velmi jednoduché. Z předchozího textu je již známa požadovaná konfigurace neuronové sítě, tedy např. 175-10-525. Zápisem `nn = mlp(175, 10, 525, 'logistic');` je zajištěno vytvoření sítě požadovaných parametrů. Zápis `'logistic'` určuje požadovaná tvar aktivační funkce neuronů, v tomto případě bude tvar funkce obvyklá logistická sigmoida.

Následující blok zdrojového kódu určuje konfiguraci sítě. K nastavení požadovaných parametrů slouží ve Free NN NETLAB Toolboxu konfigurační pole `options` o 18 hodnotách. Většina z těchto hodnot je podstatná pro jiné složitější sítě. Nejdříve

je tedy pole `options` naplněno nulovými hodnotami. Následně je možné přistoupit k nastavení konkrétních parametrů, které se provádí zápisem hodnoty 1 na konkrétní pozici v konfiguračním poli `options`. První hodnota pole určuje, zda se bude vypisovat chyba sítě během učení, v tomto případě není výpis požadován, položka je tedy zakomentována a neuplatní se. Čtrnáctou hodnotou pole je určen počet trénovacích cyklů, tato hodnota je velmi důležitá, její vliv na funkci sítě bude probrán dále v textu. Posledním řádkem je spuštěno trénování sítě zadané konfigurace pomocí trénovacích dat. Parametr `'scg'` aktivuje zaznamenávání chyb během učení a zároveň označuje metodu učení (v tomto případě se jedná o výchozí nastavení, kde je učení prováděno metodou sdružených gradientů, pro složitější sítě je možné využít i jiné metody) [19].

```
options = zeros(1,18);
%options(1) = 1; % Výpis chyby během učení
options(14) = 180; % Počet trénovacích cyklů
[nn, options] = netopt(nn, options, data, class, 'scg');
```

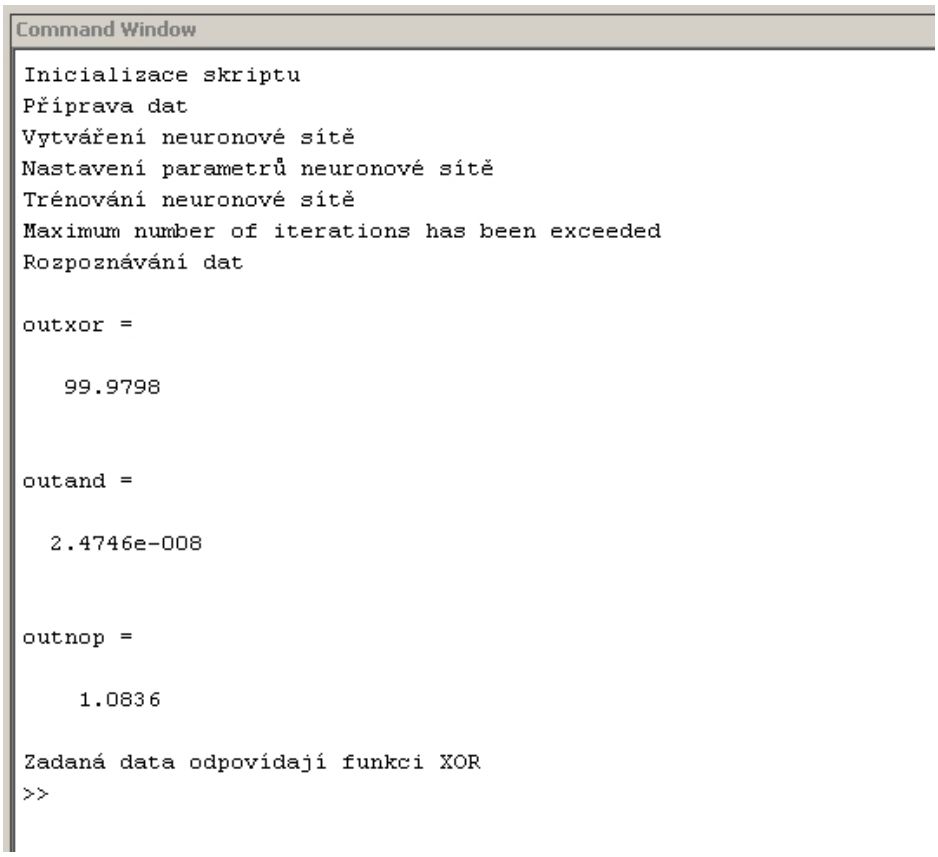
Po ukončení trénování je síť připravena k rozpoznávání dat. Zápisem `res = mlpfwd(nn,xor1)` je neuronové síti předložen vzorek hodnot. Výsledek rozpoznávání (klasifikace) je uložen do pole `res`. Pole obsahuje celkem 525 hodnot a je složeno ze 3 částí o 175 hodnotách. Každá část obsahuje výpis pravděpodobností příslušnosti jednotlivých hodnot ke konkrétní funkci. Uspořádání výsledků je znázorněno na obrázku 4.4.



Obr. 4.4: Uspořádání výsledků rozpoznávání.

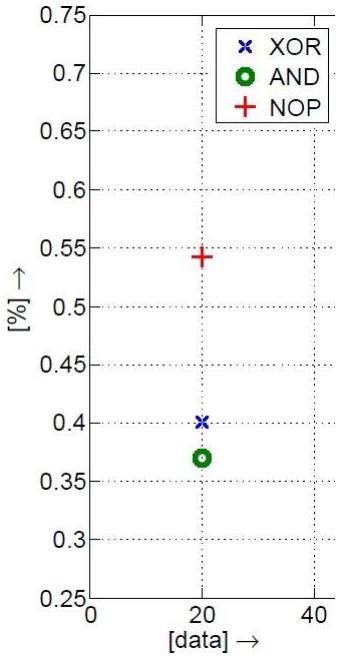
Zpracování výsledků probíhá vytvořením 3 samostatných polí z celkového pole `res` tak, aby bylo možno graficky znázornit výsledek klasifikace a vypočítat procentní výsledek klasifikace. Celý průběh vykonávání skriptu zachycuje obrázek 4.5.

Výpočet procentního výsledku klasifikace je realizován jako prostý aritmetický průměr všech hodnot pravděpodobností z příslušného pole vzniklého rozdělením pole `res`. Jak je patrné z výsledku rozpoznávání vzorku funkce XOR, který dosáhl hodnoty 99,9798%, mají chyby měření pouze velmi malý vliv na rozpoznávání. Výsledek rozpoznávání dat je doprovázen grafickým znázorněním výsledku klasifikace.

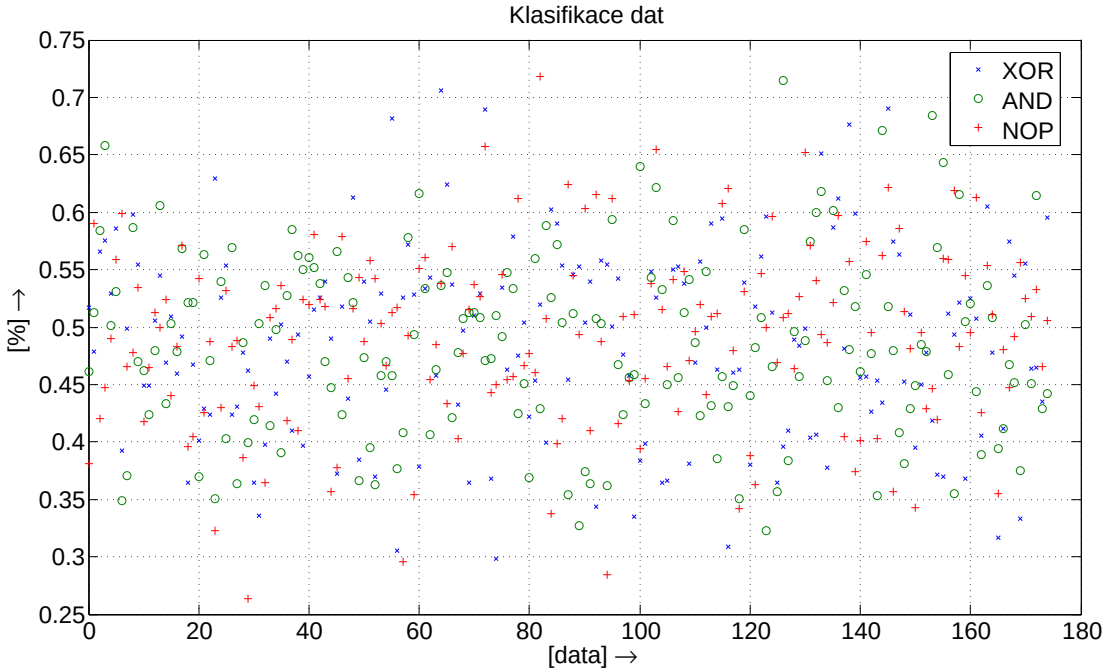


Obr. 4.5: Průběh vykonávání skriptu

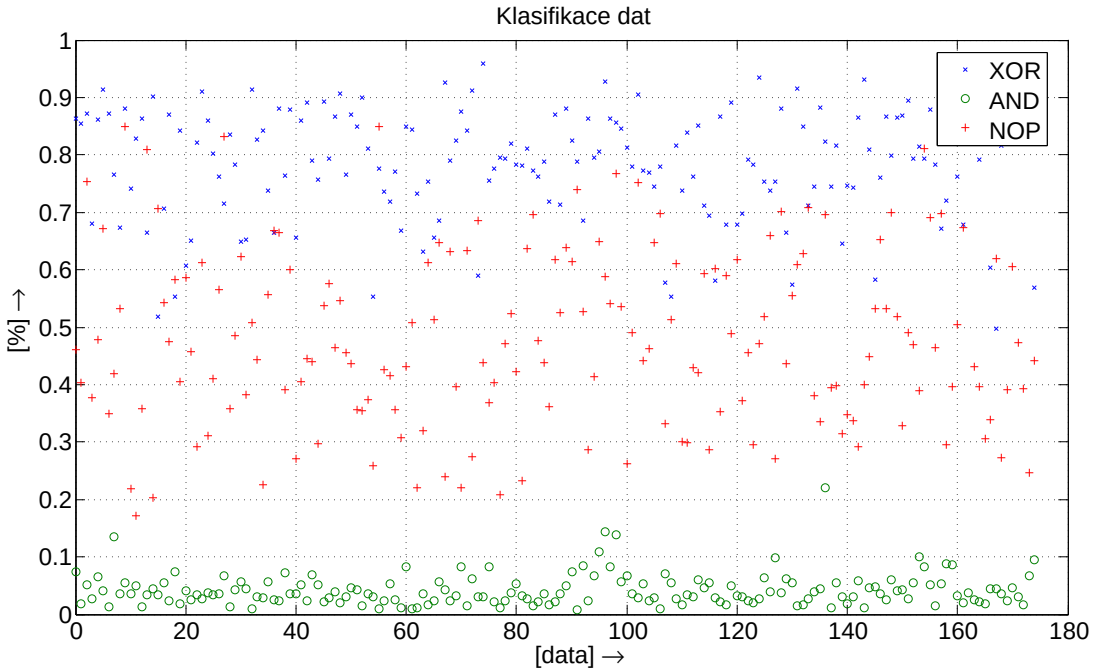
Na obrázku 4.6 je zachycena část grafu, na které jsou zvýrazněny pravděpodobnosti dvacáté hodnoty rozpoznávaného vzorku. Pro dvacátou hodnotu rozpoznávaného průběhu tedy dle grafu platí, že dvacátá hodnota náleží k funkci NOP s pravděpodobností 54%, k funkci XOR s pravděpodobností 40% a k funkci AND s pravděpodobností 37%. Po jednom trénovacím cyklu je výsledkem rovnoměrné rozložení pravděpodobností pro všechny průběhy, tento stav zachycuje obrázek 4.7. Pro další vybrané počty trénovacích cyklů jsou výsledky zachyceny na obrázcích 4.8, 4.9.



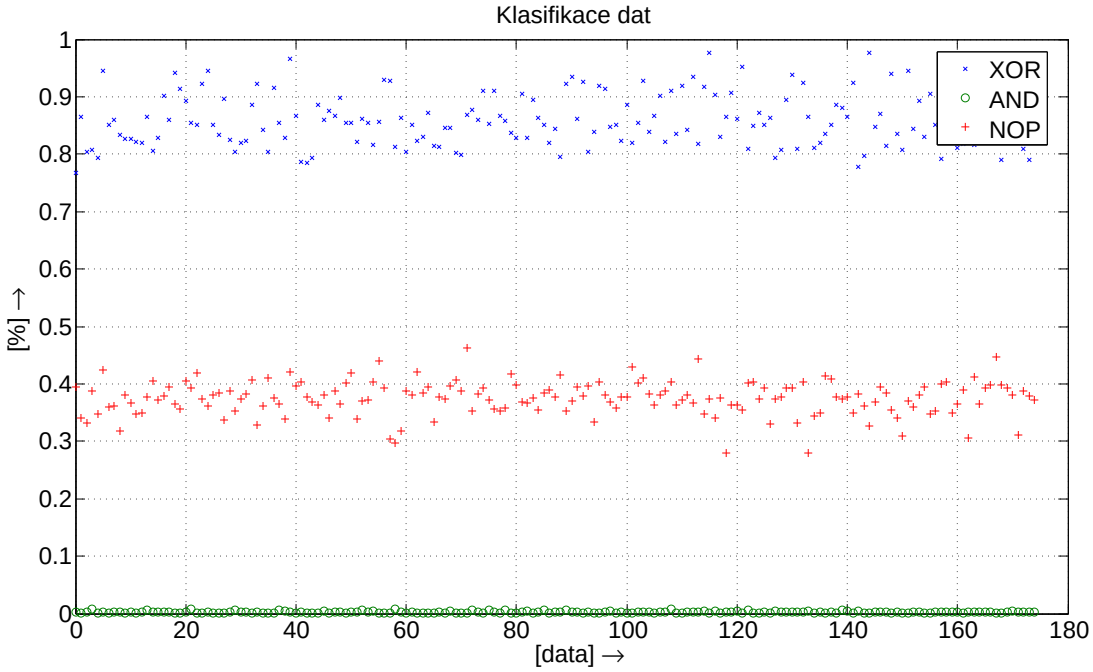
Obr. 4.6: Interpretace výsledků z grafického zobrazení výsledků.



Obr. 4.7: Výsledek rozpoznávání dat po 1 trénovacím cyklu.



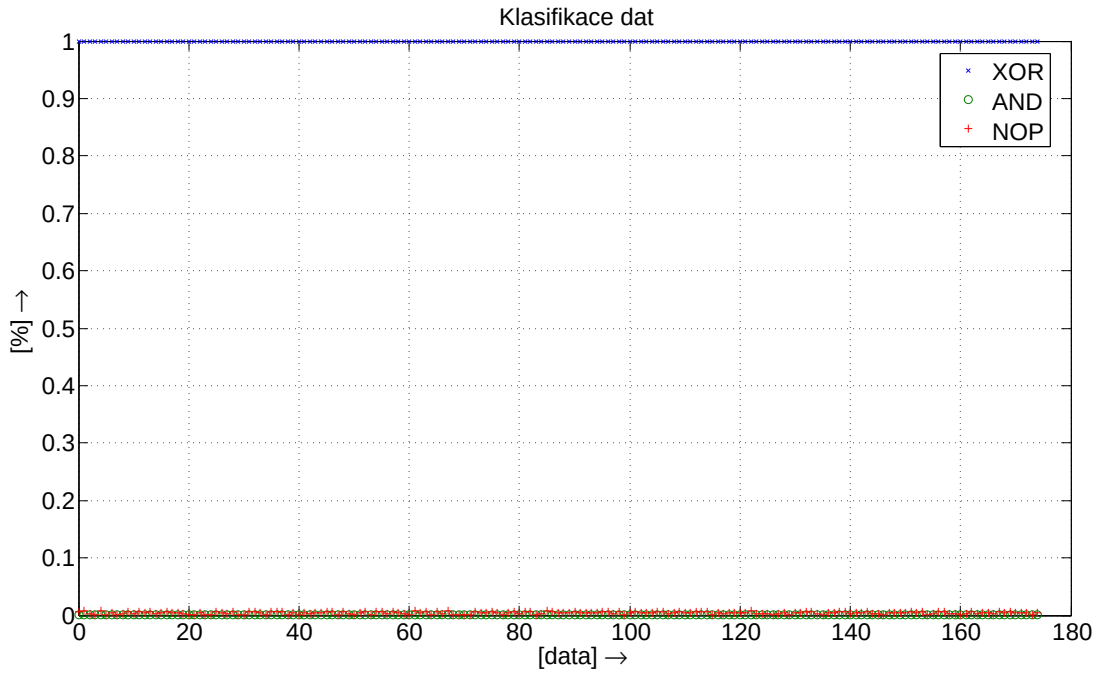
Obr. 4.8: Výsledek rozpoznávání dat po 20 trénovacích cyklech.



Obr. 4.9: Výsledek rozpoznávání dat po 50 trénovacích cyklech.

Na obrázku 4.10 je klasifikace zcela dokončena. V grafu je jednoznačně určeno, ke které funkci náleží zadané hodnoty. Výsledek rozpoznávání dosahuje přesnosti více než 90%, ve většině případů se však hodnota pohybuje kolem 99%. Přesnost a tedy i schopnost rozpoznání je velmi dobrá. Výhodou tohoto řešení je také skutečnost, že rozpoznání a přiřazení proběhne vždy a to i v případě, že na zadaný průběh síť nebyla trénována nebo je průběh zatížen extrémní chybou. V takovém případě dojde k přiřazení k „nejpodobnější“ funkci. Pro ověření byl v testech využit čtvrtý průběh, který patří k funkci SWAP, na který síť nebyla trénována. Výsledkem je přiřazení k funkci AND, která je svým průběhem k funkci SWAP nejbližší. Při rozpoznávání v běžném provozu bude síť natrénována na všechny funkce, které umožňuje konkrétní mikrokontrolér, není tedy žádoucí, aby program obsahoval navíc i možnost určení neznámého průběhu.

Z výše uvedených výsledků vyplývá, že rozpoznávání a klasifikace na bázi neuronové sítě dosahuje vynikajících výsledků. Z pohledu zadání práce a následně stanovených požadavků splňuje všechny vytyčené cíle a v uplatnění pro aplikaci postranních kanálů je toto řešení vhodné.



Obr. 4.10: Výsledek rozpoznávání dat po 150 trénovacích cyklech.

5 ZÁVĚR

Cílem první části práce bylo nastudování teoretických informací o postranních kanálech, zejména optického postranního kanálu. Úvod do kryptografie a základní pojmy z této oblasti obsahuje kapitola 1. Přehled základních metod útoků pomocí postranních kanálů obsahuje kapitola 2.

Informace o optickém postranním kanálu obsahuje kapitola 3. Celá kapitola 3 postupně popisuje celý proces přípravy vzorku až po samotnou analýzu prováděnou na komerčních automatech. Závěr kapitoly zachycuje současný stav problematiky a několik vlastních experimentálních ověření teoretických informací.

Experimentální část kapitoly 3 se zabývá ověřením vnitřního uspořádání mikrokontroléru a zjištěním informací, které výrobce běžně neuvádí v katalogovém listu. Zjištěné informace jsou shrnuty v tabulce 3.2. Dále byla experimentálně ověřena propustnost IR světla křemíkového čipu v infračerveném světelném pásmu. Kapitola 3.2.1 uvádí postup odkrytování čipu spodní stranou pouzdra, při které je nutné ztenčit čip právě z důvodu propustnosti IR světla a tedy i samotné možnosti emise fotonu mimo čip. Experimentem v kapitole 3.6.2 bylo pomocí histogramů zjištěno, že pro zachování dostatečné propustnosti IR světla je nutné ztenčit substrát ze spodní strany čipu zhruba o 72%, což odpovídá výsledné tloušťce čipu zhruba 84µm. Tato hodnota koresponduje s hodnotou využitou při laborním experimentu uvedeném v pramenu [4].

Jelikož dostupnost potřebných zařízení neumožnila realizaci celé analýzy pomocí optického postranního kanálu v laboratorních podmínkách FEKT VUT v Brně, je poslední kapitola práce zaměřena na samotné rozpoznávání dat z analýzy optickým postranním kanálem. Z teoretického základu uvedeného v práci byl znám formát dat analyzátoru využívaného v jiných laboratořích, samotná data ovšem nebyla k dispozici. Z uvedených důvodů a také kvůli požadavku vysoké flexibility softwarového řešení, jak uvádí zadání práce, byla převzata data z měření výkonového postranního kanálu. Na reálných datech mnohem lépe vynikly všechny přednosti a nedostatky navrženého softwarového řešení.

Pro realizaci softwaru pro rozpoznávání dat bylo zvoleno prostředí MATLAB a celý systém rozpoznávání byl postaven na základu, který tvořila neuronová síť. Díky této kombinaci vzniklo univerzální řešení umožňující rozpoznávání dat z více druhů postranních kanálů, v některých případech je pouze nutné upravit vstupní část programu. Teoretický základ k využití neuronových sítí obsahuje kapitola 4.2. Celý postup vytvoření klasifikátoru popisuje kapitola 4.3, kde je také rozebrán zdrojový kód programu a podrobnosti k sestavení samotné neuronové sítě.

Výstupní hodnoty funkčního skriptu pro klasifikaci dat dosahují vynikajících výsledků. Při klasifikaci s využitím reálných vzorků zatížených v některých případech

velmi vysokou chybou (dáno problematikou a metodami pro analýzu pomocí výkonového postranního kanálu) dosahovaly výsledky klasifikace úspěšnosti více než 90%, ve většině případů dokonce více než 99%. Z těchto výsledků je patrné, že využití neuronových sítí v této oblasti kryptografie je velmi výhodné zejména z důvodu vysoké přesnosti a jednoduché implementace pro konkrétní případ.

Úplný zdrojový kód výše popisovaného softwarového řešení je umístěn na přiloženém DVD, které obsahuje i kompletní toolbox, pomocí kterého byl program vytvořen.

LITERATURA

[1] PINKAVA, J. *Úvod do kryptologie* [online]. 1998 [cit. 18. 11. 2009], dostupné z URL: <http://crypto-world.info/pinkava/uvod/uvod98.pdf>.

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

[3] KOCHER, P., JAFFE, J., JUN, B. *Introduction to Differential Power Analysis and Related Attacks*. San Francisco, 1998.

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

[5] ULTRATEC Mfg., Inc. *ULTRASLICE Datasheet* [online]. 2009 [cit. 18. 11. 2009], dostupné z URL: <http://ultratecusa.com/PDFlibrary/ULTRASLICE%20Datasheet.pdf>.

[6] ULTRATEC Mfg., Inc. *ASAP-1-brochure* [online]. 2009 [cit. 18. 11. 2009], dostupné z URL: <http://ultratecusa.com/PDFlibrary/ASAP-1%20Brochure%20low%20res%20-S-10-07.pdf>.

[7] ULTRATEC Mfg., Inc. *Rapidetch-brochure* [online]. 2009 [cit. 18. 11. 2009], dostupné z URL: <http://ultratecusa.com/PDFlibrary/Rapidetch-brochure-w.pdf>.

[8] Norfalco. *H_2SO_4 TechBrochure* [online]. 2009 [cit. 18. 11. 2009], dostupné z URL: <http://www.norfalco.com/documents/NorFalco_H2SO4TechBrochure.pdf>.

[9] Platinum Metals Rev. *The Manufacture of Nitric Acid* [online]. 1967 [cit. 18. 11. 2009], dostupné z URL: <http://www.platinummetalsreview.com/pdf/pmr-v11-i1-002-009.pdf>.

[10] ULTRATEC Mfg., Inc. *SESAME-1000 Data Sheet* [online]. 2009 [cit. 18. 11. 2009], dostupné z URL: <http://ultratecusa.com/PDFlibrary/SESAME-1000.pdf>.

[11] ULTRATEC Mfg., Inc. *FA-2000 Data Sheet* [online]. 2009 [cit. 18. 11. 2009], dostupné z URL: <http://ultratecusa.com/PDFlibrary/FA-2000Dsheet.pdf>.

[12] ULTRATEC Mfg., Inc. *TEC Note #1 Selected area polishing (SAP) of semiconductor devices – F.A.Q*, [online]. 2009 [cit. 3. 11. 2009] dostupné z URL: <http://www.ultratecusa.com/PDFlibrary/Selected%20Area%20Polishing%20-%20FAQ.pdf>.

[13] Microchip Technology Inc. *PIC16F84A Data Sheet* [online]. 2009 [cit. 21. 10. 2009], dostupné z URL: <http://ww1.microchip.com/downloads/en/devicedoc/35007b.pdf>.

[14] Fujifilm. *Sensia 400 Data Sheet* [online]. 2010 [cit. 29. 1. 2010], dostupné z URL: <http://www.fujifilm.cz/cs/download/sensia400_datasheet.pdf>.

[15] Fujifilm. *Neopan 1600 Professional Data Sheet* [online]. 2010 [cit. 29. 1. 2010], dostupné z URL: <http://www.fujifilm.cz/cs/download/neopan-1600-professional.pdf>.

[16] HANUS, S. *Základy televizní techniky I.* Skriptum, ústav radioelektroniky, Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 82 s.

[17] Hamatsu: *Photomultiplier tubes Basics and Applications* [online]. 2010 [cit. 14. 2. 2010], dostupné z URL: <http://sales.hamamatsu.com/assets/applications/ETD/pmt_handbook_complete.pdf>.

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

[19] Bishop C. M., Nabney I. T. *NETLAB Online Reference Documentation*, [online]. 1997 [cit. 12. 5. 2010], dostupné z URL: <http://www1.aston.ac.uk/EasySiteWeb/GatewayLink.aspx?alId=40589>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

ASAP Automatic selected area polisher

CCD Charge-coupled device

CNES Centre National d'Etudes Spatiales

DIL Double in line

FAQ Frequently ask and questions

IR Infrared

ISO International organization for standardization

MFF UK Matematicko-fyzikální fakulta Univerzity Karlovy

Mfg., Inc. Manufacturing Incorporated

NIR Near infrared range

PEM Program execution monitor

PICA Picosecond imaging circuit analysis

SAP Selected area polishing

SIL Single in line

SEZNAM PŘÍLOH

A OBSAH PŘILOŽENÉHO DVD

- bp.pdf – elektronická verze bakalářské práce
- klasifikator.m – zdrojový kód skriptu pro rozpoznávání dat
- NETLAB – Free NN NETLAB Toolbox