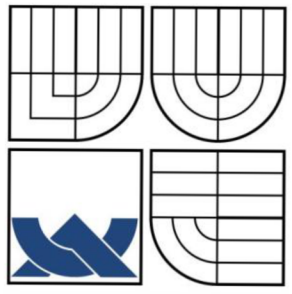
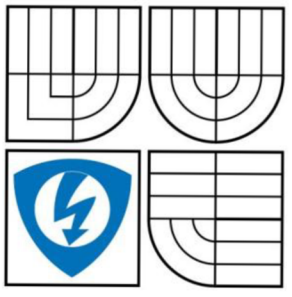


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

POSTRANNÍ KANÁLY U SMART CARD

THE SIDE CHANNELS AT THE SMART CARD

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

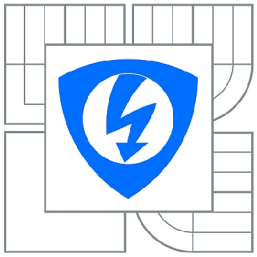
AUTOR PRÁCE
AUTHOR

Bc. KAREL POSPÍŠIL

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. JIŘÍ SOBOTKA

BRNO 2011



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Karel Pospíšil	***ID:***	70213
Ročník:	2	***Akademický rok:***	2010/2011

NÁZEV TÉMATU:

Postranní kanály u Smart Card

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s implementací kryptografických algoritmů prostřednictvím čipových karet. Prostudujte a popište známé metody útoků na čipové karty postranními kanály. Pomocí měření napájecích charakteristik Smart Card během komunikace, odvození změn napájení v závislosti na probíhajících výpočtech, monitorování komunikace karty a terminálu navrhněte způsob odposlechu a analýzy zpracovávaných informací.

DOPORUČENÁ LITERATURA:

[1] RANKL, Wolfgang; EFFING, Wolfgang. Smart Card Handbook. 4th edition. Munich : John Wiley & Sons, Ltd., 2010. 1043 s. ISBN 978-0-470-74367-6
[2] RANKL, W. Overview about attacks on smart cards, 2003. http://www.wrankl.de/SCH/Attacks.pdf.

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

Vedoucí práce: Ing. Jiří Sobotka

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

UPOZORNĚNÍ:

ABSTRAKT

Diplomová práce se zaměřuje na čipové karty a popisuje známé typy útoků, které využívají postranních kanálů. Čipová karta spadá do skupiny nejmladších a nejchytřejších karet. Ve svém těle, které je nejčastěji vyrobeno z PVC, má vložen čip obsahující mikroprocesor. Útoky postranními kanály jsou útoky, které se snaží využít unikající informace z fyzické implementace systému při práci kryptografického algoritmu. Těchto unikajících citlivých informací se snaží využít útočník, protože mohou být za určitých okolností závislé na vstupních datech.
Teoretická část se věnuje popisu čipových karet a jejich typů, následně se zaměřuje na jejich bezpečnost. Popisuje rozdělení útoků na čipové karty a zahrnuje přehled vybraných kryptografických algoritmů, které jsou používány v čipových kartách. Popisuje vybrané fyzické, logické útoky a nejčastější útoky postranními kanály. Dále nastiňuje možnosti měření napěťově proudového postranního kanálu. Praktická část se potom věnuje použitému softwaru a hardwaru. Tato část se věnuje měření napájecích charakteristik čipové karty a analýze zpracovávaných informací, a to za využití osciloskopu a pracovní stanice s měřící kartou AD 622 a vývojového prostředí Simulinku.

KLÍČOVÁ SLOVA

Čipová karta, Matlab, karta AD 622, postranní kanál, Real Time ToolBox, Simulink.

ABSTRACT

The thesis is dealing with smart cards and describes the known types of side channel attacks. Smart card belongs into the group of the youngest and smartest cards. In the card body, made mostly from PVC, there is a chip inserted which contains a microprocessor.Side channel attacks are trying to use the leaking information from the physical implementation of the system while processing the cryptographic algorithm. The attacker is trying to use the leaking sensitive information because under certain circumstances it can be dependent on the input data.
The theoretical part is devoted to description of smart cards, their types and their safety. It describes the classification of attacks on smart cards and includes the overview of selected cryptographic algorithms used in smart cards. It also describes selected physical and logical attacks and the most frequent side channel attacks. The thesis furthermore describes possibilities of measuring the voltage-current side channel. The practical part deals with used software and hardware. This section is devoted to the measurement of power specification of smart cards and to the analysis of processed information, using the oscilloscope and workstation with AD 622 card and Simulink development environment.

KEYWORDS

Smart card, Matlab, card AD 622, side channel, Real Time ToolBox, Simulink.

Citace práce

POSPÍŠIL, K. *Postranní kanály u Smart Card*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2011. 80 s. Vedoucí diplomové práce Ing. Jiří Sobotka.

Prohlášení o původnosti práce

Prohlašuji, že jsem svoji diplomovou práci na téma „Postranní kanály u Smart card“ vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny uvedeny v seznamu literatury na konci práce.

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

V Brně dne …… ……

podpis autora

Poděkování

Děkuji vedoucímu diplomové práce Ing. Jiřímu Sobotkovi za užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce. Dále mé poděkování patří Ing. Pavlu Hanákovi za umožnění měření na osciloskopu MSO9104A a za pomoc při tomto měření.

V Brně dne …… ……

podpis autora

Seznam obrázků

Seznam tabulek

Úvod

Dlouhou řadu let je sváděn boj mezi výrobci, kteří vymýšlí nové zabezpečovací řešení, a útočníky, jež se snaží prolamovat ochrany různých zařízení. Je to nekonečný koloběh neustálých soubojů, ve kterých se obě strany neustále střetávají a získávají nové znalosti a zkušenosti. Jelikož neexistuje absolutní bezpečnost, mohou útočníci tuto bezpečnost narušit, pokud mají dostatek času a finančních prostředků.

Čipové karty spadají do skupiny nejmladších a nejchytřejších identifikačních karet. Jsou velice flexibilní. Ve svém tradičním těle, které je vyrobeno z PVC nebo ABS, mají vložený čip obsahující mikroprocesor, na který se ukládají všechna potřebná data. Čipová karta je jedním z nejbezpečnějších médií, kam lze v současnosti uložit data. Mikroprocesor bývá umístěn pouze v jediném čipu, čím se zajistí vyšší odolnost čipových karet proti možným útokům. Tyto karty jsou využitelné především v oblastech, kde je zapotřebí dosáhnout vyššího stupně zabezpečení. Za poslední desetiletí došlo k velkému nárůstu požadavků na čipové karty. Proto začali výrobci dodávat karty, které poskytovaly více funkcí a ty starší dále vylepšovali a rozšiřovali, aby zůstaly konkurence schopné a odolaly novým formám útoků. Současné čipové karty jsou odolné vůči drahým a sofistikovaným útokům, dokáží jim velmi účinně čelit a v krajním případě dokážou také zničit uložená data.

Čipové karty nás dnes a denně obklopují na každém kroku a mají velmi různé využití. Svojí velkou univerzálností nacházejí uplatnění v mnoha různých oblastech, jako jsou platební a identifikační systémy, dále také zdravotnictví, předplacené karty pro parkování a dopravu, řízení přístupů do budov a systémů, placených televizí či mobilních telefonů nebo telefonních karet. Zde všude jsou převážně využívány čipové karty, které se šíří celým světem s vysokým nasazením.

Útoky postranními kanály se zaměřují na zařízení a sledování mikroprocesoru v činnosti. Jedná se tedy o úplně jiný přístup, který při svém prvotním představení odhalil překvapivé slabiny a možný velký potenciál. Útoky postranními kanály se obvykle snaží využít nedostatku, že je výpočet za určitých okolností na mnoha místech přímo ovlivňován vstupními daty. Ke zneužití dojde, jestliže se informace o citlivých datech dají získat přes výstupní kanály.

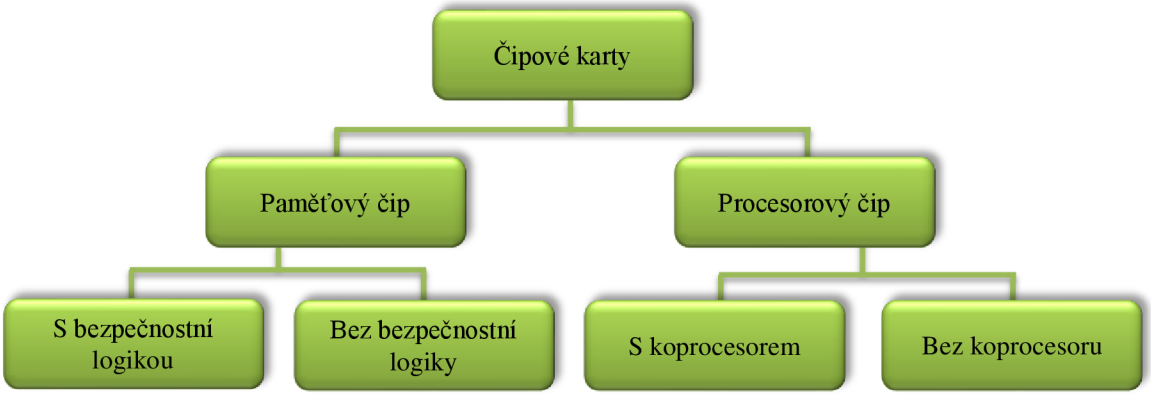
Cílem práce je bližší seznámení s čipovými kartami a jejich bezpečností. Teoretická část se zabývá možnými metodami útoků, které využívají postranních kanálů. Dále popisuje časové, napěťově proudové, elektromagnetické a chybové postranní kanály a také rozebírá již realizované útoky. Popisuje možnosti měření napěťově proudového postranního kanálu pomocí odporového bočníku. Následně se věnuje použitému softwaru a hardwaru. Praktická část měření se věnuje měření napájecích charakteristik čipové karty při její komunikaci. Poslední kapitola představuje praktickou část práce, která se zabývá měřením napájecích charakteristik čipové karty a analýze zpracovávaných informací s využitím pracovní stanice s měřící kartou AD 622 a vývojového prostředí Simulinku.

1 Čipové karty

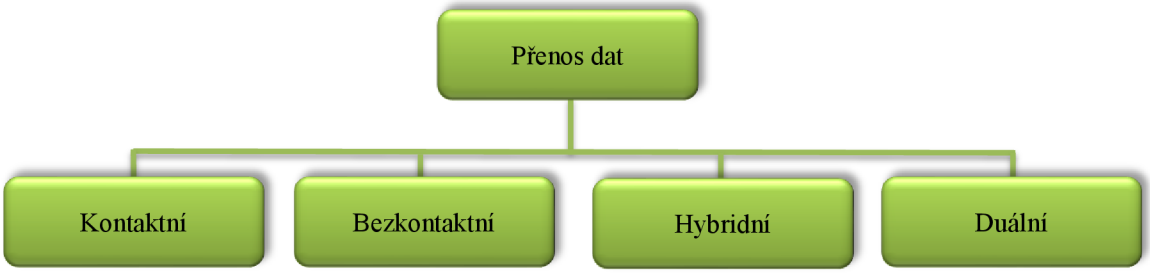
Tyto karty se řadí mezi nejmladší a nejchytřejší z karet formátu ID-1(identifier). Ve svém těle, které je nejčastěji vyrobeno z PVC (polyvinyl chloride), mají vložený čip. Čip obsahuje mikroprocesor, který zajišťuje další z funkce potřebné pro chod karty, jako je ukládání, přenos a zpracování dat. Funkce a vlastnosti čipových karet specifikuje norma ISO 7816 (International Organization for Standardization).

Mezi největší výhody zajisté patří ochrana uložených dat před neoprávněným přístupem a manipulací. Uložená data mohou být chráněna proti neoprávněnému přístupu a manipulaci. K datům se přistupuje přes sériové rozhraní, o které se stará operační systém a bezpečnostní logika. Na kartu mohou být uložena tajná data, která se zpracovávají pouze uvnitř čipu mikroprocesorové jednotky. Při manipulaci s daty, jako je mazání, čtení a zapisování, jsou využívány jak hardwarové, tak softwarové mechanismy. To umožňuje vytvořit nespočetné množství bezpečnostních mechanizmů, které se dají přizpůsobit konkrétním podmínkám užívání. Další výhodu představuje současná paměťová kapacita pohybující se v řádu megabajtů, která s příchodem nových čipových generací narůstá. Větší kapacitu než čipové karty mají pak pouze optické čipové karty. Další nespornou výhodou je dlouhá životnost a spolehlivost oproti kartám s magnetickým proužkem, u kterých se udává životnost kolem dvou až tří let [25].

Čipové karty lze rozdělit do dvou základních skupin a to na karty paměťové a karty s mikroprocesorem, viz obr. 1.1. Jednotlivé typy se od sebe odlišují jak funkčností, tak i cenou. Podle typu komunikačního rozhraní se mohou čipové karty dále rozdělit na čtyři skupiny, viz obr. 1.2. Duální jednočipové karty využívají jak kontaktní, tak i bezkontaktní komunikační rozhraní a využívají výhod obou typů. Hybridní karty obsahují dva vzájemně nepropojené čipy. Většinou je jeden z čipů kontaktní a druhý bezkontaktní, čímž se docílí větší flexibility.



Obr. 1.1: Klasifikace čipových karet podle typu čipu.



Obr. 1.2: Klasifikace čipových karet podle přenosu dat.

1.1 Typy karet

1.1.1 Paměťové karty

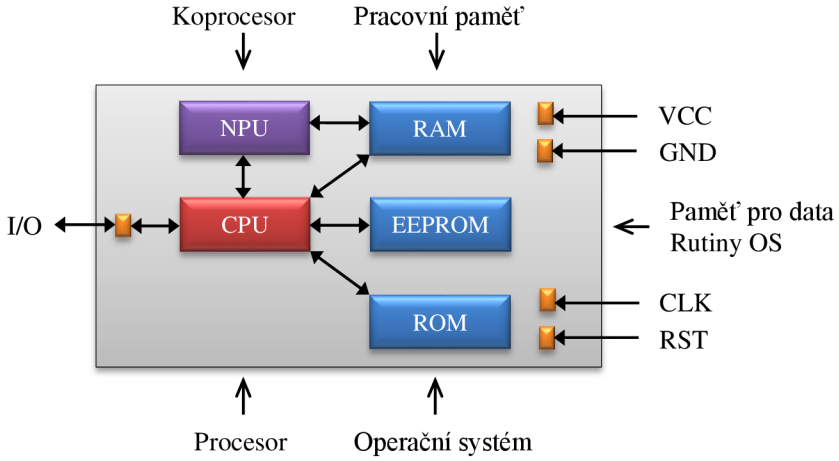
Data potřebná pro aplikace jsou obvykle uloženy v paměti EEPROM (electrically erasable programmable read-only memory), což odpovídá nejběžnějšímu způsobu. Přístup do paměti se řídí bezpečnostní logikou. Využívá se jednoduché šifrování, ochrana proti zápisu, vymazání ochrany paměti nebo jen některé z oblastí paměti. Data se přenáší z karty nebo do karty za využití I/O (input/output) portu, s použitím speciálního synchronního protokolu, který je levný a jednoduchý, nebo se může použít sběrnice I^2C (inter-integrated circuit), jež se využívá při sériovém přístupu do paměti. Vlastnosti a funkce paměťových karet se připravují co možná nejvíce na míru pro požadovanou aplikaci. To z nich dělá poměrně levné řešení. Paměťové karty se běžně používají jako karty zdravotního pojištění nebo předplacené telefonní karty.

1.1.2 Bezkontaktní paměťové karty

Bezkontaktní paměťové karty se staly hitem posledních let. A to z důvodu využití v mnoha běžných činnostech, jako jsou identifikační karty s různým druhem zaměření, jízdenky městské hromadné dopravy nebo dokonce i jako elektronická peněženka, která najde uplatnění při platbě za použité služby. Bezkontaktní paměťová karta dokáže pracovat na vzdálenost 10 až 100 cm podle typu karty, dále dokáže ochránit proti neoprávněnému čtení, zapisování a mazání. Její ROM (Read-Only Memory) paměť obsahuje unikátní sériové číslo a autentizační logiku výzva-odpověď.

1.1.3 Mikroprocesorové karty

Mikroprocesorové neboli SMART karty jsou aktivní karty s procesorem a operačním systémem. Hlavním komponentem mikroprocesorových karet je mikroprocesor CPU (central processing unit), který podporuje paměti RAM (random access memory), ROM, EEPROM a I/O port, viz obr. 1.3.

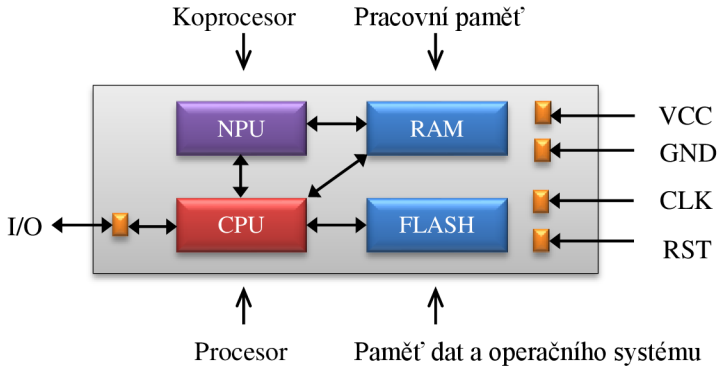


Obr. 1.3: Typická architektura mikroprocesorové karty s kontakty [25].

Maska ROM obsahuje čip, do kterého se hned při výrobě zapíše operační systém, se kterým už nejde dále manipulovat. Kód a data programu mohou být za pomocí operačního systému čteny a zapisovány do paměti EEPROM. EEPROM je čip

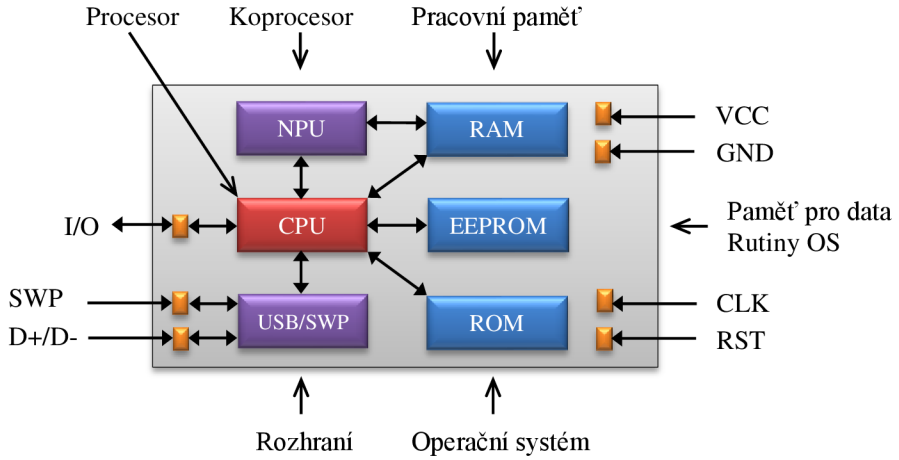
beznapěťové paměti. RAM je využita jako pracovní paměť pro procesor, která se smaže při ztrátě napájení. Sériové I/O rozhraní se nejčastěji skládá z jednoho registru, přes který jsou data předávána bit po bitu. Mikroprocesorové karty jsou ve své oblasti využití silně flexibilní. Mohou být využity a přizpůsobeny pro konkrétní aplikaci.

Moderní operační systémy čipových karet umožní provozovat na jedné kartě více aplikací [26]. V takových případech se při výrobě do paměti ROM zapíše pouze operační systém. Do paměti EEPROM se zapíší data specifických aplikací podle toho, za jakým účelem bude karta využita. Takové informace mohou být zapsány na kartu přímo nebo po vydání uživateli karty. O bezpečnost se stará speciální hardware a software, který plní úlohu dozorce. Dohlíží tak na dodržování a neporušování bezpečnostních pravidel pro různé druhy aplikací, pro které se karta využívá. Výrobci jsou v dnešní době schopni vyvíjet a dodávat mikroprocesorové čipy s velkým výpočetním výkonem, velkou paměťovou kapacitou a s důmyslnou bezpečnostní logikou. Novější typy čipových karet využívají paměť typu Flash k uložení dat a operačního systému, viz obr. 1.4.



Obr. 1.4: Typická architektura s kontakty a pamětí Flash [25].

Ta nahrazuje starší ROM a EEPROM. Výhoda spočívá ve větší pružnosti při výrobě. Operační systém lze upravit dle potřeb až po výrobě. S nástupem nových generací karet se zvyšuje paměťová kapacita, proto bylo nutné přizpůsobit i přenosovou kapacitu. Sériové rozhraní už nedostačuje, proto byly vyvinuty další protokoly a nové typy přenosových rozhraní, které mají vyhovět novým požadavkům. Jedná se o USB (Universal Serial Bus) a SWP (Single-wire Protocol) rozhraní. Postupem doby však bude přibývat čipových karet, které budou podporovat více paralelních řešení I/O jednotek viz obr. 1.5.



Obr. 1.5: Typická architektura s kontakty a rozhraním [25].

1.1.4 Bezkontaktní čipové karty

Nabízejí řadu nových služeb a řeší mnohé nedostatky, které nastávají u karet s kontakty. Kontakty jsou totiž nejčastějším zdrojem selhávání elektromechanických systémů. Faktory ovlivňující poruchovost jsou např. statické náboje, opotřebení, oxidace a znečištění.

Obrovskou výhodou bezkontaktních čipových karet je, že odpadá uživatelsky nepřívětivá manipulace s kartou ve chvíli, kdy je zapotřebí vložit kartu do čtečky. Stačí mít kartu například v kapse, kabelce či peněžence. Karta dokáže pracovat na vzdálenost 10 cm někdy i na 100 cm v závislosti na typu karty. Typy s menším dosahem mají označenou pozici, kam se má karta přiložit. Další výhodou je lepší vzhled karty, protože neobsahuje mechanické kontakty nebo může nabývat úplně jiného vzhledu.

Rozdíl je však vykoupen větší složitostí, od které se odráží i vyšší cena. Uplatnění nachází v zabezpečovacích, docházkových systémech nebo ve veřejné dopravě. Multifunkční karty dokáží zajistit více různých služeb v jediné kartě. Odpovídají kombinaci kontaktních a bezkontaktních karet. Tyto karty se nazývají karty s duálním rozhraním nebo kombinované karty. Kontaktní technologie se využívá především při platebních operacích.

1.2 Fyzikální a elektrické vlastnosti

Mnohé vlastnosti čipových karet se odvíjí od jejich předchůdců. Při myšlence vkládání mikroprocesorového čipu do plastového těla karty bylo využito mnoha norem, které specifikovaly fyzikální vlastnosti předchozích embosovaných karet a karet s magnetickým proužkem.

Ve skutečnosti je většina fyzikálních vlastností čistě mechanické povahy, např. formát karty, odolnost proti deformaci, citlivost na světlo a teplo nebo také odolnost vůči vlhkosti a elektrickému náboji. Jelikož je karta složena z plastového těla a čipu, je velmi důležité, aby byly fyzikální vlastnosti co možná nejvíce podobné. Například jestliže čip bude poškozen, ale odolá tělo karty, pak se jako celek stane nepoužitelná.

Elektrické vlastnosti čipových karet se odvíjejí od použitých mikrokontrolérů. Předpokladem je, že většina nově vyrobených mikroprocesorů pro čipové karty bude dodržovat elektrické parametry GSM (Global System for Mobile Communications), protože se uvádí i na telekomunikační trh. Situace je taková, že je mnoho různých tipů čipových karet a čteček, proto jsou vyžadovány elektricky identické vlastnosti, aby byla zajištěna kompatibilita. Základ pro elektrické vlastnosti čipových karet zajišťuje norma ISO/IEC (International Electrotechnical Commission) 7816-3. Obsahuje specifikace maximální spotřeby proudu, rozmezí napětí a aktivační a deaktivační sekvence.

1.2.1 Formáty karet

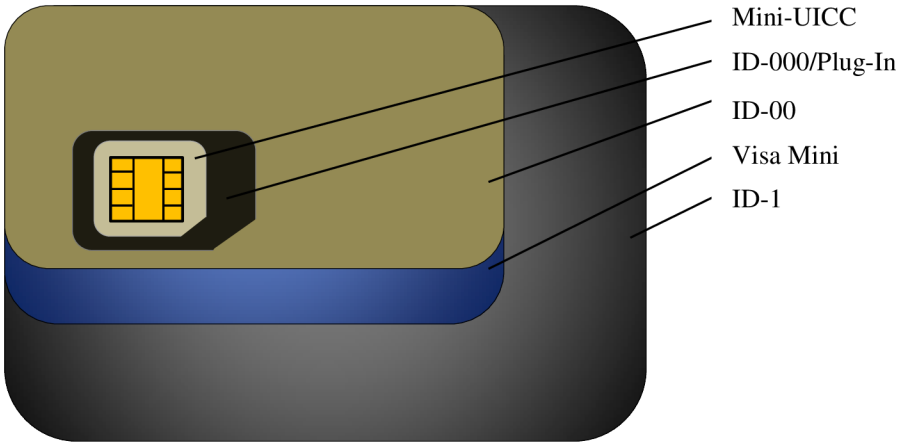
Formát ID-1 je zajisté nejznámějším formátem, který se vryl lidem do podvědomí s typickými rozměry 85,6 na 54 mm a výškou pouhých 0,76 mm. Tento standard vznikl již v roce 1985 a jeho specifikace jsou uvedeny ve standardu ISO 7810. V této době však ještě neexistovaly karty s čipem, proto standard popisoval embosované plastové karty s magnetickým proužkem. Uplynulo několik let a vznikly normy, které definovaly umístění kontaktů na kartě a zahrnovaly i přítomnost čipu v kartě. V dnešní době je k dispozici veliké množství karet, které se dají využít v mnoha aplikacích, viz tab. 1.1. Mnohdy je těžké určit, zda právě tato karta je kartou čipovou. Nejlepším vodítkem se

naskytuje vložený čip a výška karty. Rozměry karet se od počátku odvíjí zejména od potřeb uživatelů.

Karty nesmí být z důvodu snadné ztráty příliš malé, ale ani velké kvůli praktické přenositelnosti např. v peněžence, kabelce či kapse. Proto byl zvolen kompromis mezi oběma rozměry. Pokud by byla karta využita v mobilních telefonech, tak by její formát v dnešní době určitě neobstál. A to z důvodu velkých rozměrů a zbytečné hmotnosti navíc. Bylo tak zapotřebí přijít i s jinými formáty, kterými se staly ID-000 a ID-00.

ID-000 formát byl vytvořen již pro využití ve zmiňovaných mobilních telefonech a jako bezpečnostní modul ve čtečkách. Zde odpadá i potřeba větších rozměrů kvůli ztrátě, protože se karta vloží jen jednou a je bezpečně uložena v přístroji, přičemž je chráněna krytem přístroje. Není s ní nutné tak často manipulovat jako s platebními kartami.

ID-00 je poměrně nový formát, který se využívá např. u klíčenek. Rozměrově vyplňuje mezeru mezi formáty ID-1 a ID-000. Výhodou tohoto typu je pohodlnější manipulace a snížení výrobních nákladů. Jelikož sílila poptávka i po rozměrově jiných karetních formátech, přišly karty, které vyplňovaly mezery mezi formáty např. Mini UICC (universal integrated chip card) a Mini od Visa, viz obr. 1.6. Karty se vyrábí z flexibilních materiálů PVC, ABS (acrylonitrile butadiene styrene), PC (polycarbonate) a PET (polyethylene terephthalate) [25]. Nejvíce používaným materiálem je PET, protože je nelevnější a umožnuje snadné zpracování.



Obr. 1.6: Relativní velikosti formátů [25].

Tab. 1.1: Formáty čipových karet a jejich rozměry.

Formát karty		**ID-1**	**Visa Mini**	**ID-00**	**ID-000/Plug-In**	**Mini-UICC**
Vnější obdélník	Šířka [mm]	85,72	65,50	66,10	25,10	15,00
	Délka [mm]	54,03	40,00	33,10	15,10	12,00
Vnitřní obdélník	Šířka [mm]	85,46	–	65,90	24,90	–
	Délka [mm]	53,92	–	32,90	14,90	–
Výška [mm]		0,76	0,76	0,76	0,76	0,76
Zaoblení [mm]		R=3	–	R=3,18	R=1	R=0,8

1.2.2 Pole kontaktů

Pokud jsou data a elektrická energie přenášena přímým elektrickým spojením s mikrokontrolérem, potom karty musí vlastnit elektrické kontakty. Když karta obsahuje mikrokontrolér, tak se pravděpodobně jedná o čipovou kartu. Opatřuje se šesti nebo osmi pozlacenými kontakty, jež jsou viditelné na levém horním rohu karty. Umístění stanoví norma ISO 7816-2. Rozměry všech kontaktů jsou shodné s délkou 2 mm a šířkou 1,7 mm.

1.2.3 Moduly čipu

Čip je nejdůležitějším prvkem čipové karty a je velice křehký. Je proto také ukryt do modulu, aby se zabránilo poškození při každodenním používání. Čipmodul je také využíván pro poskytování kontaktních ploch. Elektrické spojení mezi čipy se provádí metodou lepení drátů. Další metodou je flip-chip technologie, kdy se jedná o přilepení polovodičového čipu k substrátu. Čip je již od výroby opatřen kontaktními kulovitými ploškami.

1.2.4 Elektrické zapojení a napájecí napětí

Čipové karty mají šest nebo osm kontaktů, přes které probíhá komunikace prostřednictvím elektrických signálů, viz tab. 1.2. Původní napájecí napětí čipových karet bylo 5V s odchylkou ±10 %. Doba a trend jdou však dopředu, a proto se postupem času toto napětí začalo snižovat. Aktuální hodnoty specifikuje norma ISO/IEC 7816-3.

Tato norma pak upravuje dělení na tři třídy. Na třídu A (5V ±10 %), B (3V ±10 %) a C (1,8V ±10 %). Norma také stanovuje zvláštní postup pro výběr dodávky napětí, přičemž se tímto postupem snaží nalézt odpovídající třídu napětí. Při získání ATR (answer to reset) se pokusí o analýzu, zda karta preferuje určitou třídu. Pokud ano, tak čtečka začne komunikovat pomocí aktivačních sekvencí požadované třídy. Napájecí proud se získává přes kontakt C1. Od dodávek napájecího napětí odvodí mikrokontrolér dodávku proudu.

Tab. 1.2: Označení a funkce kontaktů [25].

Kontakt	**Označení**	**Funkce**
C1	VCC	Napájecí napětí čipu
C2	RST	Reset
C3	CLK	Hodinový signál
C4	AUX1	D+ pro USB; jiné zařízení (dříve nevyužité)
C5	GND	Zem (referenční napětí)
C6	SPU	Standartní použití; SWP u telekomunikací
C7	I/O	Vstup a výstup pro sériovou komunikaci
C8	AUX2	D- pro USB; jiné zařízení (dříve nevyužité)

Mikroprocesory obvykle neobsahují generátor hodin. Signál hodin se musí dodat externě. Tento signál se využívá i jako referenční signál pro přenášená data. Frekvence hodinového signálu může být jiná, než vnitřní frekvence hodinového signálu pro procesor. Nejběžnější je, že vnitřní hodinová frekvence odpovídá polovině vnější frekvence. Pokud je čipová karta uvedena do režimu spánku, může se využít zastavení generátoru hodin, čím se docílí značné úspory energie.

1.3 Mikrokontroléry čipových karet

Mezi hlavní funkční komponenty čipové karty s mikrokontrolérem patří procesor (CPU), paměť více typů (RAM, ROM, EEPROM a Flash) a v neposlední řadě adresová a datová sběrnice. Dále obsahuje také jednotku pro komunikaci s okolím. S těmito jednotkami se běžně setkáváme, protože jsou povinnou součástí čipové karty. Mezi nepovinné spadají prvky např. rozhraní pro jiné přenosové protokoly a metody, speciální čipy numerických koprocesorů pro kryptografické algoritmy a další hardwarové doplňky.

1.3.1 Typy procesorů

Procesory pro čipové karty musí být velice spolehlivé, proto se používají převážně procesory, které se už v praxi osvědčily, a nejde se cestou nejnovějších trendů. Většinou je použita o jednu nebo dvě řady starší generace, než je aktuální stav techniky. Veškeré typy procesorů od sedmdesátých let až do současnosti prodělaly obrovský technologický vývoj. Za tu dobu získaly mnohem lepší parametry, než měly ve svém raném vývoji. Neustále dochází ke snižování velikosti použité výrobní technologie a energetické spotřebě.

Zvyšuje se výpočetní výkon, který se odvíjí od použité architektury a počtu tranzistorů. Narůstá paměťová kapacita a odolnost proti útokům. S příchodem větších kapacit bylo třeba rozšířit adresovatelnou paměť. S tím také souvisí zásadní nedostatky v podobě složitosti programu a komplikovanějšího rozdělení kódu programu do bank. Čím je program složitější, tím roste pravděpodobnost chyb.

Využívá se RISC (reduced instruction set computer) a CISC (complex instruction set computer) architektura. RISC má instrukční sadu maximálně redukovanou, zatímco CISC využívá instrukční sadu kompletní. Omezujícím faktorem je tu cena, proto je nutné přistupovat ke kompromisu mezi ní a požadovanými parametry.

1.3.2 Typy pamětí

Další součástí, bez které se čipové karty neobejdou, je paměť. Slouží k ukládání programu a dat. Paměti se podle energetické závislosti dělí do dvou skupin, a to na energeticky závislé (RAM) a energeticky nezávislé (ROM, EEPROM, Flash). RAM paměti zabírají na čipu nejvíce prostoru, přibližně čtyřikrát více než paměť typu EEPROM, stejně tak ROM spotřebuje oproti EEPROM přibližně čtyřikrát méně prostoru. Flash paměť zabírá téměř stejně místo jako paměť ROM [25].

ROM paměť je určena pouze ke čtení uložených dat, které jsou do paměti vloženy jednou a to hned při její výrobě. Je využívána při výrobě velkých sérií stejného typu. Pokud se v paměti vyskytne chyba, je paměť dále nepoužitelná a musí se celá vyměnit. Rychlost čtení dat z paměti je menší než z paměti RAM.

EPROM paměť se využívala pouze v začátcích vývoje čipových karet. V té době to byla jediná paměť, která byla schopna uchovat data bez potřeby napájení a byla mazatelná UV (ultraviolet) zářením.

EEPROM paměť je energeticky nezávislá a umožnuje opětovné zapisování a upravování dat podle potřeby. Je technologicky náročnější než ROM a RAM. Její životnost je určena poškozováním vrstvy oxidů. Proto tyto paměti mají omezený počet přístupových cyklů. Není proto vhodná pro ukládání citlivých dat kvůli možnému narušení bezpečnosti.

Flash paměť umožnuje jak čtení, tak i ukládání dat a je energeticky nezávislá. Správně se jedná o paměť Flash EEPROM. Je velice podobná svému předchůdci EEPROM. Existují dva typy těchto pamětí, a sice NOR flash a NAND flash. NOR flash je vhodný pro ukládání kódu programu, protože umožnuje čtení jednotlivých buněk. Nevýhodou je jeho složitost, od které se odvíjí větší nároky na plochu. Výhodou paměti NAND flash je větší hustota uložení a její nižší ceny. Naopak nevýhodou je, že nedokáže číst jednotlivé buňky, a proto je musí číst po blocích. Je nevhodná pro ukládání kódu programu, současně však neumí náhodný přístup, který procesor vyžaduje. U čipových karet převládají paměti s jednou úrovní buněk.

RAM paměť je energeticky závislá a umožnuje opakovaný zápis. V čipových kartách se používá pouze statická paměť typu SRAM (static random access memory). Je realizována jako bistabilní klopný obvod. Počet přístupů je neomezený. Výhodou je krátká přístupová doba a minimální příkon. Nevýhodou je poměrně vysoká cena v poměru cena/kapacita.

1.3.3 Doplňkový hardware

Čipové karty s běžným hardwarem nedokáží vždy splnit zvláštní požadavky, proto musí být na čip přidán doplňkový hardware. Komponenty, které bude třeba dodat, ovlivní cílové nasazení čipové karty. Doplňkové funkce, které se realizují na hardwarové úrovni, jsou většinou určeny k zamezení možných útoků na čipovou kartu.

Komunikace mezi čipovou kartou a vnějším světem se obvykle skládá z přenosu dat po obousměrném sériovém rozhraní pomocí T=0 nebo T=1 přenosového protokolu. Původně se o takový přenos dat staral pouze software operačního systému, bez využití hardwarové podpory. Kvůli složitosti takového softwaru mohl vznikat prostor pro možné chyby. Také rychlost softwaru byla ovlivňována rychlostí procesoru, což je hlavní problém této technologie. Postupem času s hektickým vývojem procesorů, které dovolily větší integraci na čipu a snížily cenu, bylo již možné přenosy realizovat za pomocí hardwaru. Řešení přišlo v podobě UART (universal asynchronous receiver transmitter), které se staly pro dnešní dobu standardem. Pokud se využije UART, který umožní přímý přístup k paměti DMA (direct memory access), ulehčí tak práci procesoru, protože dokáže data přesouvat a kopírovat.

Pro výměnu dat mají některé procesory implementovány doplňkový hardware. USB rozhraní je určeno k výměně dat s čtečkou. V závislosti na implementaci jsou podporovány dva režimy přenosu, a sice nízko rychlostní (1,5 Mbit/s) a vysoko rychlostní (12 MB/s) [25]. Přidaný hardware provádí kontrolu CRC (cyclic redundancy check), která je nezbytná při výměně dat a také NRZI (non return to zero inverted) kódování/dekódování, jež obsahuje vstupní a výstupní baffry. Výpočet CRC kódu je standardní metodou pro ochranu dat pomocí kódu pro detekci chyb. Softwarové počítání CRC je velice pomalé, protože je potřeba manipulovat s velkým počtem bitů.

Proto je vhodnější použít hardwarovou implementaci, která je rychlejší a nezatěžuje procesor. Dalším podobným doplňkovým hardwarem je MMC (MultiMediaCard).

MMC byl navržen jako levná komunikace pro paměťové karty, které obsahovaly paměti NAND flash. Komunikace za pomocí SWP je využívána mezi SIM (subscriber identity module) a NFC (near field communication) kontrolérem v mobilním telefonu souběžně s dalšími komunikačními procesy. Dalším z velice používaných rozhraní je dvouvodičová sběrnice I^2C. Ta dovoluje různé přenosové rychlosti a je funkčně podobná klasické UART.

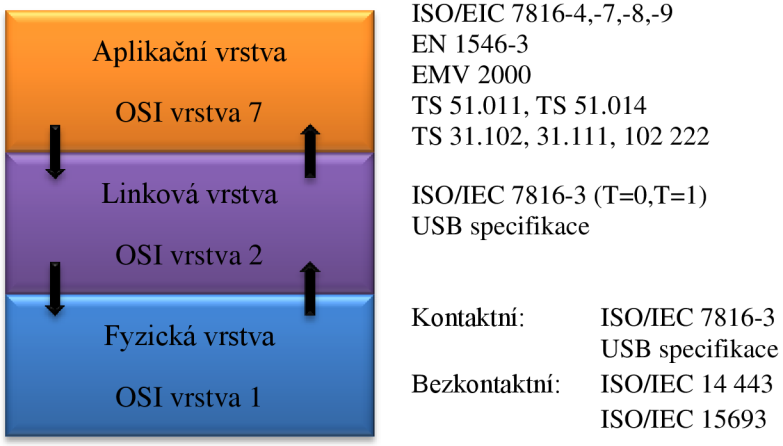
Časovač v čipové kartě je připojen k vnitřním hodinám procesoru nebo UART hodinám přes nastavitelný dělič, který má rozsah 16 nebo 32 bitů. Bez zasahování procesoru počítá hodinové impulzy od začátku do konce příkazu nebo počítá do předem stanovené hodnoty a pak vyvolá přerušení.

Generátor náhodných čísel se v čipových kartách využívá pro generování a ověřování čipových karet a čteček. Generátory hardwarové povahy by neměly být ovlivnitelné teplotou či napětím, měly by generovat opravdu náhodná čísla a ne pseudonáhodná, která jsou vytvářena za pomocí softwaru.

Další hardwarovou nástavbou může být java urychlovač, který urychluje zpracování java instrukcí a dokáže znatelným způsobem ovlivnit výpočetní výkon. Mezi koprocesory pro symetrické kryptografické algoritmy se výrazným způsobem prosadili DES (Data Encryption Standard) a nověji AES (Advanced Encryption Standard). Jdou jednoduše hardwarově implementovat a snižují doby potřebné k výpočtu. AES dokáže pracovat s klíči dlouhými 128, 192 a 256 bitů. Koprocesor pro asymetrické kryptografické algoritmy RSA (Rivest, Shamir and Adleman Algorithm) a eliptické křivky je optimalizován pro aritmetické operace modulo a získání zbytku po dělení velkých čísel. Tyto výpočty jsou potřebné při výpočtu klíčů. Koprocesory RSA dokáží pracovat s délkou klíče 1024 bitů a eliptické křivky až do velikosti 256 bitů.

1.4 Komunikace s čipovými kartami

Celý proces přenosu dat do čipové karty a z čipové karty může být reprezentován pomocí vrstev OSI modelu, viz obr. 1.7. Tento model rozlišuje elektrické události na vstupu a výstupu linek logickými procesy v přenosovém protokolu a činností aplikací, které používají tyto procesy. Chování a vztahy mezi těmito vrstvami určuje několik mezinárodních standardů.



Obr. 1.7: ISO model komunikace mezi čtečkou a čipovou kartou [25].

Komunikace mezi čipovou kartou a čtečkou probíhá v half-duplexním režimu. Jeden vysílá, druhý přijímá a naopak. To znamená, že v jeden okamžik nemohou jak přijímat, tak vysílat. Komunikaci pokaždé zahajuje čtečka a karta vždy reaguje na příkazy čtečky, viz obr. 1.8. Tomuto režimu odpovídá komunikace master-slave. Master je čtečka a čipová karta je slave. Při vložení karty do čtečky se nejprve spojí kontakty mechanicky, dále se pět aktivních kontaktů povoluje elektronicky. Karta se uvede do činnosti přivedením napájení na RESET a pak pošle odpověď na RESET (ATR) čtečce. Odpověď je posílána přes I/O linku a obsahuje informace o napájecím napětí, hodinový signál a jaký byl použit reset signálu. Následně čtečka ATR, obsahující parametry týkající se karty a přenosu dat, vyhodnotí a pošle první příkaz. Karta zpracuje příkaz a vygeneruje odpověď, kterou odešle zpět čtečce.

Mezi ATR a prvním příkazem posílaným kartě, může čtečka volitelně zaslat příkaz PPS (protocol parameter selection). Protokol výběru parametrů je nezávislý na použitém protokolu a umožňuje změnit některé z parametrů protokolu, pokud je to povoleno. Po této fázi inicializace začne komunikovat aktuální přenosový protokol.

Existují dva typy nastavení čipové karty, a to studený a teplý reset. Studený je spuštěn při připojení čipové karty a nastavování během probíhajícího procesu, naopak teplý reset probíhá již při napájení čipové karty, kdy dojde pouze k provedení resetování signálu z čtečky. Nejběžnější používanou formou výměny zpráv mezi kartou a čtečkou je přenos dat pomocí šesti či osmi kontaktů. V kartě není potřeba integrovat anténu, což je výhodou, stejně jako jednoduchý přenos.

Čtečka		**Čipová karta**
Reset	→	**Spuštění operačního systému čipové karty**
	←	**ATR**
Volitelná část		
PPS požadavek	→	**PPS zpracování**
	←	**PPS odpověď**
Příkaz APDU 1	→	**Zpracování příkazu**
	←	**Odpověď APDU 1**

Obr. 1.8: Sekvence příkazů a operací při startu čipové karty [26].

1.4.1 Linková vrstva

Na linkové vrstvě pracují přenosové protokoly, které definuje norma ISO/EIC 7816-3. Nejvíce mezinárodně využívaným standardem se stal protokol T=0 a T=1. T=0 je starší z dvojice a byl zaveden v roce 1989, struktura příkazu, viz obr. 1.9. Mladší protokol, tj. T=1, byl uveden v roce 1992. Datové jednotky, přepravované těmito přenosovými protokoly, nemají mechanizmus pro opravu chyb a jsou pojmenovány jako přenosový protokol datových jednotek TPDUs (transmission protocol data unit). Přehled a srovnání základních vlastností, výhod a nevýhod protokolu T=0 a T=1, viz tab. 1.3.

Obr. 1.9: Struktura příkazu u protokolu T=0.

Tab. 1.3: Souhrn vlastností asynchronních protokolů T=0 a T=1 [25].

Kritérium	**Protokol T=0**	**Protokol T=1**
Transport dat	Asynchronní Half-duplex Bajtově orientovaný	Asynchronní Half-duplex Blokově orientovaný
Standard	ISO/IEC 7816-3, TS 51.011, EMV	ISO/IEC 7816-3, EMV
Řetězení bloků	Nepodporováno	Podporováno
Dělitel	Volně definovatelné, obvykle 372	Volně definovatelné, obvykle 372
Detekce chyb	Paritní bit	Paritní bit, Chybový detekční kód
Paměť potřebná pro implementaci	300 bajtů	1100 bajtů

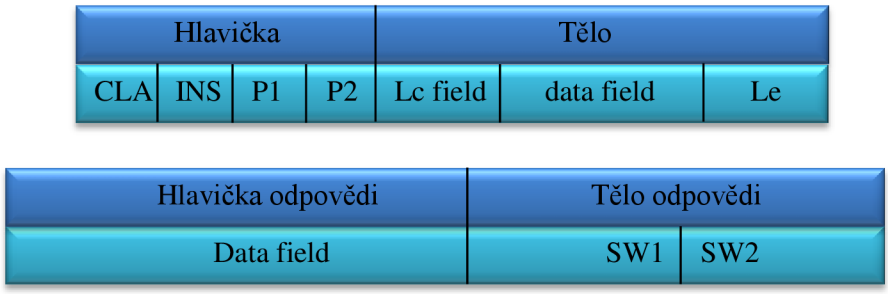
1.4.2 Aplikační vrstva

U čipových karet je aplikační vrstva přímo nad vrstvou přenosových protokolů. Na aplikační vrstvě se pro přenos používá mezinárodně standardizovaná datová jednotka APDU (application protocol data unit). APDU je jednotný formát zpráv, který se používá k výměně všech dat mezi čipovou kartou a čtečkou. Dodržuje normu ISO/IEC 7816-4.

Standard je navržen tak, aby byl nezávislý na přenosovém protokolu. Protokol APDU rozlišuje dva příkazy C-APDUs a R-APDUs. C-APDUs jsou příkazy odeslány kartě a R-APDUs jsou odpovědi na odeslané příkazy. Struktura příkazu je definována prvním bajtem. Příkaz APDU je rozdělen na dvě části, hlavičku a tělo. Odpověď je rozdělena na hlavičku odpovědi a tělo odpovědi, viz obr. 1.10.

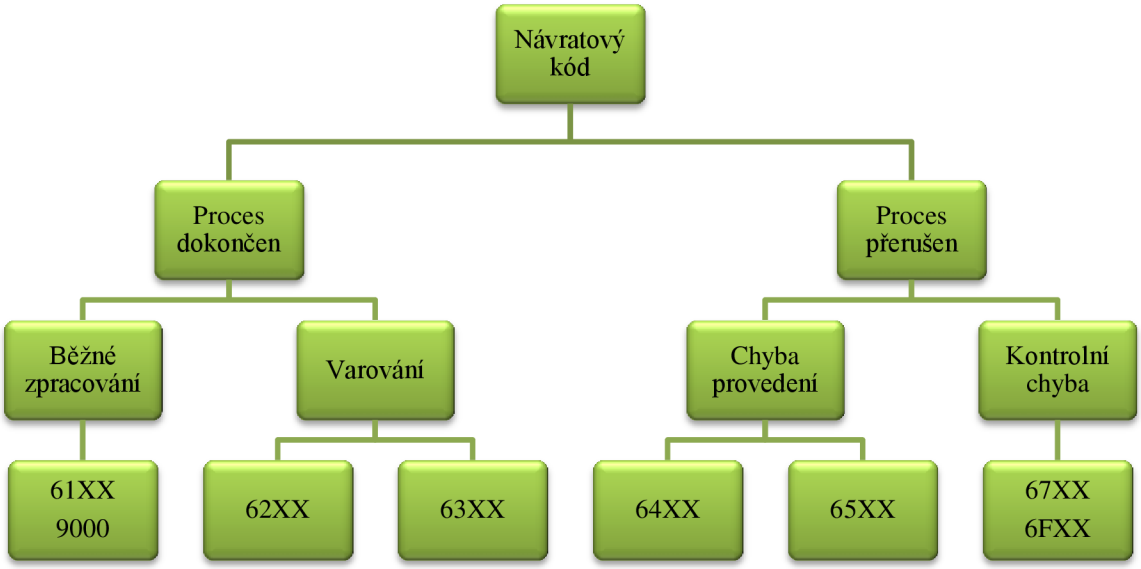
Hlavička je povinná a obsahuje čtyři části. CLA (class) slouží pro identifikaci instrukční třídy (1 bajt). INS (instruction) označuje konkrétní instrukci z instrukční třídy definovanou CLA (1 bajt). P1 (parameter 1) a P2 sloužící k definici parametru (1 bajt).

Tělo obsahuje volitelné části, Lc (length command) udává velikost dat předávaných v rámci příkazu do karty v bajtech (1 bajt). Datové pole v obou případech obsahuje transportovaná data. Le (expected length) udává velikost dat očekávaných v odpovědi v bajtech (1 bajt). SW1 (status word) a SW2 je povinné pole, které obsahuje návratové kódy příkazu (1 bajt). Existuje více než 50 návratových kódů, které udávají, jak byl příkaz vykonán např. proces ukončen nebo proces přerušen. Obrázek 1.10 znázorňuje strukturu příkazu a odpovědi.



Obr. 1.10: Struktura příkazu a odpovědi u APDU.

Chybové odpovědi APDU můžou obsahovat dvě pole stavových informací, jsou označeny SW1 a SW2. Tyto návratová pole vrací mikroprocesor karty čtečce karet, která obdrží návratový kód. Kód má podle standardu ISO 7816-4, schéma číslování. První bajt slouží k vyjádření kategorie chyby a následující bajt nese informaci, která se používá k předání konkrétního příkazového stavu nebo chybových údajů. Číselné schéma je zobrazeno, viz obr. 1.11.



Obr. 1.11: Návratové kódy ISO/IEC 7816-4.

Bezpečnostní příkazy jsou propojeny s každou komponentou souborového systému, ten je omezen přístupovými právy. Přes tahle přístupová práva může být definováno, že čipové karty musí být uvedeny do stavu, kdy jsou úspěšně provedeny série příkazů, které dovolí přístup k souborovému systému.

Mezi nejzákladnější operace souborového systému patří výběr konkrétního souboru. Do vybraného souboru, lze zapisovat nebo číst ze souboru. Někdy je ale vyžadováno před provedenou operací zadat PIN, a tím dokázat nějaké společné tajemství např. tajný klíč karty. Příkaz Verify (ověření) je příkaz odesílaný aplikací na straně čtečky bezpečnostnímu systému na kartě, který kartě povoluje ověřit správnost hesla uloženého na kartě viz obr. 1.12. Úspěšné provedení tohoto příkazu znamená, že bylo dobře zadáno heslo a je povolen následný přístup k střeženému souboru. Pokud příkaz neproběhne správně, je přístup omezen.

CLA	INS	P1	P2	Lc	Data
$C0_{16}$	20_{16}	00_{16}	00_{16}	03_{16}	$53_{16}\ 61_{16}\ 53_{16}$

Obr. 1.12: Příkaz Verify.

2 Bezpečnost čipových karet

Čipové karty umožnují bezpečné ukládání důvěrných dat za předpokladu připravenosti hardwaru na tento účel a využití bezpečných kryptografických algoritmů. Další nedílnou součástí bezpečnosti čipových karet jsou metody, zásady, a to jak pro výrobu čipové karty, tak pro vývoj aplikací.

Bezpečnost aplikací na čipových kartách je založena na tajném klíči kryptografického algoritmu. Je nemožné zajistit dokonalé zabezpečení, které zabrání všem útokům. Zde záleží na úsilí, finančních prostředcích a času, který je schopen útočník obětovat pro svůj záměr. Pokud využije nemalých prostředků, velkého úsilí a dostatečně dlouhé doby, může narušit bezpečnost, nebo systém zdiskreditovat (zmanipulovat). Tohle všechno provádí jen za předpokladu, že se mu informace, které získá, vyplatí. Přínos je pro něj větší než vynaložené náklady.
Bezpečnost čipové karty je postavena na čtyřech složkách [25].

- Samostatná karta
- Hardwarový čip
- Operační systém
- Aplikace chránící data a programy

Za bezpečnou kartu se považuje taková karta, která využívá všech čtyř bodů a jejich obranné mechanizmy jsou dobře navrženy a implementovány. Pokud některý z těchto bodů nesplňuje nutné požadavky, karta přestává být bezpečnou, protože je narušen bezpečnostní vztah. Karta je určena přibližně k době života okolo tří roků. Pro tak krátkou dobu se dají dobře implementovat protiopatření, která znemožní nebo minimalizují šance možných útoků na úspěch. Proto je cílem vývojářů a výrobců poskytnout karty, které budou bezpečné po tuto dobu a zůstat ve výhodě před potenciálními útočníky. Lze to přirovnat ke známé hře na kočku a myš, zde je to hra opatření a protiopatření při útoku a obraně. Pokaždé není možné udržet takové vedení, proto je důležité při návrhu dbát i na to, aby jeden povedený útok na čipovou kartu nezkompromitoval celý systém např. GSM kde je využito karet SIM.

Při objevení nějakého bezpečnostního problému na něj lze zareagovat při další generaci karet a tím bezpečnost zvýšit. Pokud ale potřebujeme karty používat delší dobu, je tento cíl mnohem hůře splnitelný např. u SIM karet používaných v GSM, u kterých se životnost pohybuje mezi 10-15 roky [25]. Ovšem systém GSM má tu výhodu, že je online systémem a tak umožňuje reagovat proti známým formám manipulace. Útočník se může věnovat výrobě klonů, tím vytvoří přesné kopie. Nevýhodou je, že online systém je snadno pozná. Další možností je vytvořit přímo novou kartu, která není kopií. Tyto karty jsou odhalitelné opět pouze v online systému a to porovnáním seznamu všech použitých karet s jejich unikátními identifikátory.

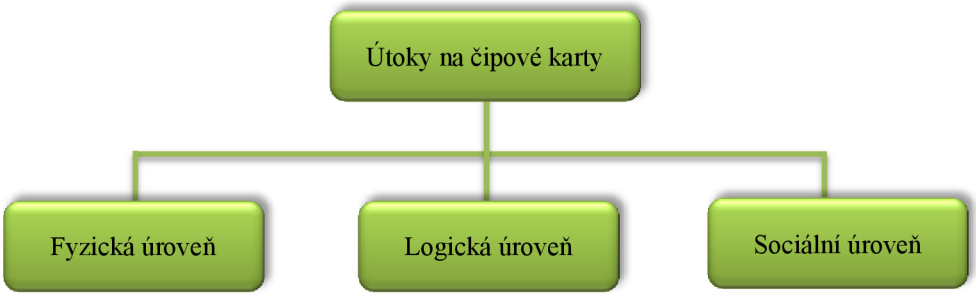
Čipové karty mohou spadat do čtyř úrovní zabezpečení FIPS 140 (Federal Information Processing Standards). Jsou to počítačové bezpečnostní standardy, které specifikují požadavky na kryptografické moduly. NIST (National Institute of Standards and Technology) vydal publikaci 140 pro koordinaci požadavků a norem pro kryptografické moduly, které zahrnují hardwarové tak i softwarové součásti pro použití v různých státních agenturách ve spojených státech. FIPS 140 ukládá požadavky v jedenácti různých oblastech. Měl zaručovat, že systém postavený z použitých modulů

je bezpečný. Požadavky nejsou kladeny pouze na kryptografické moduly, ale také na jejich dokumentaci a nejvyšší stupeň zabezpečení, vyhodnocuje i zdrojový kód.

FIPS 140-2 definuje čtyři úrovně bezpečnosti 1 až 4. Úroveň jedna stanoví nejnižší úroveň zabezpečení, klade velmi malé požadavky a tím určuje základní bezpečnostní požadavky na kryptografický modul. Úroveň dvě vylepšuje fyzickou bezpečnost kryptografického modulu z první úrovně. Úroveň tři vyžaduje zvýšenou fyzickou bezpečnost a odolnost proti útočníkovi, aby nezískal přístup k tajným bezpečnostním parametrům, které probíhají uvnitř modulu. Úroveň čtyři poskytuje nejvyšší úroveň zabezpečení. Fyzická ochrana zajišťuje kryt, který je kolem kryptografického modulu a je určen k detekci narušení zařízení útokem z libovolného pohledu. Úrovně bezpečnosti konkrétního zařízení nebudou zajisté trvat věčně. Postupem času dojde k jeho poklesu, protože útok bude možné provést v budoucnosti, až nároky na požadovaný útok nebudou tak velké a stane se dostupným. V současné době je ve vývoji standard verze FIPS 140-3 [7].

2.1 Klasifikace útoků na čipové karty

Útoky na čipové karty se dělí na tři typy, a sice na útoky na sociální, fyzické a logické úrovni, viz obr. 2.1. Další typy útoků využívají kombinace předešlých. Prvotní útok připraví podmínky pro následný útok. Jak je dobře známo, je podstatně jednodušší se bránit proti známým formám útoku, než proti neznámým [25].



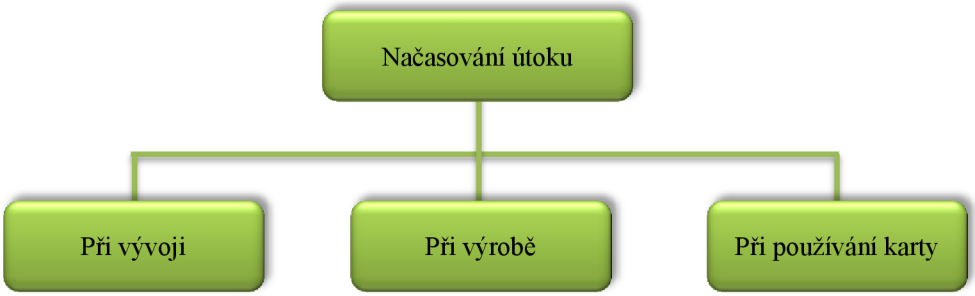
Obr. 2.1: Klasifikace útoků na čipové karty.

Útoky na fyzické úrovni vyžadují určité množství technických zařízení. Proto je nutné zajistit fyzický přístup k hardwaru a nějakým možným způsobem hardware analyzovat.

Fyzikální metody pro analýzu čipových karet se dělí na statickou a dynamickou analýzu. Při statické analýze není mikrokontrolér v provozu, naopak u dynamické analýzy je mikrokontrolér v provozu. Fyzické útoky se opět dělí na statické a dynamické útoky. U statických fyzických útoků není útočník omezen časem, může postupovat svým vlastním tempem. Naopak u dynamických útoků je již útočník omezen časem. Musí měření provést rychle a používat hodně rychlé záznamové zařízení.

Útok na logické úrovni je založen na výpočtu nebo přímém záměru. V dnešní době využívá většina útoků této formy. Do této kategorie spadá jak klasické dešifrování, tak známé nedostatky operačních systémů anebo trojské koně. Útoky můžeme opět rozdělit na aktivní a pasivní. Při pasivním útoku, který je neinvazivní, se snaží útočník využít analýzy zašifrovaného textu nebo kryptografického protokolu bez jeho zásahu. Aktivní útok, který je řazen do skupiny invazivních útoků se snaží manipulovat s přenášenými daty nebo přímo s mikrokontrolérem.

Útok na sociální úrovni se zaměřuje na lidi, kteří manipulují s čipovými kartami. Do této skupiny patří vývojáři čipů, vývojáři softwaru a vlastníci karet. Tomuto typu útoku dokáží technické prostředky odolávat jen stěží. Prioritou proto musí být dodržování organizačních prostředků, např. zajištění nemožnosti vidět zadávání pinu za pomocí bočních bariér. Je vhodné algoritmus zveřejnit a neudržovat jej v tajnosti, aby jeho síla nebyla závislá jen na jeho utajení. Při podrobení zkoumání celou veřejností jsou lépe odhalitelné nedostatky, které ovlivňují bezpečnost. Pokud se v průběhu testování objeví chyby, dají se odstranit a následně je možné opravený algoritmus znovu použít. Načasování útoku na čipovou kartu může být rozděleno, jak je znázorněno, viz obr. 2.2.



Obr. 2.2: Klasifikace podle načasování útoku na kartu.

2.1.1 Klasifikace útočníků

Nejprve je zapotřebí získat představu o možných typech útočníků a útoků, odhadnout jejich silné a slabé stránky. Tyto informace pak zahrnout do návrhu obranné strategie a obranných mechanizmů. Jednotlivé typy útočníků můžeme rozdělit do dvou skupin na organizace a osoby. Skupina osob zahrnuje např. hackera, kriminálníka a zasvěceného. Skupina organizace využívá např. akademiků, zločinců a konkurence. Každý z možných útočníků může využívat různé množství zainteresovaných osob, které mají různé schopnosti a možnosti.

Útočníci si většinou vybírají formy útoků, kde stačí malé náklady a úsilí. Jsou motivováni chtíčem nebo si kladou za cíl se zviditelnit a získat obdiv a lepší postavení v jejich komunitě. Při provedení úspěšného útoku může výrobce přijít o jeho dobrou pověst, což nezůstane nepřehlédnuto a následně se to projeví na jeho příjmech. Odběratelé se určitě přikloní k spolehlivějším řešením než k těm, která byla narušena. Pokud je vytvořen návod a program, který dokáže provést útok automaticky a v dnešní době si dokáže šířit internetem obrovskou rychlostí, tak se výrobce ocitne rázem ve velice nepříjemné situaci. Na jaře roku 1998 čelilo několik operátorů sítě GSM událostem, kdy byly provedeny útoky proti kryptografickému algoritmu COMP 128, který byl použit u A3 a A8 funkcí [25]. Útok neměl zásadní vliv na provoz sítí, ale nastínil možné útoky. Následkem tohoto útoku byl výbor donucen vydat prohlášení, kde bylo uvedeno, že COMP 128 byl jen příklad a poskytovatelům doporučil přijít s vlastními algoritmy. Byly implementovány určité opatření, ale ty stále nedosahovaly potřebné funkčnosti, tím nadále poskytovatelé ignorovali možné hrozby [3]. Většinou je jedno, jestli měl útočník dobrý nebo špatný záměr. Pokud útok chtěl využít buď ve svůj prospěch anebo pouze poukázat na mezeru v zabezpečení, jsou proti němu provedeny právní kroky.

2.1.2 Klasifikace a atraktivita útoků

Pokud má být zajištěno uspokojující preventivní opatření, které se bude využívat, musí se brát v potaz i atraktivnost útoku a vyhodnotit všechny možné bezpečnostní slabiny. Hodnocení se provádí matematickým způsobem, když se vezmou pravděpodobné cíle útoku a jejich potřebné náklady na uskutečnění. Zjednodušený popis poměrně dobře dokáže odhadnout atraktivnost možných útoků pro útočníka, protože si útočník většinou vybírá takovou formu útoku, kde musí vynaložit co možná nejmíň finančních nákladů a úsilí. Atraktivita je velmi silně závislá na vybavení, které má útoční k dispozici. Útočník je ovlivněn šesti faktory při jeho přípravě na útok, viz tab. 2.1.

Tab. 2.1: Faktory ovlivňující úsilí a náklady potřebné při útoku na bezpečnostní prvky [25].

Stupeň atraktivity	nízká	průměrná	vysoká
Potřebné znalosti a dovednosti	vysoké	průměrné	nízké
Nezbytné tajemství	velké	průměrné	malé
Potřebný čas	dlouhý	průměrný	krátký
Pořízení nezbytného vybavení	těžké	průměrné	lehké
Přístup napadené součásti	těžký	průměrný	lehký
Hodnota výsledku (peníze nebo reputace)	nízká	průměrná	vysoká

Čipové karty jsou ve výrobě od druhé poloviny 80. let, již od této doby byly známy některé z útoků. Útoky z první poloviny 90 let byly směřovány proti hardwaru čipové karty. V druhé polovině 90 let započaly útoky využívat matematické podstaty a kombinovat je s analýzou, která se prováděla na logické úrovni. Každý rok se objeví v průměru dva nové typy útoků. Postupem času s velkým rozvojem internetu se začaly využívat mnohé teoretické útoky, které do té doby nebyly možné. Internet umožnil vyřešení dvou zásadních problémů. Prvním je snadná a dostupná komunikace a sdílení možných návodů a zkušeností. Druhým je možnost získání velké výpočetní síly za pomocí internetu, konkrétně se o něj opírá útok hrubou silou, který zkouší všechny možné varianty klíče. Při spojení velkého množství osobních počítačů prostřednictvím internetu, lze získat i výpočetní sílu superpočítače. Využito je volného procesorového času počítačů z celého světa pomocí internetu. Ty se věnují distribuovanému výpočtu, je to výpočet, který je rozporcován na menší části a každý počítá jen přidělenou část, která není tak složitá jako celek. To může být použito jen u algoritmů, které jsou paralelizovatelné. Super počítače mohou způsobit kryptografům značné problémy.

Rozhodně neexistuje velká množina útočníků, kteří by jen tak lehce mohli získat přístup k potřebným systémům. Pokud ovšem takový přístup získají, např. to dokázala mezinárodní skupina v laboratořích LACAL (Laboratory for cryptologic algorithms) ze švýcarského Lausanne. Na mušku si vzali hashovací algoritmus MD5 (Message-Digest algorithm 5), který úspěšně pokořili. Celkový výpočet jim trval několik desítek hodin a byl proveden na clusteru, který byl poskládán z více než 200 herních konzol PlayStation 3 s procesory Cell od firmy IBM [5]. V bezpečí dnes už není ani novější hashovací algoritmus SHA-1 (Secure Hash Algorithm-1). Protože si takové výkonné systémy nelze jen tak pořídit, tak se v dnešních dobách dají využít nabídky třeba od amerického Amazou. Ten umožňuje pronájem virtuálního serveru. Jmenuje se EC2

(Amazon Elastic Compute Cloud) a je postaven na virtuálním Linuxu nebo Windows serveru a aplikačním serveru, na kterém si můžete spustit vámi vytvořené aplikace. Následně zaplatíte jen za procesorový čas. Nejdražší varianta je zpoplatněna přibližnou částkou dolar za hodinu. Tím se dostanete k výkonu, jakému přibližně odpovídá 20 Opteronů nebo Xenonů na taktu až 1,2 GHz, paměťová kapacita je 7 GB RAM a uložiště o velikosti 1700 GB [5].

2.2 Fyzické útoky

Fyzické útoky a metody analýzy jdou rozdělit do dvou skupin na statický typ, kdy čip není v provozu, ale může být připojen k napájení, anebo na dynamický typ, kdy čip provádí určené operace, což je mnohem složitější, protože se musí zpracovat velké množství informací. Útoky na fyzické úrovni jsou finančně nákladné. Vyžadují fyzickou manipulaci s čipem karty a při tom používají reverzní inženýrství. Lze je rozdělit do čtyř skupin, a sice na útoky na procesor, paměť, sběrnici nebo senzory. Ochranné mechanismy v hardwaru tvoří základ pro další ochranné mechanismy. Při útoku na hardware je potřeba vlastnit speciální technické zařízení. Do potřebného vybavení může spadat mikroskop, laserová řezačka, mikromanipulátory, chemické leptání, rychlé počítače, prostředky pro záznam a vyhodnocení elektrických procesů v čipu. Při provádění útoku na fyzické úrovni je zapotřebí si kartu předem připravit. Prvním krokem je odstranění modulu z karty např. pomocí nože. Druhým krokem je odstranění epoxidové pryskyřice a očištění např. použitím kyseliny dusičné a dočištění acetonem. Na útočníka však čeká ještě řada dalších bezpečnostních opatření.

Ochrana se dělí na pasivní a aktivní prvky. Pasivní se zakládají na technologii výroby polovodičů a zahrnují všechny metody a procesy, které se mohou využít k ochraně paměti. Další součást má za úkol odolávat různým typům analýz. Do aktivních ochranných prostředků spadají různé druhy čidel, které jsou přímo integrovány na křemíkový čip, např. světelný nebo tepelný senzor. Při narušení těchto senzorů dojde ke ztrátě citlivých dat. Software čipových karet se stará o zpracování a vyhodnocení informací získaných ze senzoru, to lze ovšem provádět jen tehdy, pokud je čip funkční a pod napájením. Dále jsou uvedeny některé z aktivních a pasivních fyzických útoků na čipové karty [28].

Aktivní útoky

- Suché leptání dokáže oklamat senzory, které testují přítomnost pasivační vrstvy.
- Laserový nůž zvládne přerušit spoje a odstranit pasivační vrstvy.
- Iontový paprsek dokáže vytvořit nové spoje.

Pasivní útoky

- Mikroskopické sondy osahují sadu jehel, které umožní elektrické sledování signálů na čipu.
- Elektronový mikroskop umožňuje sledování signálů procházejících přes sběrnici.
- Spodní rentgenování dovolí pozorování tranzistorů zespod čipu za využití vlnové délky, pro kterou je křemíkový substrát průhledný.
- Elektrooptické vzorkování sleduje krystal niobátu lithia laserovým paprskem a tím zjišťuje přítomnost elektrostatického pole pod krystalem.

2.3 Logické útoky

Logické útoky nevyžadují fyzickou manipulaci s čipem karty. Využívají softwarových chyb, které zůstanou neodhaleny při bezpečnostních testech a používání, protože není zcela možné všechny chyby odstranit. Na čipové karty, podporující Java Card, je možné nahrát a posléze spustit nahraný software. Tento software může být napsán jako škodlivý, který se dá použít k přípravě logického útoku.

Pravděpodobnost chyby, např. funkční, v softwaru čipových karet je poměrně velká. Špatná kontrola hodnot parametrů určitých příkazů a nekorektní reakce na chybné příkazy nebo chyby v kryptografických algoritmech patří mezi chyby, které není lehké odhalit. Funkční chyby jsou schopny oklamat čipovou kartu a získat od ní tajné informace nebo je pozměnit. Takové útoky nemají destruktivní charakter a nepotřebují k provedení značné prostředky. Většinou jsou málo úspěšné. Opravdu užitečnými se mohou stát, pokud jsou navzájem zkombinovány i s fyzickým útokem. Dále jsou uvedeny některé z možných logických útoků na čipové karty [25].

- Chyby transportních protokolů – zneužívá chyb u přenosových protokolů.
- Průzkum souborového systému – prohledává souborový systém karet.
- Využívání chyb – útok využívá objevených chyb, které následně může využít k provedení nelegálních operací.
- Objevení neplatných a nepovolených požadavků – hledá neplatné a zakázané požadavky, kterých následně využívá.
- Kryptografická analýza – jedná se o metodu získávání tajné informace bez znalosti tajného klíče, např. útok hrubou silou.
- Nelegální aplikace – používá škodlivé aplikace, které využívají nepovolené instrukce nebo neplatné parametry. Potom je možné získat např. výpis z paměti nebo provádět operace, které potřebují zvláštní oprávnění nebo dokonce získat plnou kontrolu nad kartou.

2.4 Kryptografické funkce

Kryptografické funkce čipových karet pokrývají celou řadu současných kryptografických algoritmů. Jednou z těchto funkcí je šifrování a dešifrování dat, které se provádí pomocí softwaru a hardwaru. Další funkcí je autentizace entit, která je obvykle prováděna pomocí symetrických šifrovacích algoritmů.

Dnešní doba směřuje od používaného DES a Triple DES k nasazování AES, a to z důvodu větší bezpečnosti. Ty funkce, které jsou založeny na asymetrických kryptografických algoritmech, poskytují celou řadu podpisových funkcí. Hash algoritmy jsou také podporovány v čipových kartách. V čipových kartách jsou používány symetrické kryptografické algoritmy např. AES (128,196,256 bitů), DES (56 bitů), TDES (112 bitů), IDEA (128 bitů). Asymetrické kryptografické algoritmy např. ECDSA (160-256 bitů), RSA (1024-2048 bitů), DSA. Hash funkce např. HMAC, MD5, RIPEMD-160, SHA-1 a SHA-2.

3 Útoky postranními kanály

Útoky se zaměřují na zařízení a sledování mikroprocesoru v činnosti, jedná se tedy o úplně jiný přístup, který při svém prvotním představení odhalil překvapivé slabiny a možný velký potenciál. Útoky postranními kanály se obvykle snaží využít toho, že je výpočet za určitých okolností na mnoha místech přímo ovlivňován vstupními daty. Zneužití proběhne, pokud se informace o citlivých datech dají získat přes výstupní kanály.

První útoky pozorovaly vliv citlivých informací na výpočetní čas. Novou myšlenkou bylo shromažďování informací o aktuální spotřebě zařízení, jako např. u čipové karty. Tento typ shromažďování informací o spotřebě se nazývá napěťově proudová analýza, která byla v posledních letech hodně vylepšena a rozšířena. Nejedná se pouze o teoretické útoky. Jdou velmi snadno aplikovat na čipové karty, které nevlastní žádné adekvátní protiopatření, i když útočník nemá téměř žádné zvláštní znalosti nebo vybavení. Útoky založené na napěťově proudové analýze jsou nákladnější, proto útočník musí investovat do speciálního hardwarového vybavení (např. do drahého osciloskopu). Ale v zásadě všechny z těchto útoků lze použít v reálné praxi. Integrace všech možných protiopatření nepředstavuje žádný snadný úkol. Nutná je znalost hardwaru a pochopení celé problematiky, což má zásadní význam pro zajištění větší úrovně zabezpečení. Musí být pochopeny principy možných útoků, aby se daly navrhnout účinné protiopatření nebo způsoby, které jim budou předcházet. Integrace efektivního protiopatření přímo ovlivňuje celkové náklady na implementaci.

Během posledních let se ukázaly útoky postranními kanály jako hlavní hrozba při zabezpečování citlivých informací. V závislosti na povaze úniku informací můžeme rozlišovat mezi útoky proti hardwaru nebo softwaru, který implementuje kryptografické rutiny. Myšlenkou postranní analýzy je odvodit nějaká tajná data z uniklé informace. Tyto nežádoucí kanály byly použity k narušení implementace všech hlavních šifrovacích algoritmů jako je DES, AES, Diffie-Hellman nebo COMP 128, jak v oblasti softwarové, tak hardwarové. Ve skutečnosti je analýza postranních kanálů tak silná, že většina útoků může uspět v praxi při použití pouhého zlomku informací uniklých tímto kanálem. Úniky informací z postranních kanálů jsou jen zřídka kombinovatelné.

Postranním kanálem je každý z nežádoucích způsobů výměny informací mezi kryptografickým modulem a jeho okolím. Často má podobu fyzikálních veličin, které se snaží útočník využít ve svůj prospěch, jako např. spotřeba energie nebo doba potřebná k provedení určité operace. Útočník měří tyto hodnoty, které jsou určitým způsobem závislé na probíhajících výpočtech uvnitř napadeného modulu. U chybových kanálů se přes normální datový výstup dostane i tajná informace, protože se objeví chyba v napadeném zařízení. Chyby mohou být úmyslné nebo neúmyslné. Úmyslná bývá vytvořena záměrně aktivním ovlivněním modulu. Kryptografické moduly jsou nejcitlivější součástí systému, proto je na ně také nejvíce zaměřován útok, a z tohoto důvodu pak musí být nejvíce chráněny.

V současné době jsou v čipových kartách samozřejmě zpravidla používané mikroprocesory, které obsahují několik hardwarových protiopatření k zamezení těchto útoků. Protiopatření integrované do softwaru v zásadě rozlišuje dva následující přístupy. První je práce na algoritmické úrovni, druhý je používání speciálních kódovacích technik, které by se měly zabývat potenciálními slabinami skutečného hardwaru. Randomizace je nejjednodušší a nejvíce běžně používaná technika, využívaná k zabránění těmto útokům.

3.1 Časová analýza

TA (Timing attack) časová analýza se poprvé objevila v roce 1995 v publikaci od Paula Kochera. V tomto článku Kocher využívá rozdíly výpočetních časů při prolomení implementace RSA kryptografického systému na základě diskrétního logaritmu. Využívá časové informace, které unikají při provádění kryptografického výpočtu s tajným klíčem, jelikož jsou délky výpočtů na klíči závislé.

Časová informace zde představuje typ postranního kanálu. Tyto informace mohou napomáhat k odhalení tajného klíče. Útok se opírá o analýzu zpracování času mezi dobou zadání příkazu čtečkou a odpovědí čipové karty. Časová analýza je vážnou hrozbou pro čipové karty. Tato forma útoku je známá již dlouhou dobu.

Všechny moderní karty jsou odolné proti tomuto typu útoku. Využívají jen takové kryptografické algoritmy, u kterých není šifrovací a dešifrovací čas závislý na vstupních datech. Tyto algoritmy jsou složitější a pomalejší než verze, které nejsou odolné proti časové analýze. Algoritmus je navržen tak, aby délka cesty přes algoritmus byla stejná pro všechny kombinace známého textu, zašifrovaného textu a klíče. Nejprve se musí zjistit nejdelší cesta a ta se potom použije jako výchozí. Dále se všechny ostatní cesty upraví tak, aby odpovídaly délce výchozí cesty.

3.2 Napěťově proudová analýza

PA (Power analysis attacks) napěťově proudová analýza je jeden z nejobávanějších útoků v dnešní kryptoanalýze, publikována byla v roce 1998. Napěťově proudová analýza využívá informace o spotřebě elektrické energie kryptografického zařízení při vykonávání výpočtu. Výkonový postranní kanál poskytuje informace o prováděných operacích a také o parametrech, které byly použity při výpočtu. Pokud se analyzuje změna spotřeby elektrické energie během vykonávání výpočtu, lze odvodit prováděné operace, které poslouží při získávání tajného klíče.

Energii, kterou čipová karta spotřebuje při výpočtu, není obtížné změřit. Čipové karty nevlastní vlastní napájecí zdroj, napájení přijímají externě, proto jsou napěťově proudovou analýzou lehce napadnutelné. Analýzu lze aplikovat přímo při běžné komunikaci čipové karty s čtečkou, bez potřeby úpravy čipové karty. Napěťově proudovou analýzu lze rozdělit do tří skupin, a sice na jednoduchou, diferenciální či diferenciální vyššího řádu.

3.2.1 Jednoduchá napěťově proudová analýza

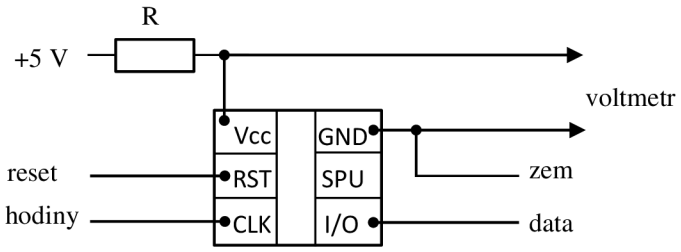
SPA (Simple power analysis) jednoduchá napěťově proudová analýza je technika zjišťování aktuální měřené spotřeby elektrické energie při vykonávání kryptografických operací v čase. Velikost odebírané energie je závislá na aktuálně prováděných instrukcích, viz obr. 3.2. Velikost proudu se měří pomocí rezistoru, který je zapojen do série s napájecím napětím, viz obr. 3.1. Okamžitá hodnota úbytku napětí na tomto rezistoru je podle Ohmova zákona lineární funkcí okamžité hodnoty proudu.

$$u(t) = R \times i(t) \tag{3.1}$$

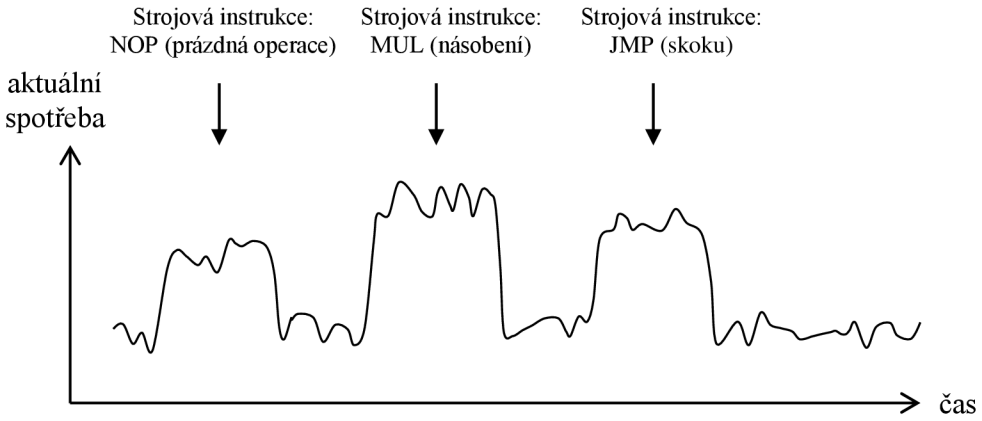
Vhodným A/D převodníkem získáme potřebný průběh proudu. Úbytky napětí na rezistoru vzorkuje převodník rychlostí jednotek až desítek megahertzů a ukládá je do paměti počítače. Naměřená data, která jsou vynesená do grafu, znázorňují spotřebu

proudu v závislosti na čase. Analýza dat následně dovolí odhalit tajné parametry, které se uplatnily při výpočtu. Následně jsou získané informace prováděné v daný okamžik, využity k odvození informací o provedených instrukcích, použitém klíči nebo zjištění Hammingovy váhy u klíče. Pomocí této informace dochází ke zjednodušení útoku hrubou silou. Napěťově proudovou analýzou se mohou rozpoznat větší části kryptografických algoritmů, které mají podobné vlastnosti, nebo se využijí při hledání rozdílů mezi použitými operacemi, jako jsou např. násobení a umocňování.

Analýzou blokových šifer lze výrazně narušit bezpečnost blokové šifry, protože se dají určit rozdíly při provádění bitového posunutí a permutací. Vychází se z pozorování jednotlivých operací, ve kterých se hledají očekávané operace, které se následně přiřadí odpovídajícím charakteristickým tvarům ze získaných informací. Pokud se jedná o zkušeného kryptoanalytika, není pro něj složité získat tajný klíč nebo jeho část rozpoznáním charakteristických průběhů, jelikož využije vztahů mezi prováděnou operací a dobou, než se dokončí daná operace.



Obr. 3.1: Jednoduché schéma zapojení měření spotřeby proudu čipové karty [25].



Obr. 3.2: Kolísání aktuální spotřeby při zpracování různých strojových instrukcí [25].

3.2.2 Diferenciální napěťově proudová analýza

DPA (Differential power analysis) diferenciální napěťově proudová analýza využívá statistických metod k odhalení tajného klíče a je ve většině praktických případů výkonnější, než jednoduchá napěťově proudová analýza. Tento typ útoku oproti předešlému SPA útoku můžeme automatizovat a odpadá tak nutnost expertní analýzy zkušeného kryptoanalytika. Je však nutné změřit velké množství napěťově proudových křivek, aby byly získány podklady pro statistiku a následně se mohl odfiltrovat šum. Útok postupuje tak, že se napřed získají data, která se později analyzují. Potom se využije statistických funkcí pro korekci chyb, čímž se získává přehled o tom, jaké operace se provádí uvnitř kryptografického systému. Data zpracovávaná

kryptografickým zařízením mají vliv na změnu výkonu zařízení. Těchto změn je možné využít k prolomení systému.

Při provádění útoku se musí napřed získat model spotřeby proudu u konkrétního kryptografického zařízení. Spotřeba energie u čipových karet je závislá mimo jiné i na přenášených datech přes sběrnici. Potom můžeme zvolit model spotřeby proudu, kde bude hodnota Hammingovy váhy přenášeného bajtu po sběrnici určovat hodnotu proudové spotřeby.

3.2.3 Diferenciální napěťově proudová analýza vyššího řádu

HO-DPA (High Oder DPA) je diferenciální napěťově proudová analýza vyššího řádu. Některé pokusy se snažily zabránit útokům pomocí DPA, ale vytvořily prostor pro HO-DPA. Pracuje na stejném základu jako DPA, ale při tom používá korelaci informace mezi několika kryptografickými operacemi.

3.3 Elektromagnetická analýza

Sofistikovanějšími útoky jsou elektromagnetické útoky EMA (Electromagnetic analysis), které využívají elektromagnetického pole vznikajícího kolem kryptografického zařízení. Byly publikovány v roce 2000 a i když jsou experimentálně složitější, mají několik výhod oproti ostatním útokům pomocí postranních kanálů. Přestože jsou více rušeny, měření má větší poměr signálu k šumu, než při napěťově proudové analýze. Takto získané informace jsou potom přesnější a dávají lepší diferenciální křivky. Díky tomu je snazší odhalit správný klíč, a to za současného využití menšího počtu vzorků.

Únik postranním kanálem je způsoben elektrickými vlastnostmi technologie používané při konstrukci čipové karty. Většina moderních čipů využívá technologie CMOS (Complementary Metal Oxide Semiconductor). CMOS invertor tvoří základ pro všechny digitální CMOS logiky [20]. Pokud mění stav z 0 na 1 nebo naopak, tak tato změna stavů generuje krátké proudové impulzy energie. Více obvodů měnících svůj stav vytvoří větší množství energie, která se následně uvolňuje. Tyto proudové impulzy způsobí změnu v oblasti EM kolem čipu, kterou lze měřit impulzní sondou. Změny proudů při činnosti kryptografického zařízení generují střídavé magnetické pole, které se dá zjistit, jestliže je dostatečně silné.

Analýzou naměřených elektromagnetických změn lze odhalit tajné parametry výpočtu. Změny zaznamenávají cívky umístěné kolem kryptografického zařízení. Cívky musí být umístěny v blízkosti nad čipem a měnit svoji pozici po malých krocích, dokud není získán nejsilnější signál. Elektromagnetické pole prochází prostorem, čímž se získá také prostorová informace, jež se dá využít při trojrozměrném přehledu, který zaznamenává změny elektromagnetického pole při výkonu kryptografických operacích u kryptografického zařízení. Měření může být analyzováno stejným způsobem jako při měření SPA nebo DPA, přičemž je nezbytné znát vnitřní strukturu polovodičových jednotek. Tyto metody jsou nazývány jednoduchou elektromagnetickou analýzou SEMA (Simple electromagnetic analysis) nebo diferenciální elektromagnetickou analýzou DEMA (Differential electromagnetic analysis). Výhodou je možné lokalizované měření, kterým lze snížit zašumění čipu. Nevýhodou této metody je její výrazně vyšší úroveň šumu ve srovnání s přímou elektrickou analýzou přes napájecí vedení. Kromě toho některé oblasti čipu, jako jsou např. sběrnice polovodičových zařízení, mohou být účinně chráněny proti tomuto druhu útoku stohováním více stop

navzájem. Elektromagnetické pole se měří pomocí citlivých detektorů a nelze jednoznačně určit, která ze stop je zdrojem signálu. Kovové štíty jsou obvykle umístěny přes aktivní strukturu čipu, aby výrazně snížily úroveň vyzařované energie, protože jejich tvary tvoří druh faradayovy klece, a proto není možné určit, kterou ze stop skutečně prochází příslušný proud. Pomocí EMA se dají narušit nebo obejít protiopatření chránící čipové karty před útoky DPA, mezi které patří např. štíty a náhodná logika.

3.4 Útok zaváděním chyb

Útoku zaváděním chyb (Fault induction attack) věnoval v posledním desetiletí průmysl čipových karet velkou pozornost. Útok zaváděním chyb využívá chyb při vykonávání výpočtu. Analýzou chyb se snaží zjistit důležité informace, které něco prozradí o systému. Chyby mohou být dočasné nebo trvalé. Některé druhy chyb kladou nároky na místo a čas výskytu. Chyba se musí objevit na určeném místě nebo nastat v požadovaný okamžik. Dočasná chyba zařízení nepoškozuje, pouze ho narušuje tak, aby prováděný výpočet neproběhl správně. Zařízení se ovlivňuje např. změnami frekvence a napětí. Stálá chyba poškodí zařízení natrvalo, proto už se zařízení nikdy nebude chovat tak, jak by mělo, ale bude ovlivněno vzniklou chybou napořád, např. je nastavena hodnota paměťové buňky na konstantní hodnotu.

Dále se chyby dělí na standardní a chyby úmyslně vytvořené. Úmyslné chyby mohou být vyvolány změnou napájecího napětí, změnou teploty, frekvence nebo ozářením. Tím se může ovlivnit instrukce podmíněného větvení tak, aby byla vybrána jiná větev než původní, která není správná. Potom se můžeme dostat do části paměti, která není za běžných podmínek přístupná, navíc pokud by byl v této části uložen tajný klíč, tak by k němu útočník získal přístup.

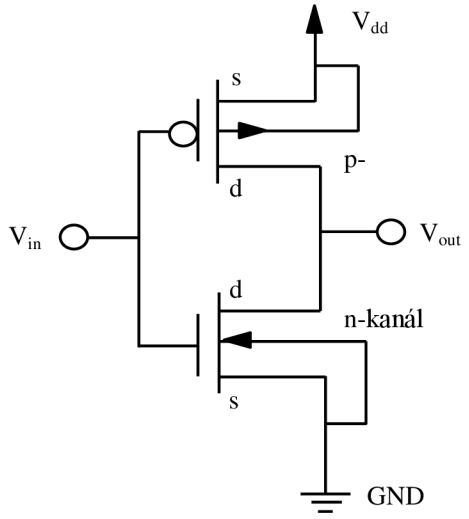
- Změna napětí – podle specifikace normy ISO/IEC 7816-3 musí čipová karta bezchybně pracovat v udávaném rozmezí ±10 % při zvolené třídě A (5V), B (3V) nebo C (1,8V). Pokud je zvýšena nebo snížena na hodnotu v rozmezí ±10 %, tak se při výpočtu může docílit chyb.
- Změna teploty – čipové karty mají definovaný rozsah pracovních teplot tak, aby pracovali bezchybně. Pokud se extrémně sníží nebo zvýší teplota, tak se opět může docílit chyb při výpočtu.
- Změna taktovací frekvence – frekvence je opět specifikována normou a ta udává i povolené tolerance. Pokud se zvýší nebo sníží a nesplňuje předepsanou toleranci, může se opět docílit chyb, při vykonávání výpočtu.
- Změna zářením – využívá se mikrovlnného ozařování při správně nasměrovaném záření, potom je ovlivněn prováděný výkon výpočtu a vznikají při něm chyby. EEPROM a flash paměťové buňky mohou být vymazány UV zářením, což způsobí, že jejich obsah se může změnit na nejnižší energetický stav. Při změně jednotlivých paměťových buněk se využívá úzkého laserového paprsku nebo přímo zaměřeného UV světla. Silný laser dokáže změnit i ROM.
- Změna osvětlením – využívá se intenzivního zdroje světla. Potom je možné měnit jednotlivé bity v paměti RAM nebo ovlivňovat instrukce. Při dopadu světla začnou tranzistory vést proud, a pokud je nad RAM pamětí umístěn mikroskop a nad mikroskopem fotoaparát s bleskem, tak se dá velmi přesně ozářit potřebná oblast. Opět je vyvolána chyba, které se dále využije.

4 Měření napájecích charakteristik čipové karty

Měření je soubor experimentálních úkonů, které slouží ke zjištění hodnoty veličiny za využití speciálních měřících prostředků. Měřící prostředky jsou všechna důležitá zařízení, která jsou potřebná pro uskutečnění měření. Měřicí přístroj je prostředek, který dokáže převést měřenou veličinu na údaj poskytující informaci o velikosti měřené veličiny. Elektrický proud má svoji kvantitativní stránku, která je vyjádřena hodnotou v ampérech, která se zjišťuje měřením. Hodnota odpovídá číslu, jež vyjadřuje velikost měřené veličiny ve zvolených jednotkách. Měření může být charakterizováno jako postup získávání informací o měřené veličině. Kapitola se dále zabývá vznikem napěťově proudového postranního kanálu a možným měřením. Popisuje nejvhodnější způsob měření a vede diskuzi o dalších možných variantách.

4.1 Vznik napěťově proudového postranního kanálu

Fyzikální podstata vzniku napěťově proudového postranního kanálu závisí na změně proudové spotřeby. U čipových karet se měření zaměřuje na napájení mikroprocesoru karty, který je sestaven z velkého množství tranzistorů, kde vznikají změny proudové spotřeby. V dnešní době jsou procesory karet převážně postaveny na technologii CMOS, která umožňuje vyšší hustotu prvků na čipu.



Obr. 4.1: CMOS invertor [20].

Základním využívaným prvkem je invertor, který obsahuje tranzistory T1 a T2, které se řídí napětím s opačným typem vodivosti. Tranzistory podle logické úrovně vstupního napětí mohou nabývat dvou stavů logické úrovně 0 nebo logické úrovně 1. Dynamická spotřeba se vytváří při přechodu mezi stavy 0 a 1 nebo naopak, protože vzniká výkonová špička. Proudová špička je závislá na počtu překlopení tranzistorů do jiného stavu. To vysvětluje, kdy dochází k úniku informací a proč se výkonová křivka koreluje s přechody Hammingovy vzdálenosti [20].

Proudová spotřeba elektronických obvodů se přímo odvíjí od operací, které jsou prováděny. Čím více je procesor zatěžován operacemi, které musí vykonat, tím více tranzistorů mění svůj stav. Od toho se odvíjí jeho výkonová spotřeba, která není konstantní s časem, protože při menším zatížení procesoru nastane méně překlopení tranzistorů, čímž dochází i k menší výkonové spotřebě [20].

4.2 Měření napěťově proudového postranního kanálu

Napěťově proudová analýza sleduje proudovou spotřebu elektrického zařízení. Měření spotřeby proudu je prováděno za předpokladu, že je mikroprocesor napájen ideálním zdrojem, který dodává konstantní napětí, potom je výkonová spotřeba přímo úměrná proudové spotřebě podle vztahu:

$$p(t) = U \times i(t) \tag{4.1}$$

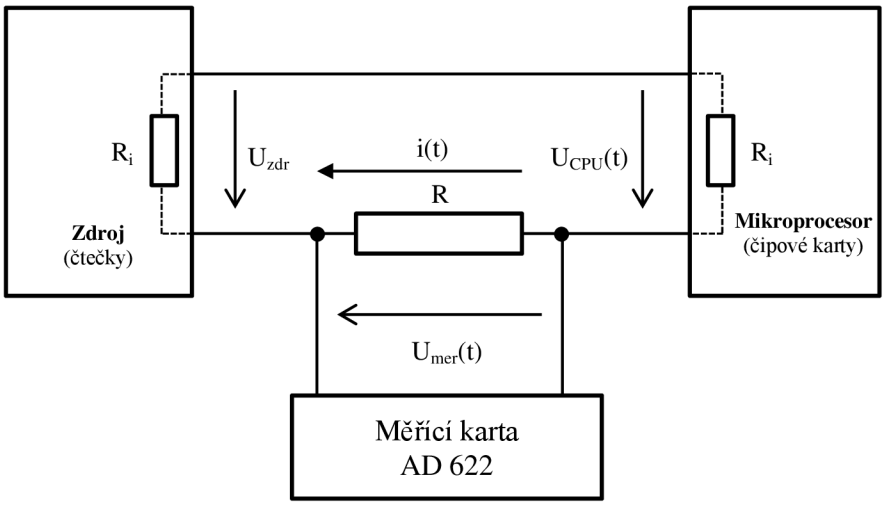
kde *p(t)* označuje elektrický příkon v čase t, *U* označuje elektrické napětí zdroje a *i(t)* označuje elektrický proud, který odebírá mikroprocesor v čase t. Napětí zdroje zůstává konstantní, mění se elektrický proud *i(t)*. K převodu měřených proudů různých velikostí na hodnoty vhodné k měření se obvykle používají bočníky, rezistory vložené do obvodu měřeného proudu, které převedou měřený proud na úbytek napětí odpovídající velikosti [2]. Úbytky na odporovém bočníku jsou malé řádově mV.

4.2.1 Odporový bočník

Při měření byl využit odporový bočník, jelikož je frekvenčně nezávislý a využívá malého rezistoru, který je vložen sériově mezi zdroj napájení a čipovou kartu. Velikostí rezistoru lze ovlivnit měřené elektrické napětí $U_{mer}(t)$, tak aby odpovídalo odebíranému elektrickému proudu *i(t)*. Na bočníku je okamžitá hodnota proměnného elektrického proudu *i(t)* převáděna na okamžitou hodnotu proměnného elektrického napětí *u(t)* dle Ohmova zákona:

$$u(t) = R \times i(t) \tag{4.2}$$

kde *R* označuje elektrický odpor bočníku a *i(t)* označuje elektrický proud v čase t. Zapojení odporového bočníku je znázorněno na obr. 4.2.



Obr. 4.2: Odporový převodník proudu na napětí s operačním zesilovačem [24].

Okamžitá hodnota získaného elektrického napětí *u(t)* je přivedena na vstup A/D převodníku, který dokáže získávat vzorky v konstantním čase. Vzorky se dále zaznamenají a zpracují. Při měření bylo využito měřící karty AD 622. Pro správnost

měření je důležitá volba bočníku. Jeho volbu je možné určit výpočtem nebo zvolit experimentálně. Výhodou odporového bočníku je jeho dobrá přesnost a cenová nenáročnost. Z důvodu relativně velkého indukčního odporu drátově vinutého rezistoru, by měl být použit metalizovaný rezistor.

4.2.2 Výpočet bočníku

Bočník se dá volit experimentálně. Při jeho odhadu lze užít vztah odvozený dle obr. 4.2. Kirhhoffův zákon říká:

$$U_{zdr} - U_{CPU} = U_{mer} \tag{4.3}$$

U_{CPU} je minimální napětí na mikroprocesoru pro zvolenou frekvenci hodinového signálu. U_{zdr} je napájecí napětí zdroje, které by nemělo překročit maximální napájecí napětí mikroprocesoru. Velikost odporu bočníku pro měření je odvozena ze vztahu 4.4.

$$R = \frac{U_{mer}}{i(t)} \tag{4.4}$$

kde U_{mer} je napětí vypočítané ze vztahu 4.3 a $i(t)$ je střední hodnota proudu odebíraného mikroprocesorem. Hodnotu většinou uvádí výrobce a je vztažená k určité frekvenci hodin a napájecího napětí.

4.3 Další možnosti měření

4.3.1 Proudová sonda

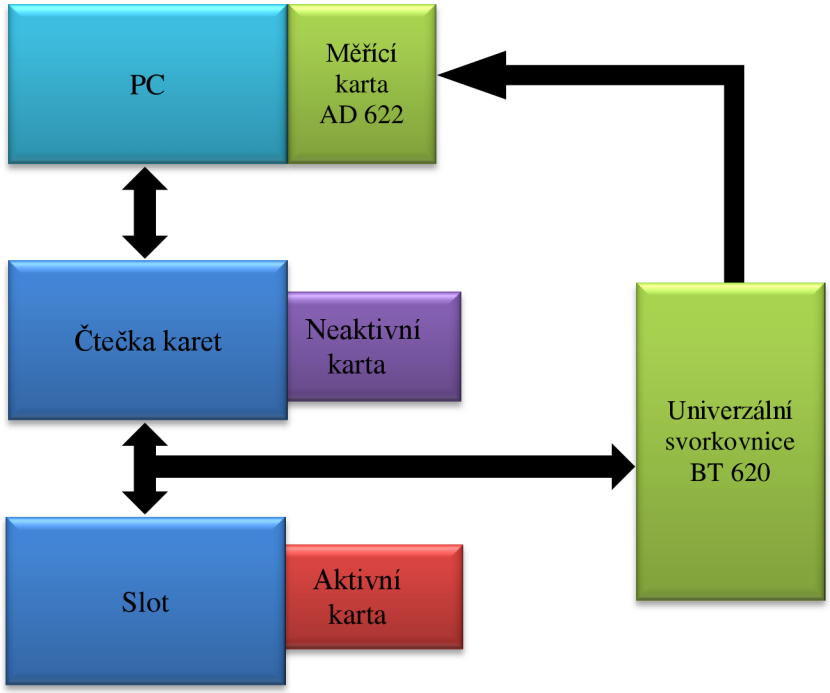
Proudová sonda, někdy také označována jako proudové kleště, slouží k měření proudu, který protéká vodičem tak, že není nutné vodič přerušit. Proudová sonda je konstruována, aby byla schopná obepnout měřený vodič, jehož proud potřebujeme změřit. Vodič potom představuje primární vinutí transformátoru sondy, sekundární vinutí je vlastní proudová sonda a má tvar toroidního transformátoru, který má tvar kleští. Při měření jsou kleště obepnuty kolem měřeného kabelu. Princip spočívá v převodu protékajícího proudu vodičem na napětí na výstupu sekundárního vinutí sondy, které se následně měří. Proudová sonda není pro potřebné měření vhodná, protože její citlivost zachycení potřebných změn proudu je nedostačující. Citlivost použitých Hallových sod bývá řádově v desetinách až stovkách V/A.

4.3.2 Převodník I→U

Pro měření proudů menších než 10^{-5} A, lze použít různé typy měřících zesilovačů. Jednou z možností je použití převodníku proudu na napětí, který umožnuje měření malých proudů bez úbytku napětí. Nevýhodou je, že se musí použít bočník poměrně s vysokým odporem, má tedy vysoký vstupní odpor a může proto sloužit jen k měření proudu poskytovaného zdrojem s řádově vyšším vnitřním odporem. Převodníky proudu na napětí s operačním zesilovačem, mají nízký vstupní odpor [2]. Nevýhodou je frekvenční závislost operačního zesilovače, proto tahle varianta měření není také vhodná. Operační zesilovač by musel mít nejméně dvakrát větší šířku přenášeného pásma, než je frekvence hodinových impulzů mikroprocesoru čipové karty.

5. Použité laboratorní pracoviště

Kapitola se věnuje popisu použitého laboratorního pracoviště, kterého bylo využito při měření napájecích charakteristik čipové karty, monitorování komunikace karty a čtečky. Návrhu způsobu odposlechu a analýzy získaných informací. Popisu softwaru a hardwaru, který byl použit při měření. Nastiňuje jejich výhody a možnosti. Blokové schéma laboratorního pracoviště je znázorněno na obr. 5.1.



Obr. 5.1: Blokové schéma zapojení laboratorního pracoviště.

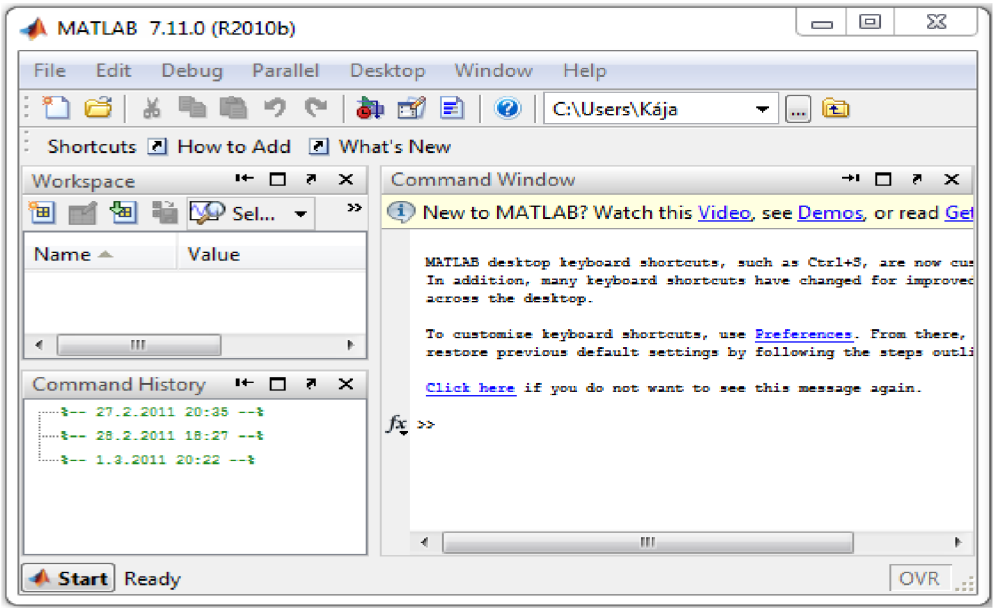
5. 1 Použitý software

Matlab je dnes jedním z nejrozšířenějších programových balíků pro technické výpočty v mnoha oborech [18]. Uplatnění nachází v celém světě, využívají ho univerzity, výzkumná pracoviště i firmy. Simulink je nadstavba Matlabu pro simulaci a modelování dynamických systémů, který využívá algoritmy Matlabu pro numerické řešení nelineárních diferenciálních rovnic. Dokáže poskytnout uživateli možnost rychle a snadno vytvářet modely dynamických soustav ve formě blokových schémat a rovnic. [12]. Při práci byl dále použit Real Time Toolbox, který umožnuje v prostředí programů Matlab/Simulink práci s externími analogovými a digitálními signály. Při analýze dat byl použit Simulink. Pro komunikaci s analyzovanou čipovou kartou je použit volně dostupný software JSmart Card Explorer.

5.1.1 Matlab

Matlab (MATrix LABoratory) odpovídá maticové laboratoři, která používá interaktivní prostředí, které je velice výkonné. Matlab dokázal spojit do jediného prostředí programovací jazyk, výpočty a vizualizaci. Umožnuje využití velkého množství rozšiřujících modulů, uplatnění nachází zejména ve výzkumu, vývoji a školní výuce.

Matlab je vyvíjen firmou MathWorks a je distribuován s širokým spektrem dalších rozšíření a toolboxů [18]. Obsahuje mnoho vestavěných funkcí, které jsou určeny se záměrem zlehčit prováděný vývoj, proto je jeho prostředí mnohem jednodušší než u jiných programovacích jazyků nebo vývojových prostředí. Typické okno Mtlabu je znázorněno na obr. 5.2.

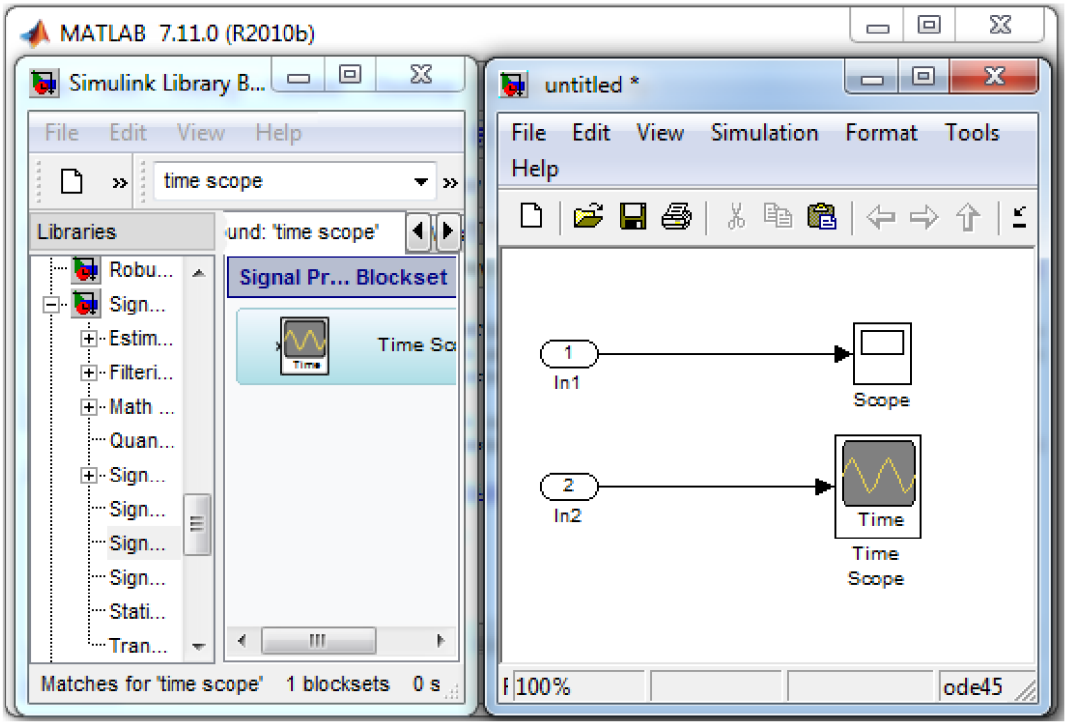


Obr. 5.2: Typické okno Matlabu.

Matlab si získal širokou komunitu z celého světa svými přednostmi a vlastnostmi. Je otevřeným a rozšiřitelným vysokoúrovňovým jazykem pro technické výpočty. Podporuje velké množství knihoven, vícerozměrná pole, datové struktury, interaktivní nástroje pro tvorbu grafického uživatelského rozhraní, import a export dat do mnoha formátů, komunikaci s externími měřícími a monitorovacími přístroji v reálném čase. Může být rozšiřován moduly pomocí jazyka C, C++, Fortran, Java [17].
Matlab lze používat na nejznámějších platformách a operačních systémech, např. Windows, Linux, Unix, MacOS. Matlab se dá rozšiřovat moduly, které jsou pojmenovány toolbooxy, největším je Simulink. Pracovní prostředí je složeno z několika částí. Příkazové okno (Commad Window) se používá pro komunikaci s výpočetním jádrem Matlabu. Nejčastěji bývá umístěno v pravé části programu a slouží při zapisování příkazů, výpisu chyb a varování. V levé části je nejčastěji pracovní prostředí (Workspace), zde se zobrazují již použité proměnné a historie příkazů (Command History), slouží pro ukládání všech příkazů zapsaných do příkazového okna.

5.1.2 Simulink

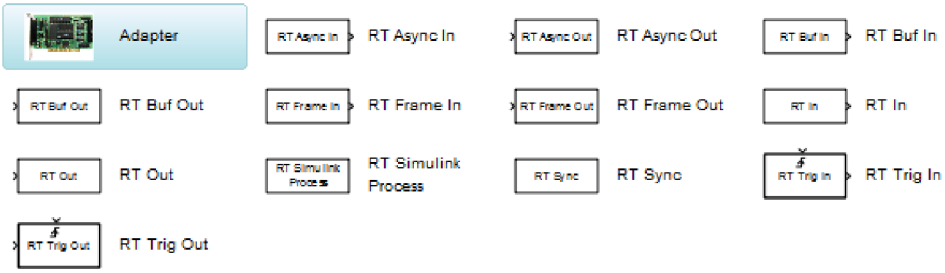
Simulink vznikl z anglických slov simulace a spojení (SIMUlation and LINK). Je nejznámějším a nejpoužívanějším rozšířením Matlabu. Má přehledné grafické rozhraní pro uživatele a je přizpůsoben k modelování, simulaci a analýze. Typické okno Simulinku je znázorněno na obr. 5.3. Práce v Simulinku je velice intuitivní. Poskytuje mnoho předdefinovaných bloků k analýze systémů.



Obr. 5.3: Typické okno Simulinku.

Simulink je spustitelný přes ikonu, která je umístěna na nástrojové liště nebo zadáním příkazu v Matlabu. Do příkazového okna se zapíše simulink. Simulink obsahuje okno s knihovnou dostupných bloků (Simulink Library Browser), které je přehledně děleno do podoblastí podle zařízení, kterých je velké množství. Dále jsou popsány použité bloky. Všechny popisy bloků se nachází také v nápovědě Simulink help.

Real Time Toolbox umožnuje v prostředí programů Matlab/Simulink práci s externími analogovými a digitálními signály. Jeho základ je výkonné jádro reálného času. Nejnovější je verze Real Time ToolBox 4.0.1, která přináší mnoho nových funkcí a vylepšení. Podporuje velké množství měřících karet a dalších zařízení od předních světových výrobců jako jsou Advantech, Axiom, Humusoft, National Instruments a mnoha dalších. Následně Simulink dovoluje experimentování s návrhy řídicích systémů, zpracováním signálu, získáváním dat a řešit další podobné úkoly. Uživatel nemusí mít skoro žádné znalosti z oblasti programování daného hardwaru. Knihovna bloků dovoluje práci v reálném čase bez nutnosti použití dalších nástrojů [13]. Simulace v reálném čase je jednou z nejnáročnějších úloh, ale Real Time ToolBox dokáže tuhle práci velice zjednodušit, stačí v Simulinku pouze přidávat potřebné bloky z jeho knihovny. Knihovny jsou zachyceny na obr. 5.4.

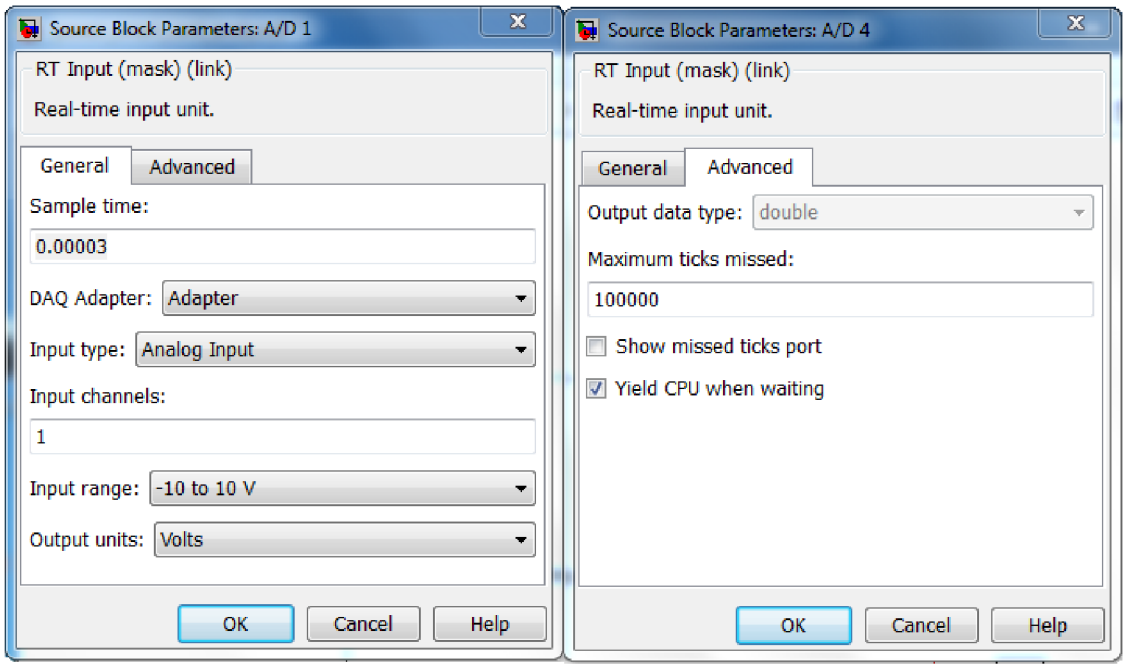


Obr. 5.4: Knihovna bloků Real Time Toolboxu.

- **Adapter** je základním prvkem pro komunikaci s měřící kartou, slouží k načtení hardwarových ovladačů měřící karty a jejich nastavení.
- **RT Async In** je určen pro aplikace, ve kterých není vstup řízen časovačem, ale vnitřním generátorem hodinového signálu Simulinku.
- **RT Async Out** je určen pro aplikace, ve kterých není vstup řízen časovačem, ale vnitřním generátorem hodinového signálu Simulinku.
- **RT Buf In** je určen k získávání a zpracování signálů v aplikacích, kde musí být všechna data zachycena ve vzorkovacích pulsech. Data zle uložit do paměti a zpracována později.
- **RT Buf Out** je určen pro systémy generující signál, kde mohou být data předem zpracována výpočtem, uložena do paměti a následně poslána na výstup zařízení.
- **TR Frame In** je využíván při získávání a zpracování signálů, kde musí být všechny data zachyceny ve vzorcích. Data lze uložit do vyrovnávací paměti a zpracovat později.
- **RT Frame Out** je využit u systémů generující signál, kde lze data předem vypočítat a uložit do paměti, následně poslat na výstup zařízení.
- **RT In** slouží pro získávání dat v aplikacích, kde musí být data zpracována okamžitě po jejich získání. U tohoto bloku lze nastavit počet ztracených vzorků, po kterém se objeví chybové hlášení.
- **RT Out** se používá pro systémy generující signál, kde musí být data poslána na výstup bez jakéhokoliv zpoždění, způsobeného ukládáním dat do paměti.
- **RT Simulink Process** umožňuje specifikovat prioritu procesu pro Simulink proces, který běží v real-time. Vyšší priorita znamená lepší real-time výkon, ale snižuje prioritu ostatní běžících úloh.
- **RT Sync** je určen pro synchronizaci signálu v reálném čase bez vykonání jakékoliv operace na vstupu či výstupu.
- **RT Trig In** je určen pro aplikace, které nemají vstup řízený časovačem, ale spínacím vstupem. Vstupní operace se vykoná při náběžné hraně spínacího signálu, takže není potřeba definovat vzorkovací periodu.
- **RT Trig Out** má podobné vlastnosti jako RT-Trig-In s tím rozdílem, že spínacím signálem je řízen výstup.

Měřící karta je zastoupena blokem Adaptér, který dovoluje měnit konfiguraci karty. Vstupy a výstupy jsou zastoupeny bloky vstupů a výstupů, přičemž u každého vstupního nebo výstupního bloku je možné nastavit různé vzorkovací periody. To umožní provádění „multi-rate“ simulací a řídících smyček. Pro získání co nejlepšího výkonu modelu je možná změna priority procesu reálného času pracujícího v rámci operačního systému pomocí bloku RT Simulink Process.
Práce s hardwarem je snadná. Velmi důležité je správně nastavit měřící kartu. Je to náročná operace, kterou dokáže Real Time ToolBox usnadnit. Stačí jen pomocí grafického rozhraní nastavit parametry karty, nebo kartu nenastavovat a nechat ji v továrním nastavení. Grafické rozhraní poskytuje snadné nastavování vstupů a výstupů, použitých kanálů, rozsahů a dalších parametrů viz obr. 5.5.

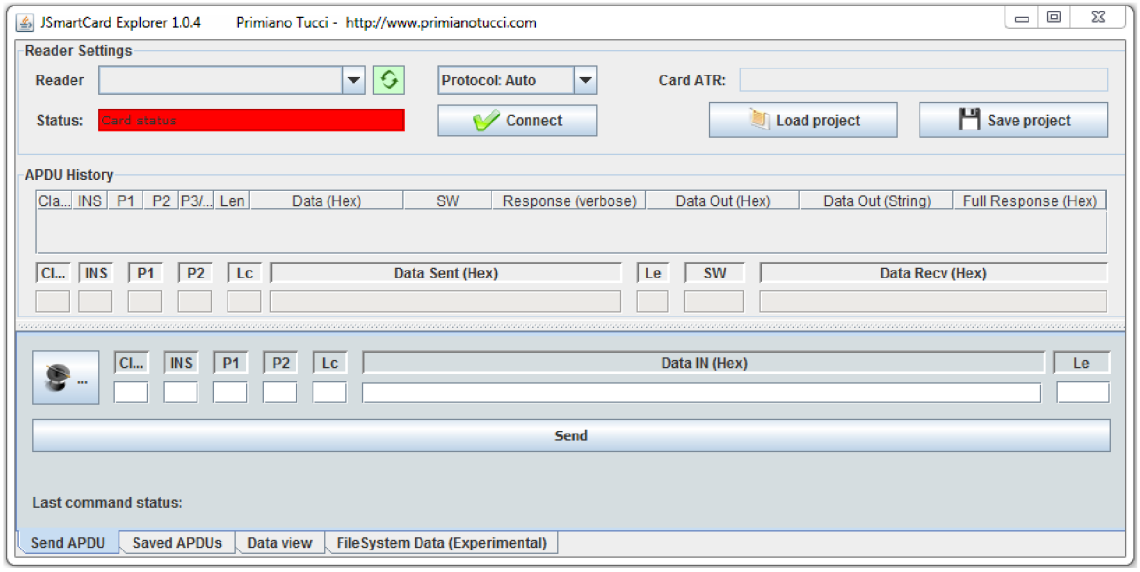
Proměnná *Sample time* určuje nastavení periody vzorkování karty v sekundách. Proměnná *Maximum ticks lost* udává počet povolených ztracených vzorků v důsledku zaneprázdnění počítače jinou činností, než dojde k chybě a zastavení programu. V takovém případě je nutné zvětšit parametr *Sample time*. Parametr *HW adapter* obsahuje název bloku *Adapter*, kterému přísluší. Je-li v počítači více měřících karet, je možno používat je současně tak, že každá karta má svůj blok *Adapter*. Parametr *Input channels* udává číslo kanálu nebo čísla kanálů.



Obr. 5.5: Nastavení bloku RT In.

5.1.3 JSmart Card Explorer

JSmart Card Explorer je program, který je volně dostupný. Vyžaduje Sun Java 1.6 +. Dokáže komunikovat s čipovou kartou pomocí APDU příkazů. Provádí potřebné výpočty a převody automaticky místo uživatele [10]. Program umožnuje výběr čtečky karet a transportní protokol T=0 nebo T=1. Práci ulehčuje předdefinovanými příkazy, které je možno libovolně upravovat, převodem dat z desítkové soustavy do šestnáctkové soustavy, automatickým výpočtem délky dat parametru P3. Zobrazuje historii použitých příkazů a ATR karty. Umožňuje uložení a opětovné načtení projektu. Typické okno programu JSmart Card Explorer je znázorněno na obr. 5.6.



Obr. 5.6: Typické okno JSmart Card Exploreru.

5.1.4 JCS Suite v 3.0

JCS Suite v 3.0 je spolu s kartami Sm@rtCafé neodmyslitelnou součástí sortimentu G&D (Giesecke & Devrient). Nabízí vynikající funkce pro podporu vývojářů. Podporuje vývoj ladění a testování java apletů pro Sm@rtCafé karty a další různé druhy java karet. Je vhodný pro vývojáře java card a je založen na Eclipse. Dokáže simulovat karty Sm@rtCafé Expert 2.1, 3.1, 3.2, 4.0 a 5.0 pomocí CardVirtual Machine. Obsahuje jednoduchý generátor APDU příkazů, který dokáže i záznam maker. Program byl využit při získávání potřebných informací o použité kartě, především pro získání parametrů karty a použitelných příkazů APDU.

5.2 Použitý hardware

Při měření byla použita pracovní stanice, kde bylo použito již zmíněného softwarového vybavení. Pracovní stanice používala procesor Intel(R) Core(TM)2 Duo CPU E8400, 3.00GHz, operační paměť DDR3 o velikosti 4096 MB, grafickou kartu Radeon HD 4850, 512 MB a operační systém Microsoft Windows 7 Professional 32 bit. Pracovní stanice byla rozšířena o zásuvnou kartu nainstalovanou do PCI (Peripheral Component Interconnect) slotu. Měřící karta AD 622 od firmy Humusoft byla použita při sběru dat. Pro komunikaci s čipovou kartou od výrobce G&D byla použita čtečka karet OMNIKEY CardMan 3121, která musela být pro potřeby měření modifikována.

5.2.1 Čipová karta

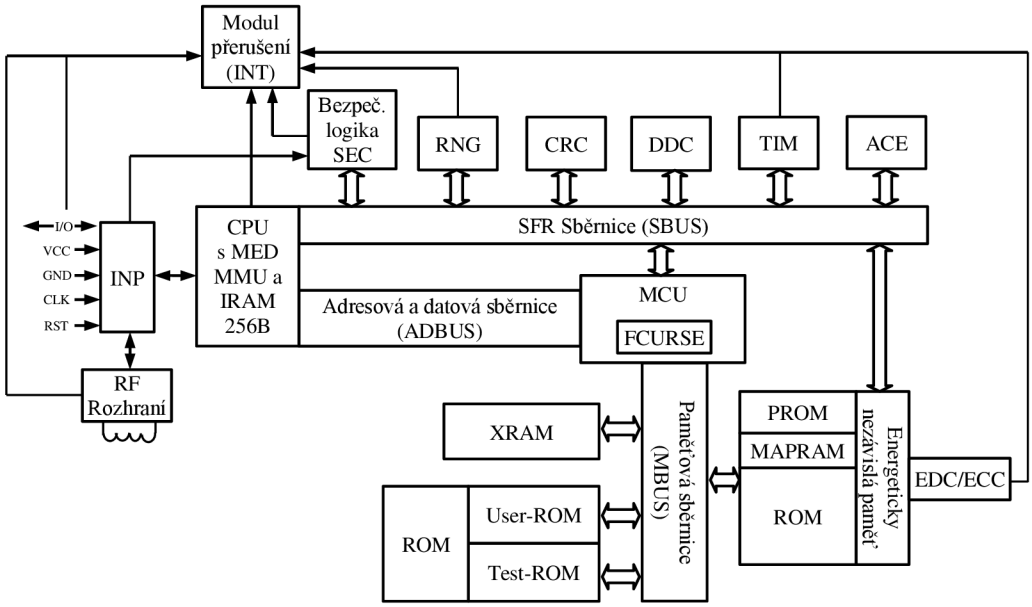
Při měření byla použita čipová karta typu Sm@rtCafe Expert 4.0 od firmy G&D. Zjištěné parametry a vlastnosti jsou uvedeny, viz tab. 5.1. Tahle verze obsahuje oproti předchozí navíc. Popis GET STATUS používaného v Security Domain s Delegated management pro získávání dat životního cyklu. Nový hardware SLE66CLX360PEM, SLE66CLX800PEN, který se odlišuje pouze v kapacitě paměti EEPROM. Nové čipy splňují nejvyšší požadavky z hlediska výkonu a bezpečnosti. Vyrábí je Infineon Technologies AG výrobním procesem 0,22 μm a technologií CMOS. Čipy jsou určeny k použití v čipových kartách, pro zvláště bezpečné aplikace. Vlastní protiopatření proti SPA, DPA, EMA a DFA útoky. Sm@rtCafé Expert je operační systém čipových karet založený na nejmodernějších kartách Java Card.

Tab. 5.1: Organizace paměti SLE66CLX360PEM [4].

SLE66CLX360PEM						
Vývojové označení	Číslo verze	Typ čipu	XRAM implementovaná [kByte]	XRAM dostupná [kByte]	ROM Modul implementovaná [kByte]	Celková ROM dostupná [kByte]
M1588	E12	B7	6	6	256	256
Test ROM dostupná IFX [kByte]	Uživatelská ROM dostupná [kByte]	EEPROM implementovaná [kByte]	EEPROM dostupná [kByte]	IRAM [Byte]	Map-RAM 1088x6 [Bits]	PROM [Bits]
20	236	80	36 + 1k Mifare	256	1280x6	128

Tab. 5.2: Organizace paměti SLE66CLX800PEM [4].

SLE66CLX800PEM						
Vývojové označení	Číslo verze	Typ čipu	XRAM implementovaná [kByte]	XRAM dostupná [kByte]	ROM Modul implementovaná [kByte]	Celková ROM dostupná [kByte]
M1580	E12	A2	6	6	256	256
Test ROM dostupná IFX [kByte]	Uživatelská ROM dostupná [kByte]	EEPROM implementovaná [kByte]	EEPROM dostupná [kByte]	IRAM [Byte]	Map-RAM 1088x6 [Bits]	PROM [Bits]
20	236	80	78 + 1k Mifare	256	1280x6	128



Obr. 5.7: Blokové schéma SLE66CLX [4].

Podporuje více aplikací a je v souladu s průmyslově přijatými specifikacemi OP (Open Platform). Odlišuje se od konvenčních čipových karet s pevnými a neflexibilními aplikacemi, Sm@rtCafé Expert umožnuje instalovat a aktivovat Java Card aplety bezpečně a dynamickým způsobem. Na rozdíl od konvenčních čipových karet, program a logické sekvence jsou definovány Java aplety karty, které si mohou sami vytvářet vývojáři. Mezi vlastnosti Sm@rtCafé Expert patří Java Card 2.2.1standard, GlobalPlatform 2.1.1, vzdálené volání metod, bezpečná správa paměti, paměťová defregmentace (EEPROM, COR), ROMed aplikace, vylepšený virtuální stroj bezpečnostního modelu, podpora výběru protokolu přenosu, více domén zabezpečení, ověřování vzorů DAP (Data Authentication Pattern), ověření pravosti (3DES nebo RSA), RSA šifrování/dešifrování až 2048 bitů, zajištěny důležité bezpečnostní metody DPA/SPA, hash algoritmy (SHA-1, SHA-256, MD5, RIPEMD-160), SEED 128 bitů, AES až do 256 bitů, MIFARE emulace, BIO API.

Tab. 5.3: Parametry a vlastnosti použité karty získané JCS Suite v 3.0.

ATR	3B F8 18 00 00 80 31 FE 45 00 73 C8 40 13 00 90 00 92
Podporované protokoly	T=0, T=1
Frekvence /MHz	5.0
Převodní koeficient taktovací frekvence (Fi)	372
Koeficient přenosové rychlosti (Di)	12
Typ karty	Convego Join 4.0 / Sm@rtCafe Expert 4.0
Free EEPROM	76681 Bajtů
Free COD RAM	3024 Bajtů
Free COR RAM	2728 Bajtů

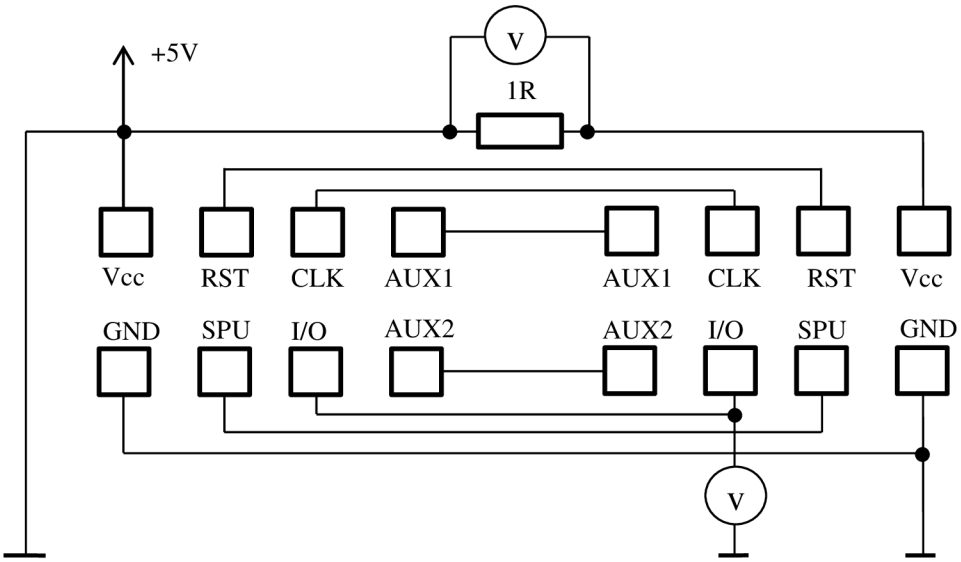
5.2.2 Čtečka karet

Čtečka karet OMNIKEY CardMan 3121 je vysoce výkonná USB čtečka čipových karet určená ke stolnímu použití viz obr. 5.8. Využívá rozhraní USB a je typu plug & play, přičemž podporuje přenosovou rychlost 420 kbps. Je kompatibilní se všemi průmyslovými standardy. Proto je čtečka prakticky schopna spolupracovat se všemi inteligentními kartami, operačními systémy a různými aplikacemi. Použití s aplikacemi je založeno na standardizovaných rozhraních jako PC/SC (Personal Computer/Smart Card), OCF (Open Card Framework) nebo CT-API (CardTerminal Application Programming Interface). Podporuje vysokorychlostní přenos dat. Splňuje požadavky standardu FIPS 201 [11].

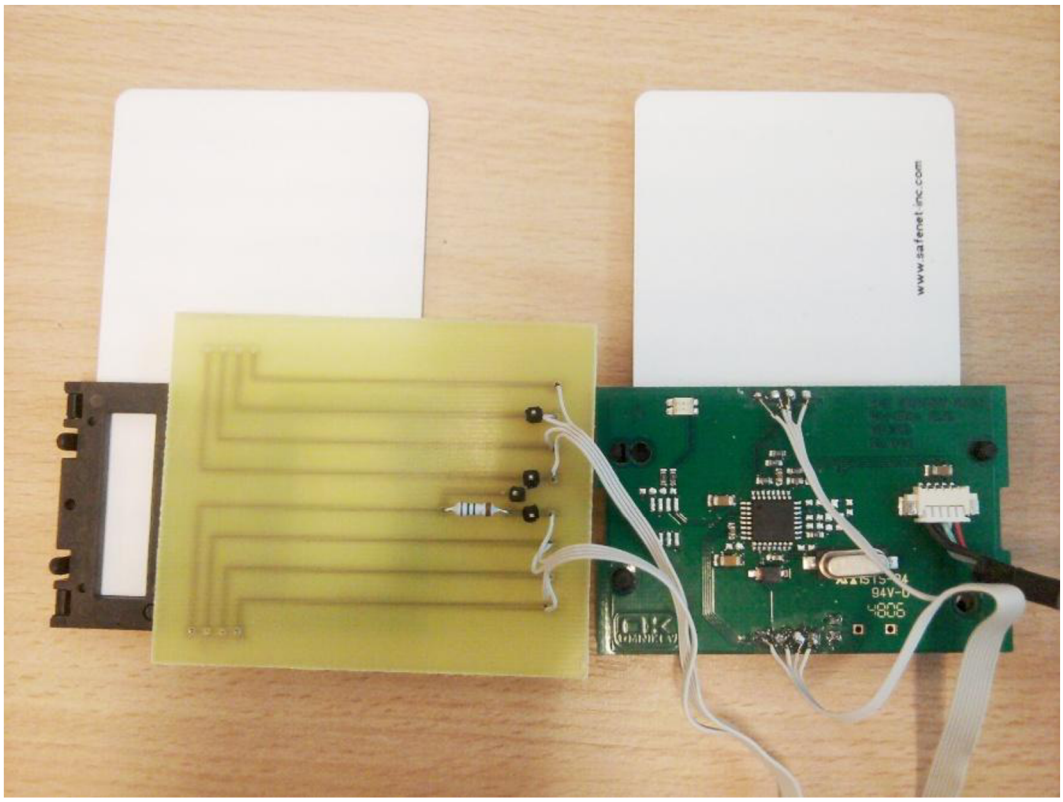
Obr. 5.8: Čtečka karet OMNIKEY 3121.

Měření nešlo uskutečnit na originální čtečce OMNIKEY, proto byla zvolena nejvhodnější metoda, která využívala odporového bočníku. Nastala nutnost modifikovat použitou čtečku. Čtečka byla zbavena ochranného obalu. To umožnilo přístup přímo k čtečce a dovolilo vložit odporový bočník, který je využit při měření proudové spotřeby (okamžitých změn napětí). Pro potřeby měření byla navržena a vytvořena deska plošného spoje s druhým slotem pro měřenou kartu, viz obr. 5.10. Kontakty slotů jsou propojeny s odpovídajícími kontakty na čtečce karet tak, aby byla zachována funkčnost. Mezi kontakt čtečky C1 (Vcc) a kontakt slotu C1 (Vcc) je vložen vybraný rezistor, který vytváří odporový bočník, viz obr. 5.9.

Velikost odporu byla zvolena $R = 1\ \Omega$, aby se projevil pouze minimální úbytek napětí a mohla být použita zjednodušená transformace U → I. Z důvodu relativně velkého indukčního odporu drátově vinutého rezistoru, byl použit metalizovaný rezistor s přesností ± 1%. Potom okamžité změny velikosti napětí odpovídají okamžitým velikostem proudové spotřeby čipové karty. Při měření na osciloskopu byl použit rezistor $R = 10\ \Omega$, proudová spotřeba je tedy desetkrát menší.



Obr. 5.9: Vložení bočníku mezi čtečku a čipovou kartu.



Obr. 5.10: Modifikovaná čtečka OMNIKEY pro potřeby měření.

5.2.3 Měřící karta

Při měření byla použita měřící karta AD 622 pro PC od firmy HUMUSOFT s.r.o. Tato karta je podporována Real Time ToolBoxem pro Matlab. Spolu s tímto programovým balíkem vytváří integrované a snadno použitelné prostředí pro vývoj aplikací pro řízení a simulování v reálném čase [14]. Karta AD 622 je určena ke sběru dat a řízení aplikací a je optimalizována pro Simulink. Instaluje se do volného PCI slotu počítače. Obsahuje osm 14-bitových analogových vstupů, osm 14-bitových analogových výstupů, osm digitálních vstupů a osm digitálních výstupů. Její výhodou je krátká doba převodu a nízká spotřeba. Nachází uplatnění při měření stejnosměrných napětí, připojení převodníků a snímačů, měření vibrací a přechodových jevů, řízení a monitorování procesů, snímání a analýze průběhů, vícekanálovém sběru dat a simulacích v reálném čase. Technické parametry karty viz tab. 5.3.

Tab. 5.4: Technické parametry AD 622 [15].

Analogové vstupy	
Kanály	8 single-ended
A/D převodník	14-bitový
Čas převodu	1,6 μs 1 kanál
	1,9 μs 2 kanály
	2,5 μs 4 kanály
	3,7 μs 8 kanálů
Vstupní rozsahy	± 10 V
Vstupní impedance	10^{10} Ω
Spouštění	programově, časovačem, externě
Analogové výstupy	
Kanály	8 kanálů, 14-bitů
Výstupní rozsah	± 10 V
Výstupní proud	max. 10 mA
Čas ustálení	31 μs
Digitální vstupy a výstupy	
Vstupní linky	8, s úrovněmi TTL
Výstupní linky	8, s úrovněmi TTL

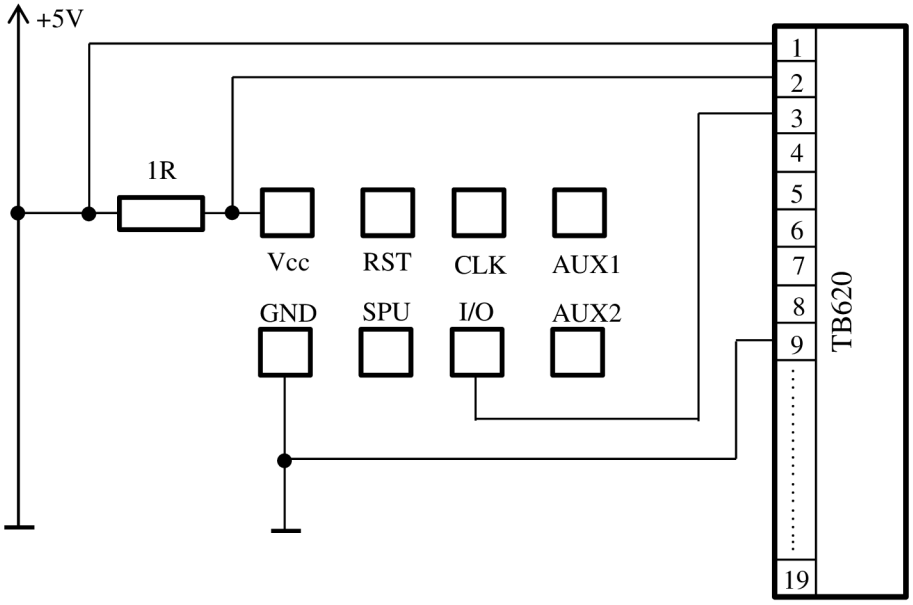
Tab. 5.5: Popis konektoru [16].

AD0-AD7	analogové vstupy
DA0-DA7	analogové výstupy
DIN0-DIN7	TTL kompatibilní digitální vstupy
DOUT0-DOUT7	TTL kompatibilní digitální výstupy
+12V	napájení +12V
-12V	napájení -12V
+5V	napájení +5V
AGND	analogová zem
GND	digitální zem

Tab. 5.6: Přiřazení jednotlivých pinů [16].

AD0	1	DA0	20
AD1	2	DA1	21
AD2	3	DA2	22
AD3	4	DA3	23
AD4	5	DA4	24
AD5	6	DA5	25
AD6	7	-12V	26
AD7	8	+12V	27
AGND	9	+5V	28
DA6	10	GND	29
DA7	11	DOUT0	30
DIN0	12	DOUT1	31
DIN1	13	DOUT2	32
DIN2	14	DOUT3	33
DIN3	15	DOUT4	34
DIN4	16	DOUT5	35
DIN5	17	DOUT6	36
DIN6	18	DOUT7	37
DIN7	19		

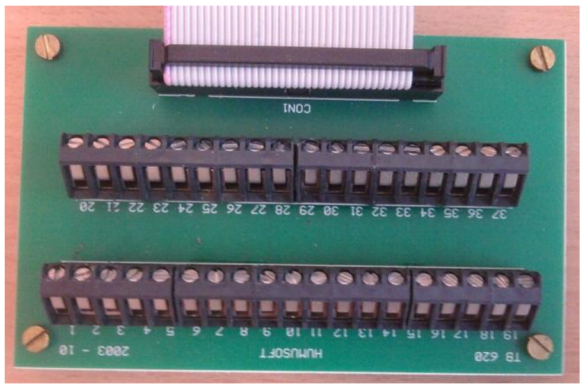
Pro potřeby měření byla karta zapojena následovně, viz obr. 5.11. Karta dokáže zaznamenat velmi malé změny napětí. Při měření bylo využito tří analogově/digitálních vstupů AD0 (1), AD1 (2), AD2 (3). Vstup analogové země AGND (9) je připojen na GND čtečky karet. Proudová spotřeba čipové karty je určena rozdílem napětí na použitých vstupech AD0 (1) a AD1 (2). Vstup AD1 (2) měří napájecí napětí čipové karty. Vstup AD2 (3) je určen pro měření napěťových změn na I/O portu. Údaje získané z kanálů AD1 (2), AD2 (3) jsou využívány při zpracování výsledků, napomáhají při rozpoznání počátku a konce komunikace čtečky a karty. Tyto hodnoty jsou nezbytné k zjištění potřebných informací o proudové spotřebě čipové karty.



Obr. 5.11: Propojení s univerzální svorkovnicí TB620.

5.2.4 Univerzální svorkovnice

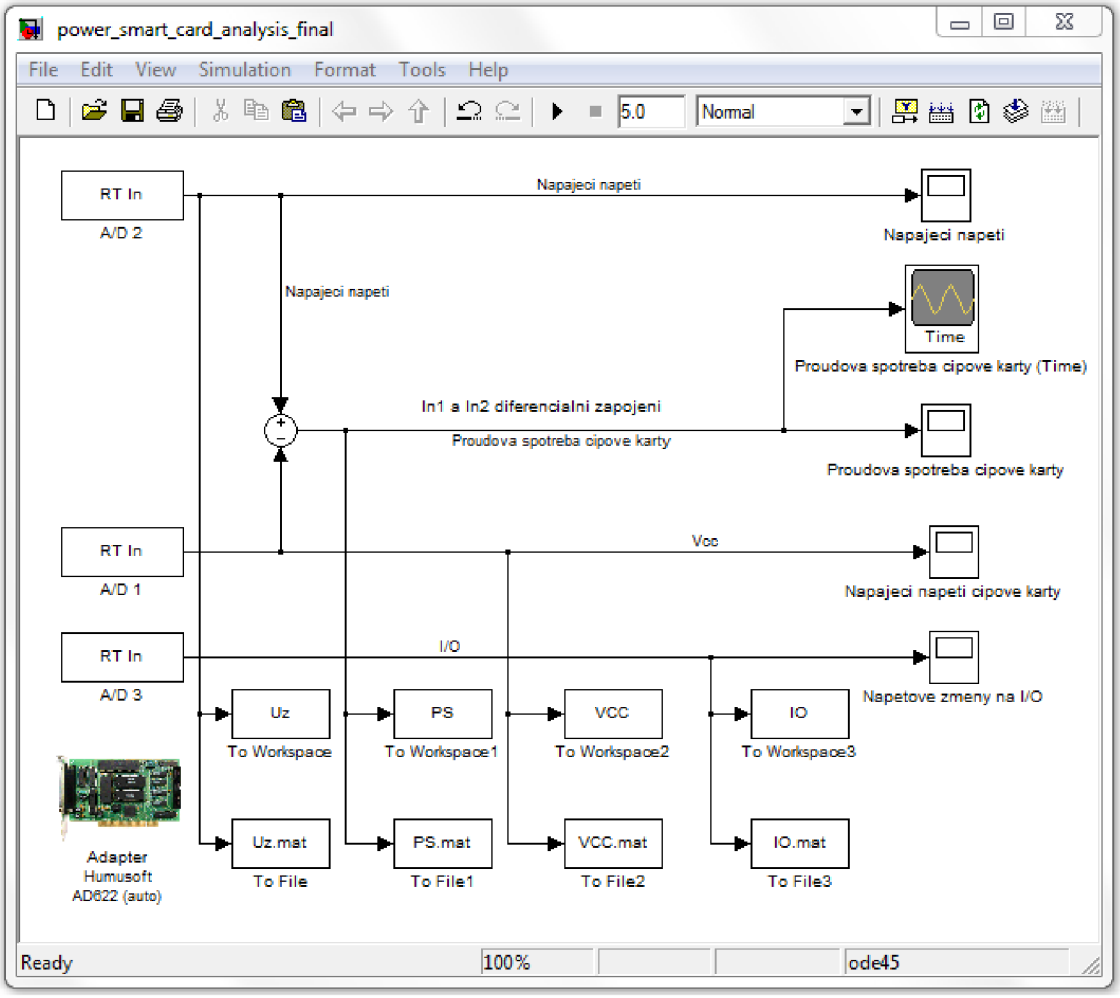
TB620 je pasivní element, který umožňuje snadné připojení externích signálů pomocí svorkovnice. TB620 je propojen 38 vodičovým kabelem s měřící kartou. Svorkovnice je zachycena na obr. 5.12. Slouží pro připojování měřených signálů k měřící kartě.



Obr. 5.12: Univerzální svorkovnice TB620.

6. Měření napájecích charakteristik během komunikace

Při měření napájecích charakteristik čipové karty byl použit software a hardware popsaný v předchozí kapitole. Navržený model power smart card analysis final, byl vytvořen v Simulinku je zachycen viz obr. 6.1. Model je použit při analýze napěťově proudového kanálu čipové karty. Využívá předefinované bloky a bloky z knihovny Real Time Toolboxu. Sestavený model je určen k měření a záznamu měřených dat.



Obr. 6.1: Použitý model pro analýzu napěťově proudového kanálu.

Blok Suma je využit pro získání rozdílů napětí měřeného na vstupu A/D 1 a A/D 2. Hodnoty jsou odečteny a předány na výstup bloku. Parametrem *List of sings* je určen počet a typ vstupních operací. Znaménko – znamená odečtení vstupu, znaménko + přičtení vstupu a znak | znamená mezeru mezi vstupy.

Měřící karta byla nastavena automaticky, pracovní stanice používá pouze jedinou měřící kartu. Při měření bylo využito tří A/D vstupů měřící karty. Vstupům (RT In) byly nastavovány různé vzorkovací časy, *Sample time* při prováděném měření. Karta by měla dle specifikací udávaných výrobcem zvládat vzorkovací čas 0.0000025 s využitím 4 A/D vstupů. Při použití této uvedené hodnoty pracovní stanice ihned zamrzala. Vhodné nastavení času vzorkování je důležité pro kvalitu a vypovídající hodnotu naměřených dat. Tímto krokem je ukončen proces potřebných nastavení a inicializací

potřebných před samotným měřením. V části *Simulation time byl* počátek simulace *Start time* ponechán na hodnotě nula a konec simulace *Stop time* nastven na požadovanou hodnotu, které následně odpovídá i délka simulace. Po spuštění simulace probíhá měření nastavených vstupů, které běží v nastavené smyčce, při tom dochází k záznamu měřených dat z použitých vstupů a rychlost odpovídá nastavenému vzorkovacímu času, dokud není smyčka u konce nebo není zastavena ručně za běhu simulace. Výsledky simulace jsou zobrazeny bloky osciloskopu. Osciloskopy zobrazují převážně nekompletní průběhy měřených veličin. Pro úpravu měřítka os je nutné použít funkci Autoscale a následně upravit měřítka os dle vlastních potřeb.

Měření v reálném čase bylo prováděno s hodnotou vzorkovacího času 0,0001, při jeho snížení se stanice začala chovat nekorektně. Měření s tímto nastavením viz obr. 6.3. Následně byl z modelu odstraněn Time osciloskop. Při měření nebyly osciloskopy v provozu, byly zobrazeny až po dokončení simulace. Byla provedena úprava priority procesu Simulinku (Matlabu) v nastavení priority z normální na vysoká, což je nejvyšší hodnota kterou lze nastavit. Bylo dosaženo funkčnosti při nastavení vzorkovacího času 0,00004. Uvedená hodnota je hraniční a pracovní stanice se nedokáže chovat po delší dobu korektně. Měření je zachyceno viz obr. 6.12, 6.13 a 6.14. Následně byl použitý model opět upraven, byl ponechán pouze jeden RT In vstup a jeden osciloskop pro měření I/O portu při komunikaci. Měření se podařilo pro čas vzorkování 0.00001. Měření je zachyceno viz obr. 6.12, 6.13 a 6.14. Další parametr, který ovlivňoval měření, byl *Maximum ticks missed*, jenž ovlivňuje maximální počet ztracených vzorů. V průběhu měření byl upravován na hodnoty tak, aby se stanice chovala korektně. Při nastavování nižšího vzorkovacího času musely být upraveny použité osciloskopy. Úprava byla provedena změnou parametru *Limit data points to last* na hodnotu 50000. Protože je čas simulace příliš dlouhý nebo krok výpočtu malý, byla by vykreslena pouze část průběhu a ostatní data by byla ztracena.

Výsledkem měření je zachycení a záznam měřených dat komunikace čtečky a karty při zaslání APDU příkazu. Naměřená data jsou zachycena třemi osciloskopy a jedním Time osciloskopem. První osciloskop zaznamenává proudovou spotřebu čipové karty. Druhý osciloskop zaznamenává napájecí napětí čipové karty. Třetí osciloskop zaznamenává napěťové změny na I/O portu. Time osciloskop zaznamenává také proudovou spotřebu čipové karty. Grafy lze následně vykreslit pomocí Matlabu příkazem plot z dat exportovaných ze Simulinku pomocí bloku To Workspace nebo použití souboru file.mat.

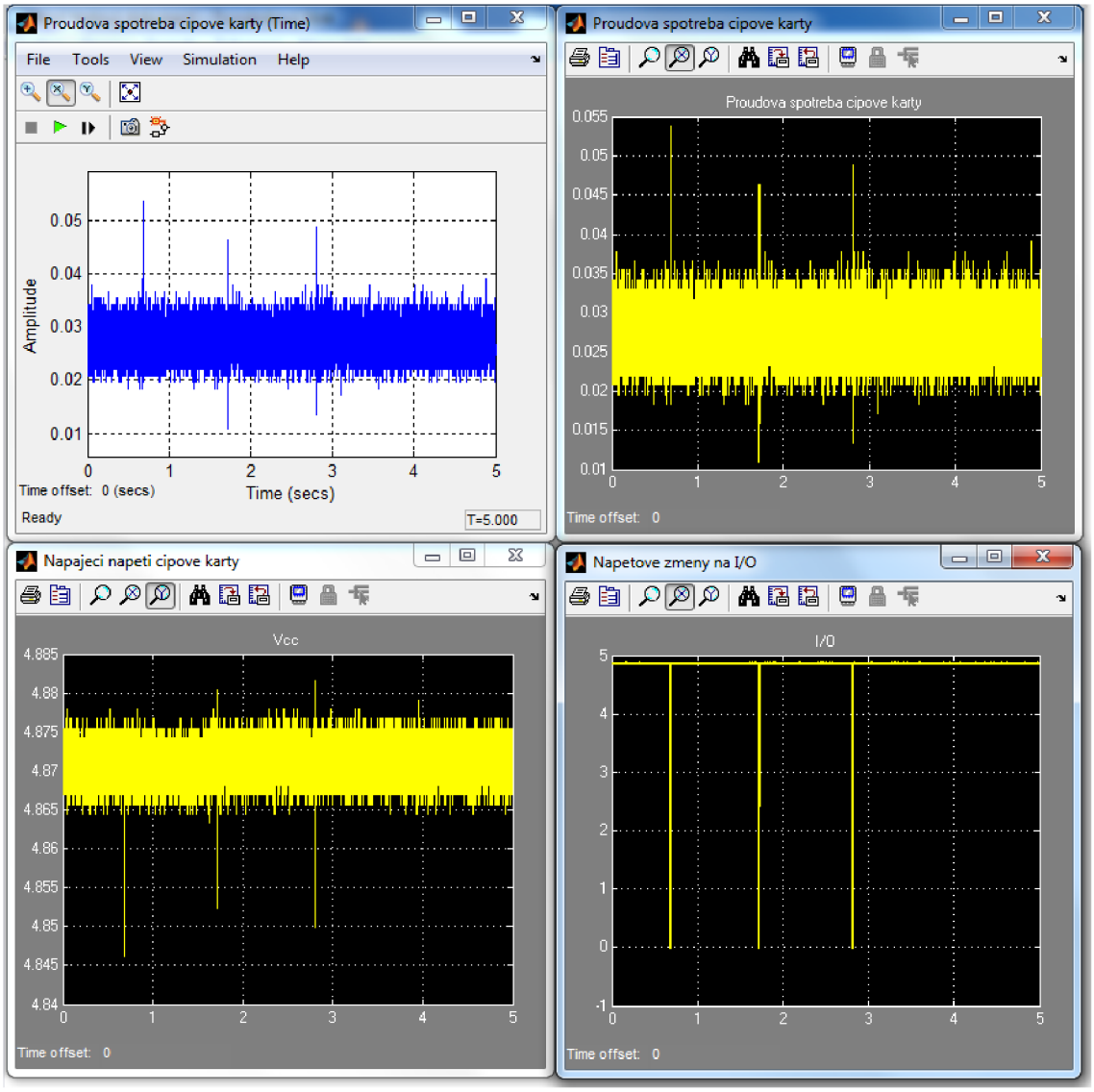
Měření je prováděno, když je programem JSmart Card Explorer zaslán APDU příkaz čtečce OMNIKEY a ta následně začne komunikovat s čipovou kartou. Karta obdrží zaslané informace, ty zpracuje a následně odpoví čtečce OMNIKEY, ta předá výsledek programu JSmart Card Explorer. Při měření byl zasílán např. APDU příkaz viz obr. 6.2. Jedná se o příkaz SELECT, který se používá k výběru appletu na logickém kanálu X. Hodnotou X=0 je vybrán první applet. Data obsahují AID (Application Identifier) vybíraného appletu.

CLA	INS	P1	P2	Lc	Data	Le
00_{16}	$A4_{16}$	04_{16}	00_{16}	08_{16}	A0 00 00 00 03 00 00 00_{16}	

Obr. 6.2: Měřený APDU příkaz.

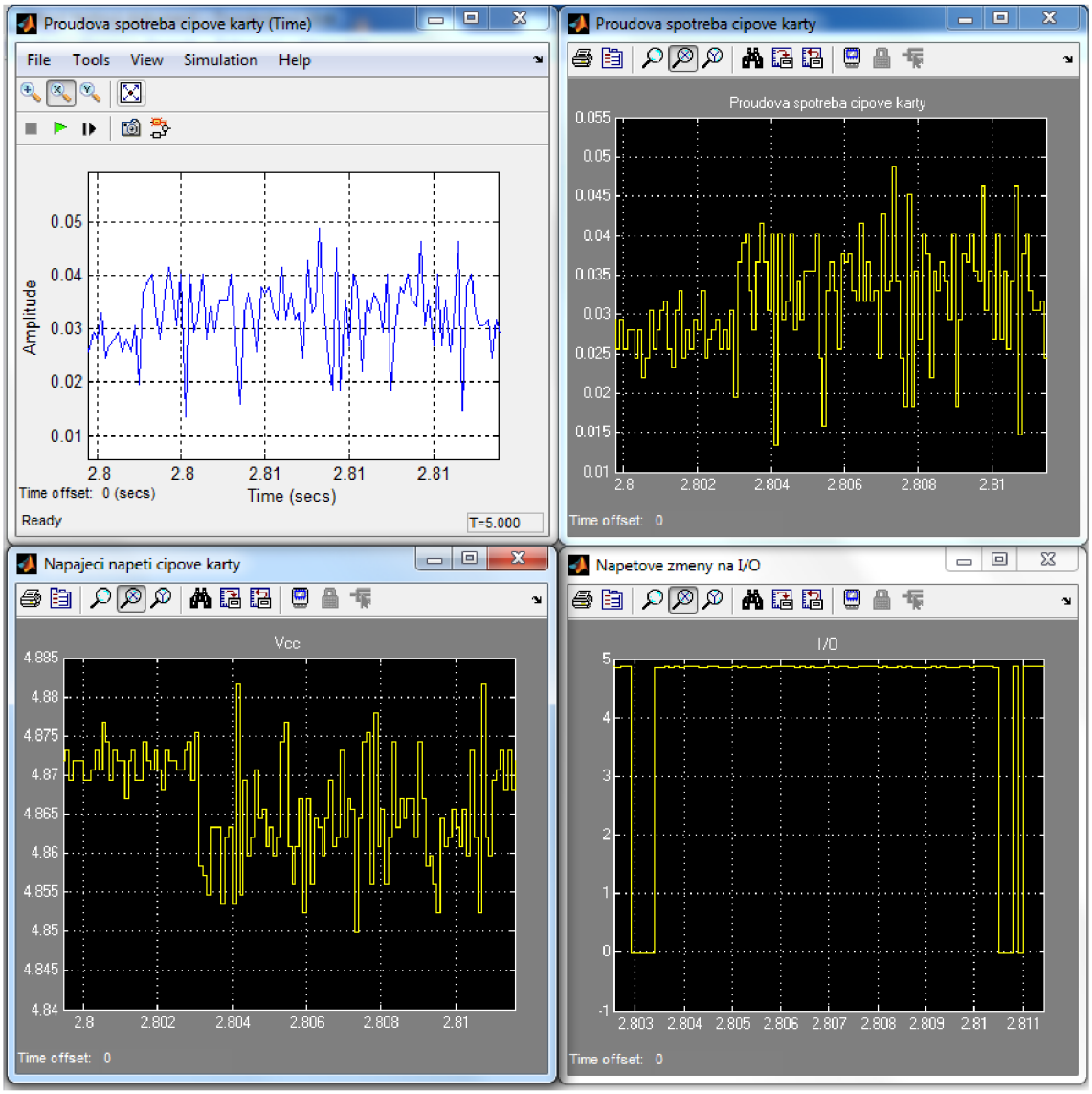
6.1 Monitorování komunikace měřící kartou AD622

Výsledky měření prováděného v reálném čase s hodnotou vzorkovacího času 0,0001 a použitými třemi A/D vstupy viz obr. 6.3. Doba simulace byla nastavena na 5 s. Za tuto dobu byly zaslány tři APDU příkazy. Jsou zachyceny na osciloskopu, který zaznamenává napěťové změny na I/O portu. V době zpracování dochází ke změnám spotřeby proudu a napětí. Změny jsou zachyceny na osciloskopu pro sledování proudové spotřeby čipové karty a na osciloskopu pro sledování napájecího napětí čipové karty. Time osciloskop je zaměřen na průběh proudové spotřeby čipové karty v čase zpracování APDU příkazu. Všechna měřená data jsou zaznamenána a uložena do souborů mat (soubor Matlabu pro ukládání dat). Tato uložená data lze následně zpětně zpracovat Matlabem a podrobit je dalšímu zkoumání a analýze.



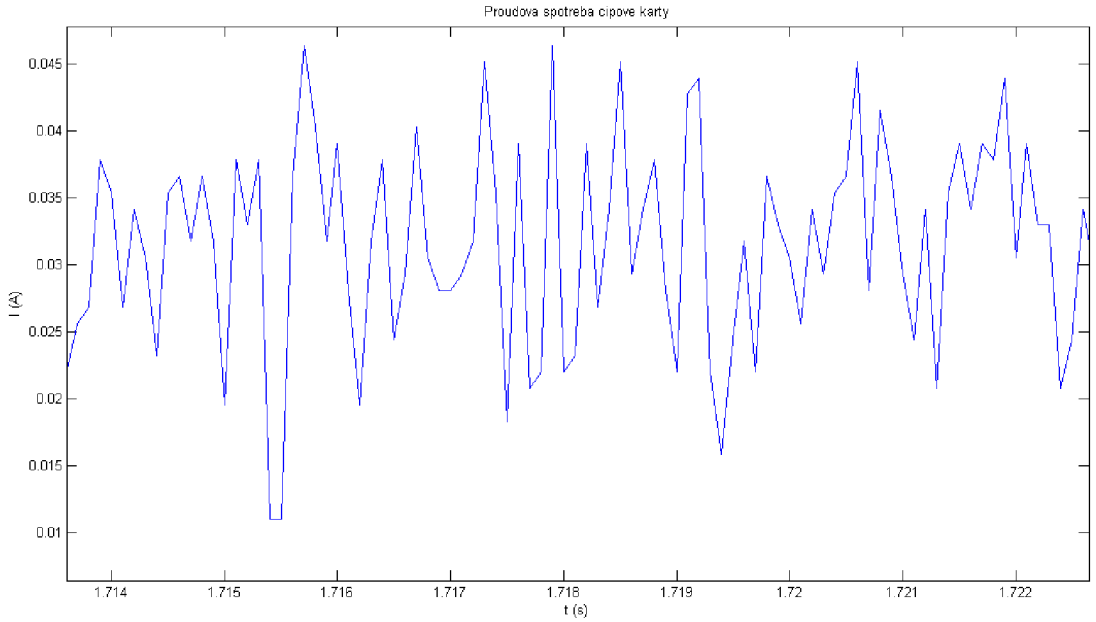
Obr. 6.3: Měření prováděné v reálném čase.

Upravené předchozí měření viz obr. 6.4. Pro lepší názornost a přesnost byly korigovány osy osciloskopů tak, aby byla zachycena pouze jedna komunikace čtečky a karty při jednom zaslaném APDU příkazu.

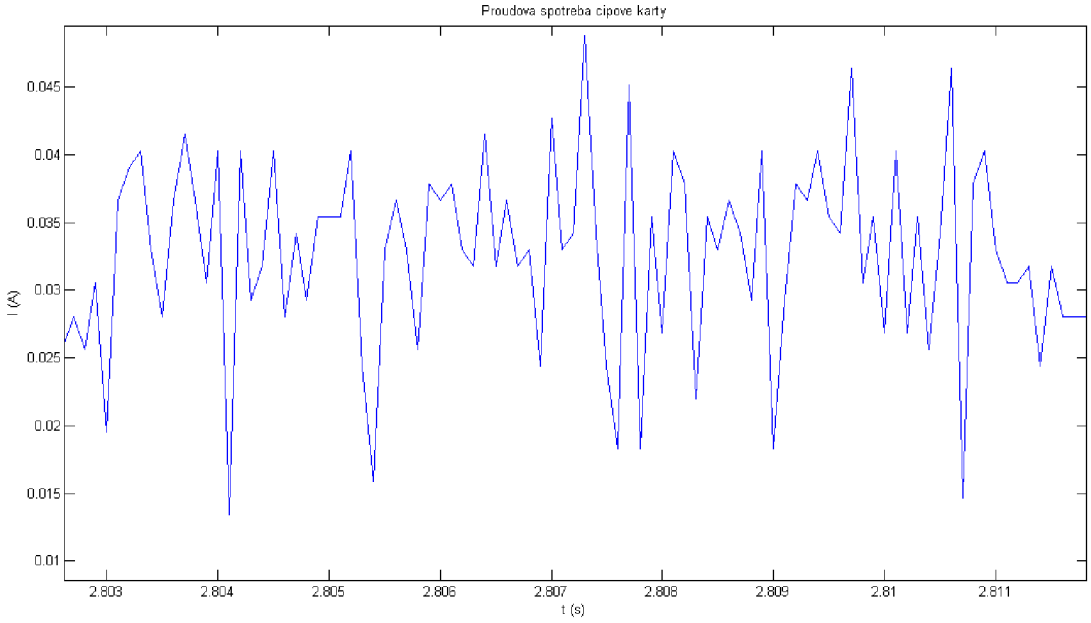


Obr. 6.4: Měření prováděné v reálném čase po korekci os.

Z měření na I/O portu byl určen počátek a konec komunikace, aby bylo možné určit čas, kdy karta zpracovávala zaslaný APDU příkaz. Proudová spotřeba při zpracování APDU příkazu je zachycena pro stejné příkazy zaslané s časovým odstupem viz obr. 6.3. K srovnání podobnosti byl vybrán druhý a třetí příkaz viz obr. 6.5 a obr. 6.6. Jak je ze zachycených proudových spotřeb patrné, tak si neodpovídají, i když je zpracováván totožný příkaz.

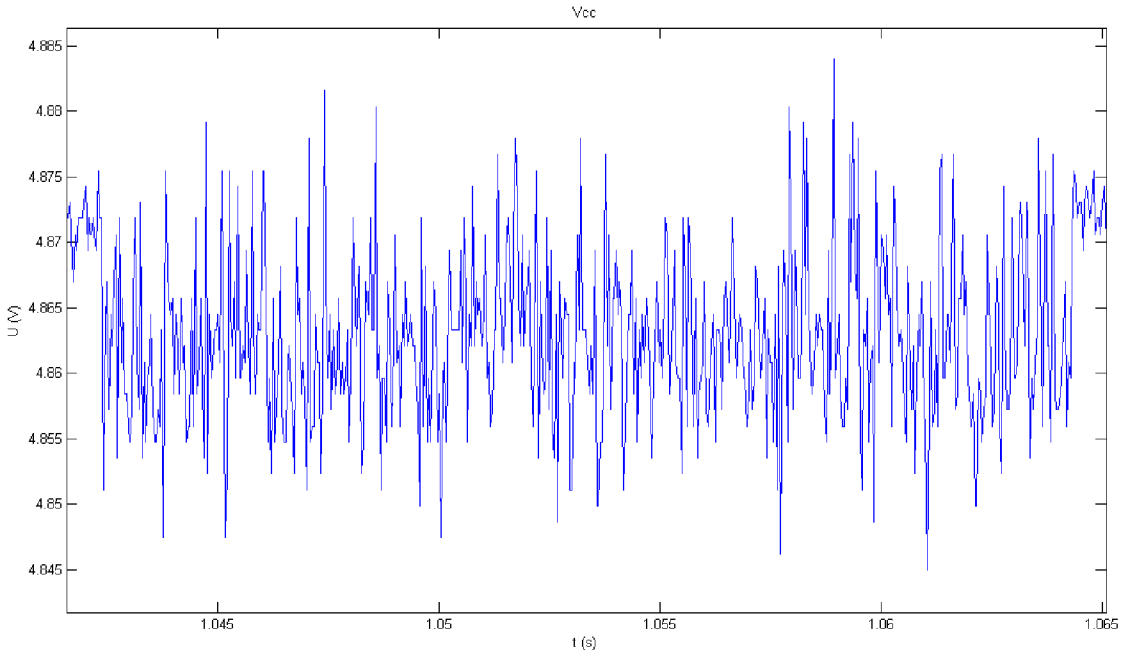


Obr. 6.5: Proudová spotřeba při druhém zaslání prvního příkazu.



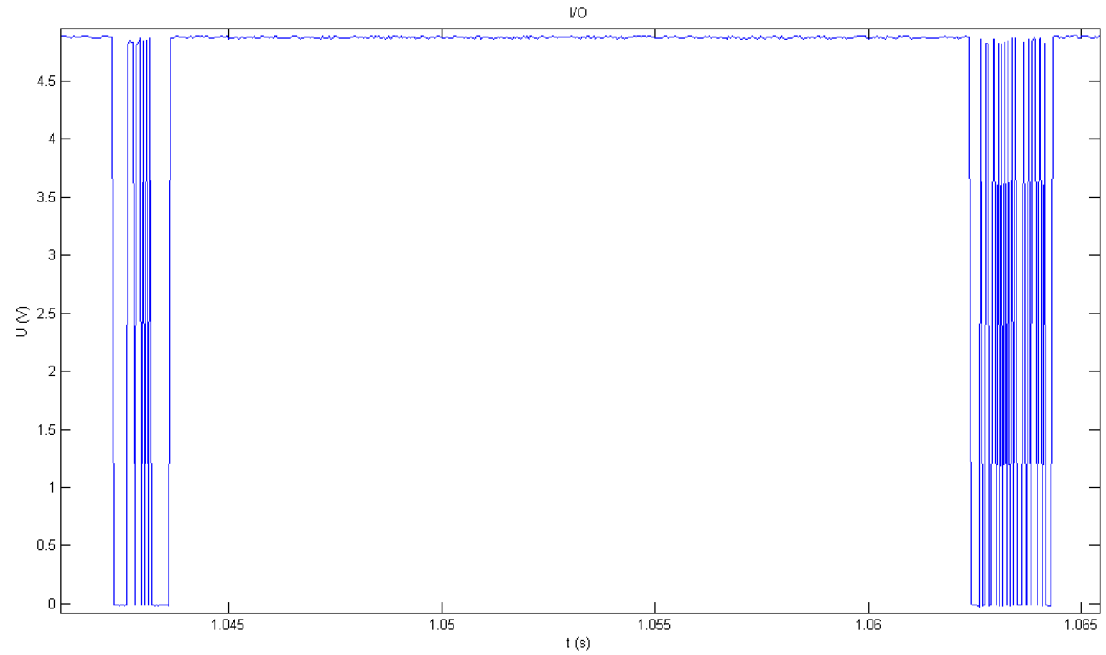
Obr. 6.6: Proudová spotřeba při třetím zaslání prvního příkazu.

Výsledky měření s hodnotou vzorkovacího času 0,0004. Při měření byly použity opět tři A/D vstupy. Měření nebylo možné sledovat přímo v reálném čase. Měřená data byla zaznamenávána do souborů mat. Záznam z prvního osciloskopu znázorňuje závislost napájecího napětí čipové karty na čase, viz obr. 6.7. Záznam z druhého osciloskopu znázorňuje závislost napěťových změn na I/O portu čipové karty na čase viz obr. 6.8.



Obr. 6.7: Závislost napájecího napětí čipové karty na čase.

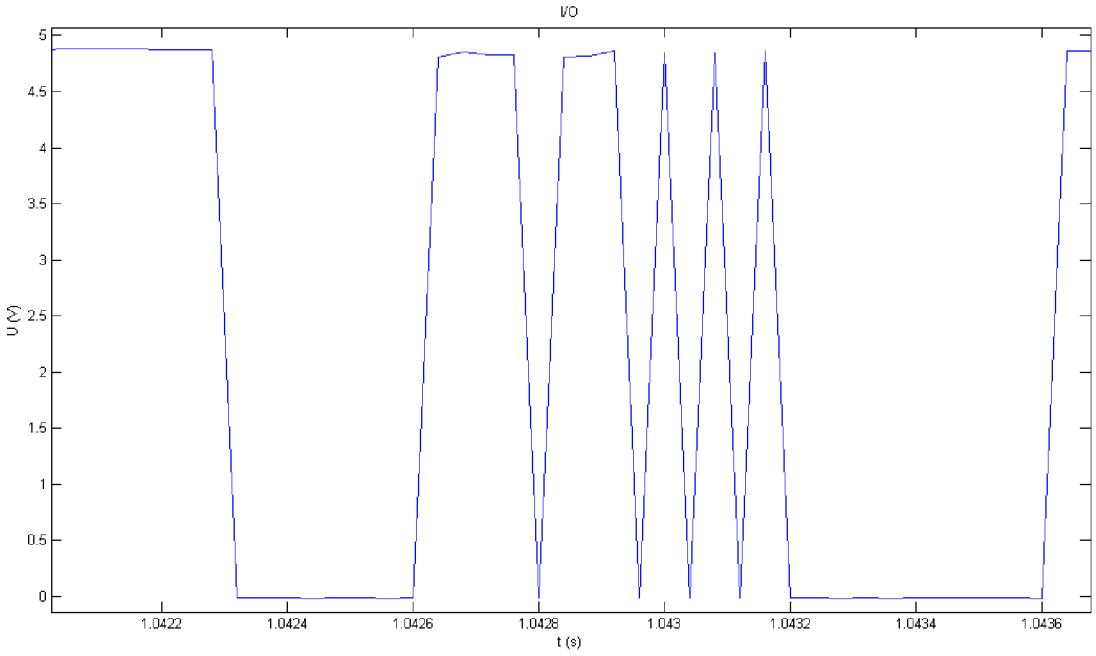
Při zpracovávání zaslaného příkazu je zachycen nepatrný pokles napětí přibližně 0.01 V, který začíná při odeslání příkazu a končí se zasláním odpovědi, viz obr. 6.7.



Obr. 6.8: Závislost napěťových změn na I/O portu čipové karty na čase.

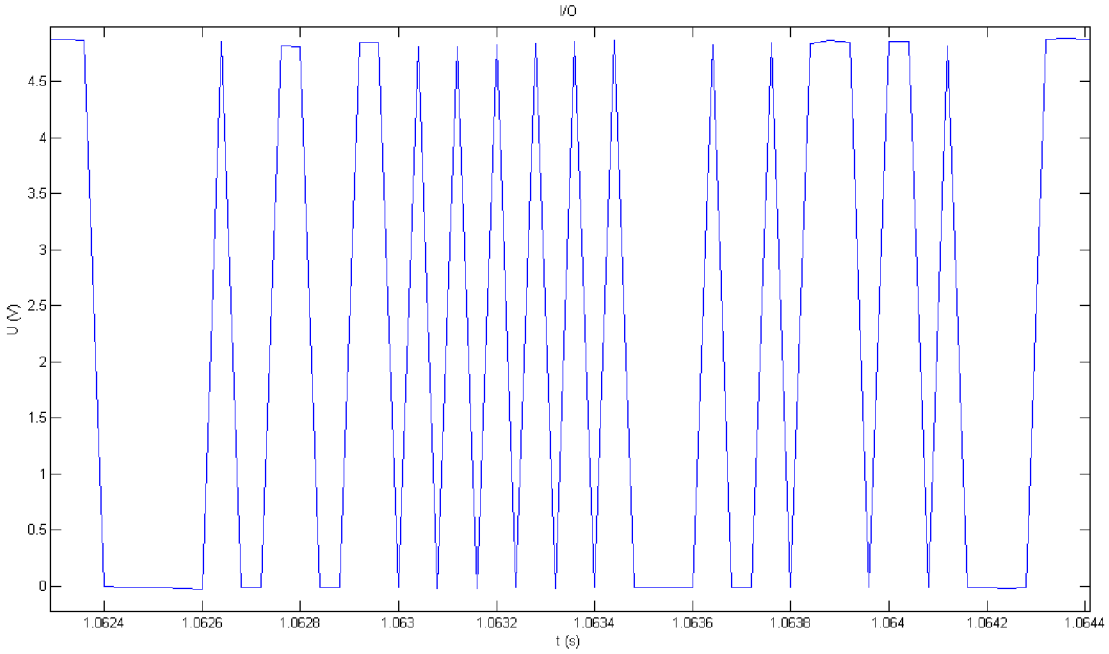
Zaslaný příkaz je předán přes I/O port z čtečky do karty. Karta následně zpracovává obdržený příkaz, po jeho dokončení odešle zpět čtečce zpracovaná data, mezi těmito kroky neprobíhá na I/O portu žádná komunikace, viz obr. 6.8.

Záznam z druhého osciloskopu v detailnějším pohledu na příkaz zaslaný kartě, který je zachycen na I/O portu čipové karty.



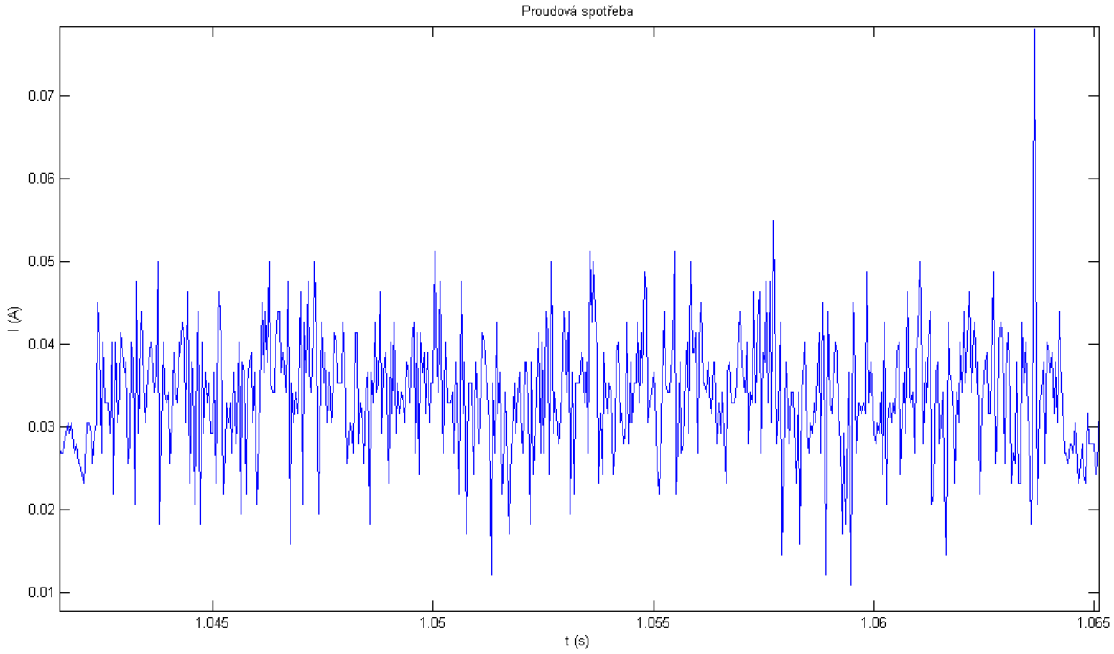
Obr. 6.9: Příkaz zaslaný kartě v detailnějším pohledu.

Záznam z druhého osciloskopu v detailnějším pohledu na odpověď, kterou zpracovala karta a odeslala přes I/O port zpět čtečce.



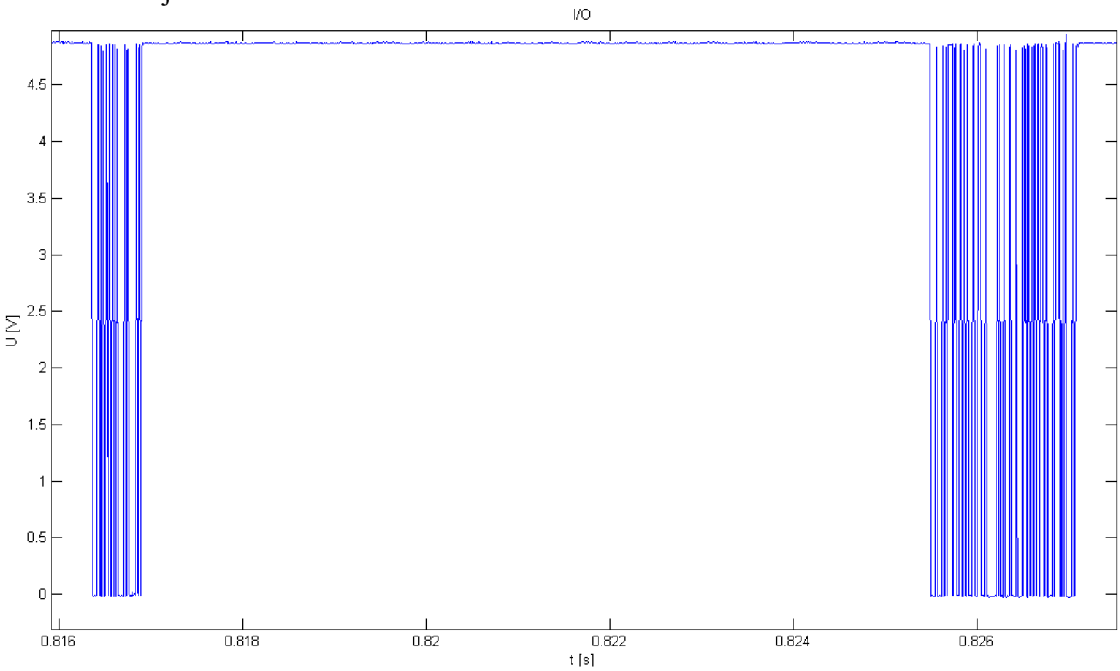
Obr. 6.10: Odpověď karty zaslaná čtečce v detailnějším pohledu.

Záznam z třetího osciloskopu znázorňuje závislost proudové spotřeby čipové karty na čase.

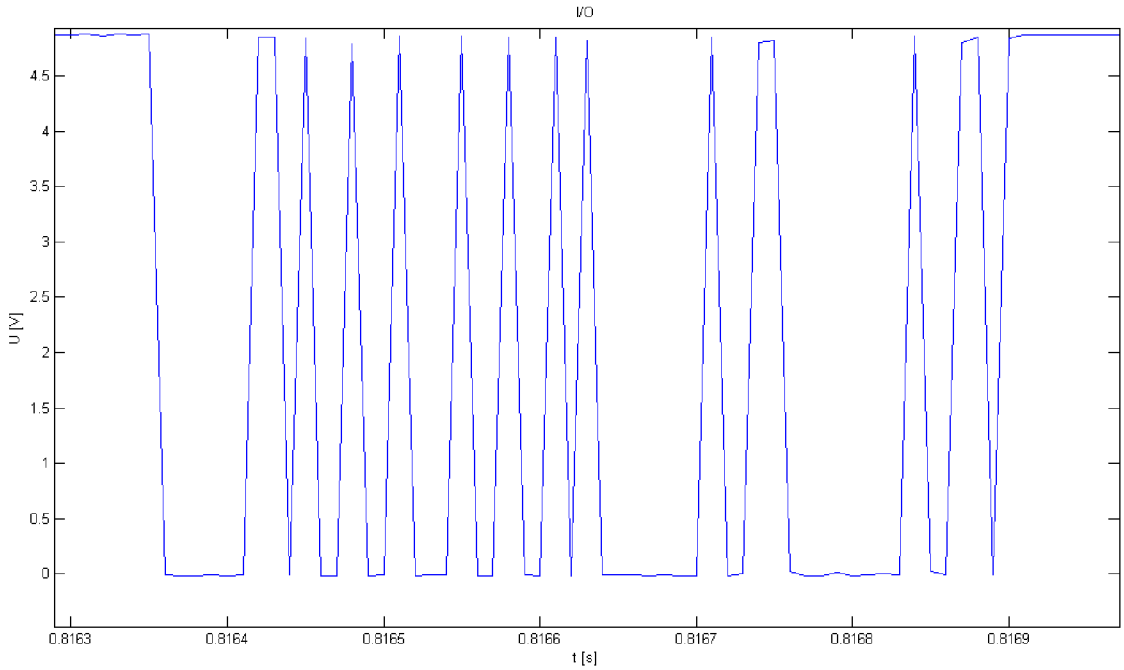


Obr. 6.11: Závislost proudové spotřeby čipové karty na čase.

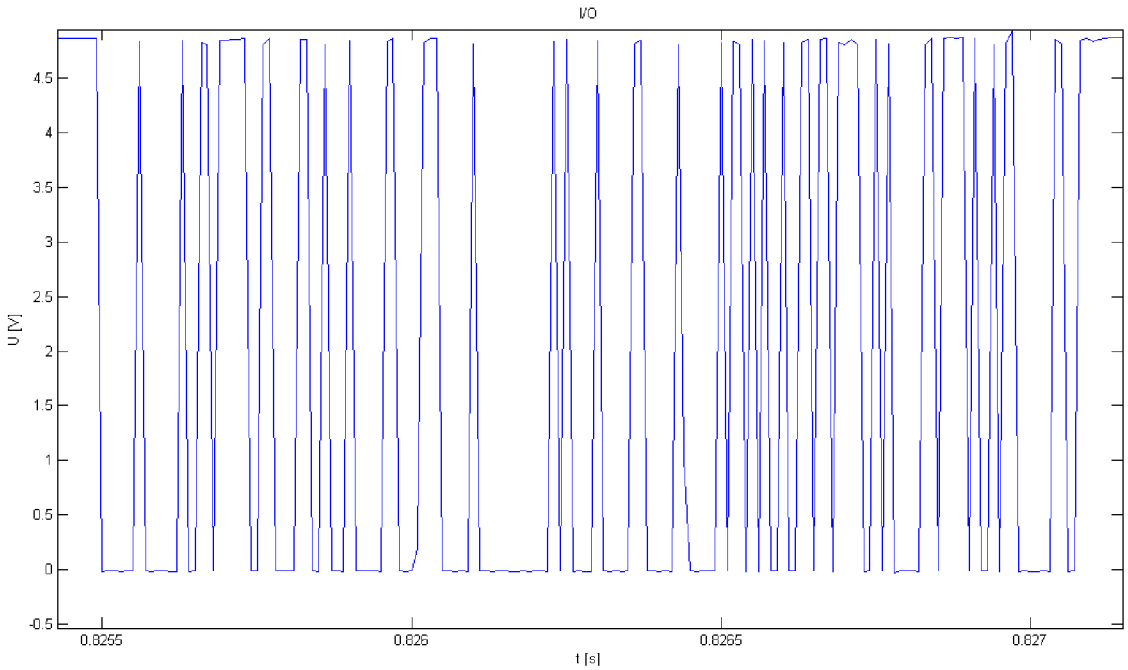
Pro dosažení většího vzorkovacího času musel být model upraven tak, že používal pouze jediný A/D vstup pro měření komunikace na I/O portu. Měření bylo provedeno s hodnotou vzorkovacího času 0,00001. Pro přehlednost je zachycena celá komunikace viz obr. 6.12. Zaslaný příkaz viz obr. 6.13. Zaslaná odpověď viz obr. 6.14. Je jasně patrné, že zachycená komunikace čtečky a karty je lépe patrná, ale vzorkovací čas není stále dostačující.



Obr. 6.12: Závislost napěťových změn na I/O portu čipové karty na čase.



Obr. 6.13: Příkaz zaslaný kartě v detailnějším pohledu.



Obr. 6.14: Odpověď karty zaslaná čtečce v detailnějším pohledu.

Z důvodů nekorektního chování pracovní stanice s měřící kartou AD622, nebylo možné se přiblížit maximálním technickým parametrům měřící karty, které by byly pro potřeby měření dostačující. Maximum udávané výrobcem je pro čtyři A/D vstupy 400 KHz a 625 KHz pro jeden A/D vstup. Měření bylo úspěšné pro hodnoty 25 a 50 KHz při použití tří A/D vstupů. Komunikace byla zachycena při použití pouze jediného A/D vstupu při vzorkovací frekvenci 100 KHz. Dosažené hodnoty nejsou pro přesné měření dostačující.

6.2 Monitorování komunikace osciloskopem

Při monitorování komunikace karty a čtečky byl použit osciloskop MSO9104A od firmy Agilent, který je určen pro nejširší možnosti měření. Maximální vzorkovací frekvence osciloskopu je 20 GSa. Měření bylo provedeno obdobným způsobem jako s měřící kartou. Při měření byly použity čtyři aktivní analogové kanály. Na prvním, druhém a třetím kanálu byla napěťová sonda. Čtvrtý kanál využíval diferenciální sondu. Osciloskop byl nastaven na hlídání sestupné hrany, která přijde na I/O port při začátku komunikace. Měřená data byla vzorkována 10 MSa/s a uložena pro následné zpracování do souboru csv (Comma-separated values). Při zpracování naměřených dat byl použit Matlab.

6.2.1 Parametry komunikace a zachycená komunikace

Přenosová rychlost udává počet bitů přenesených za sekundu a je dána vztahem (6.1). Hodinová frekvence určuje dobu zpracování příkazu, byla 4,8 MHz a převodní faktor byl 31. Dosazením do rovnice (6.1) a úpravou získáme hodnoty, viz tab. 6.3.

$$\frac{\text{hodinová frekvence}}{\text{převodní faktor}} = \text{přenosová rychlost} \tag{6.1}$$

Základní časová jednotka (etu) je interval nezbytný pro přenos jednoho bitu. Tento interval se počítá od přenosové rychlosti a je dán vztahem.

$$\frac{1}{bit\,\frac{1}{s}} = 1\ etu \tag{6.2}$$

Bity v každém bajtu jsou doprovázeny start bitem, paritním bitem a v závislosti na použitém protokolu jedním nebo dvěma stop bity, celkem je tedy přenášeno 11 nebo 12 bitů. Start bit slouží k synchronizaci komunikujících stran a je na začátku každého bajtu. Tím je pro obě strany definován každý začátek bajtu při přenosu. Paritní bit zabezpečuje přenos proti chybám. Stop bit poskytuje interval pro příjemce na konci přenosu znaku, aby mohl znak zpracovat. Stop bity jsou vždy na úrovni H a start bit je vždy na úrovni L. Interval pro přenos jednoho znaku závisí na počtu a době trvání bitů přenášených bitů. CWT (Character Waiting Time) je maximální interval mezi dvěma přenášenými znaky (tj. mezi dvěma start bity). Pokud je tato doba překročena, přijímač předpokládá, že přenos byl ukončen. BGT (Blok Guard Time) a BWT (Block Waiting Time) kontroluje přepínání mezi vysílačem a přijímačem.

Tab. 6.1: Doba komunikace.

Číslo příkazu	příkaz 1	příkaz 2
doba příkazu [ms]	1,298	1,298
doba odpovědi [ms]	1,85	0,429
doba celé komunikace [ms]	21,92	7,324

Měřeny byly dva stejné příkazy, které měly pozměněnou datovou část, viz tab. 6.2. Z naměřených dat byla zjištěna doba komunikace příkazů, viz tab. 6.1. Pro potřeby následné analýzy přenášených dat byly spočítány parametry komunikace. Podle změřených dat se dá odvodit, že komunikace probíhala na protokolu T=0. V programu byl ale vybrán protokol přenosu T=1. Diagnostický nástroj také ukazoval zvolený protokol přenosu T=1. Ze zachycené komunikace je patrné, že jsou při komunikaci používány dva stop bity a ty používá pouze protokol T=0. Z měřených dat byla zjištěna doba, za kterou je přenesen jeden bajt. Protože je pevně dané, že použitý protokol T=0 používá pro přenesení jednoho bajtu 12 bitů, lze dopočítat dobu potřebnou k přenesení jednoho bitu. Tyto parametry jsou využity při analýze komunikace karty a čtečky. Pro určení přenosové rychlosti je využito vztahu (6.2). Vztah (6.1) je použit při odhadu použitého převodního faktoru a hodinové frekvence nelze jednoznačně určit. Nejpravděpodobnější je převodní faktor 31 a hodinová frekvence 4,8 MHz. Stejnou frekvenci vypsal i diagnostický program pro čtečku OMNIKEY.

Tab. 6.2: Použité APDU příkazy.

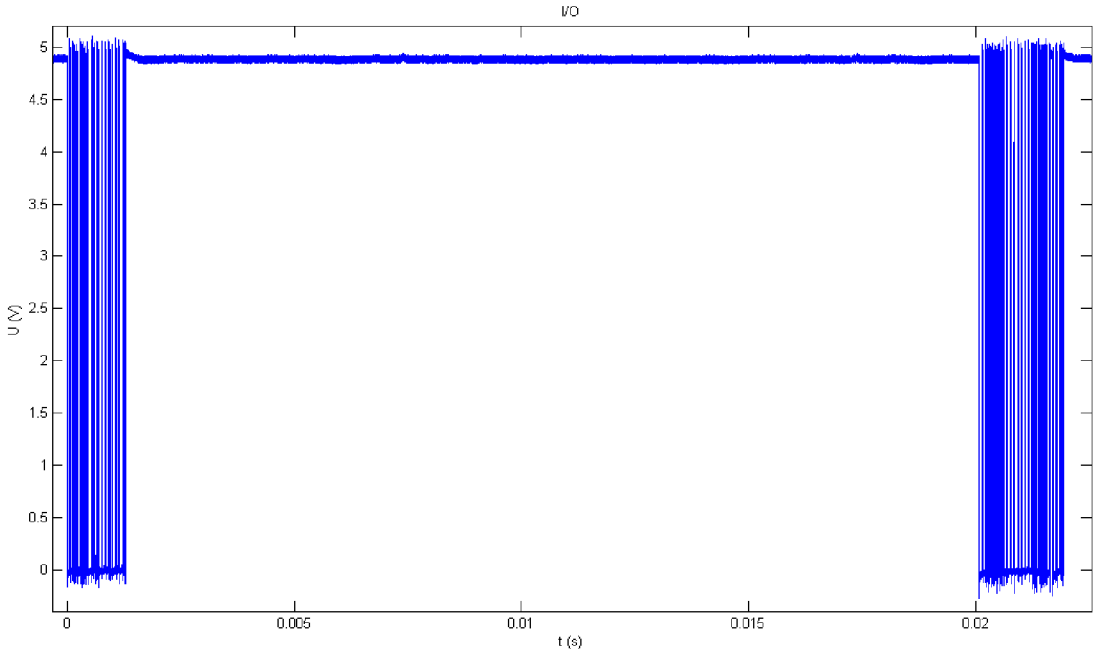
APDU příkaz 1	
příkaz	00 A4 04 00 08 A0 00 00 00 03 00 00 00 00
odpověď	6F 10 84 08 A0 00 00 00 03 00 00 00 A5 04 9F 65 01 FF 90 00
APDU příkaz 2	
příkaz	00 A4 04 00 08 A0 01 00 00 03 00 00 00 00
odpověď	6A 82

Tab. 6.3: Vypočtené parametry komunikace.

Protokol	**T=0**		**T=1**	
doba potřebná k přenesení jednoho bajtu [ms]	0,07758		0,07758	
doba potřebná k přenesení jednoho bitu [µs]	6,465		7,053	
přenosová rychlost [bit/s]	154 679		141 784	
převodní faktor [-]	31	32	31	32
hodinová frekvence [Hz]	4 795 049	4 949 728	4 395 304	4 537 088

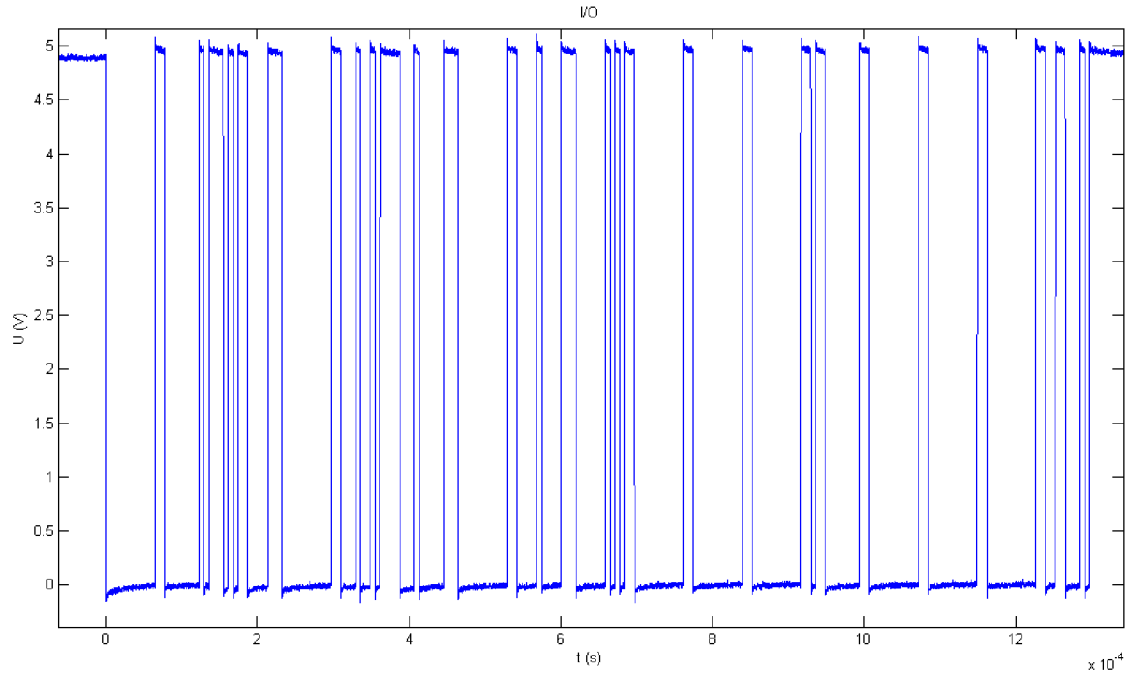
6.2.2 Zachycená komunikace

Zaslaný první APDU příkaz je předán přes I/O port z čtečky do karty viz obr. 6.15. S příchodem start bitu začíná karta pracovat a přijímá zaslaný příkaz, jeho celém přijmutí začíná příkaz zpracovávat, po zpracování příkazu odešle výsledek – odpověď zpět čtečce. Mezi příkazem a odpovědí neprobíhá na I/O portu žádná komunikace viz obr. 6.15. Z klidové doby je patrné, že přes I/O port nejsou přenášeny žádné start ani stop bity, které jsou obsaženy v každé komunikaci.



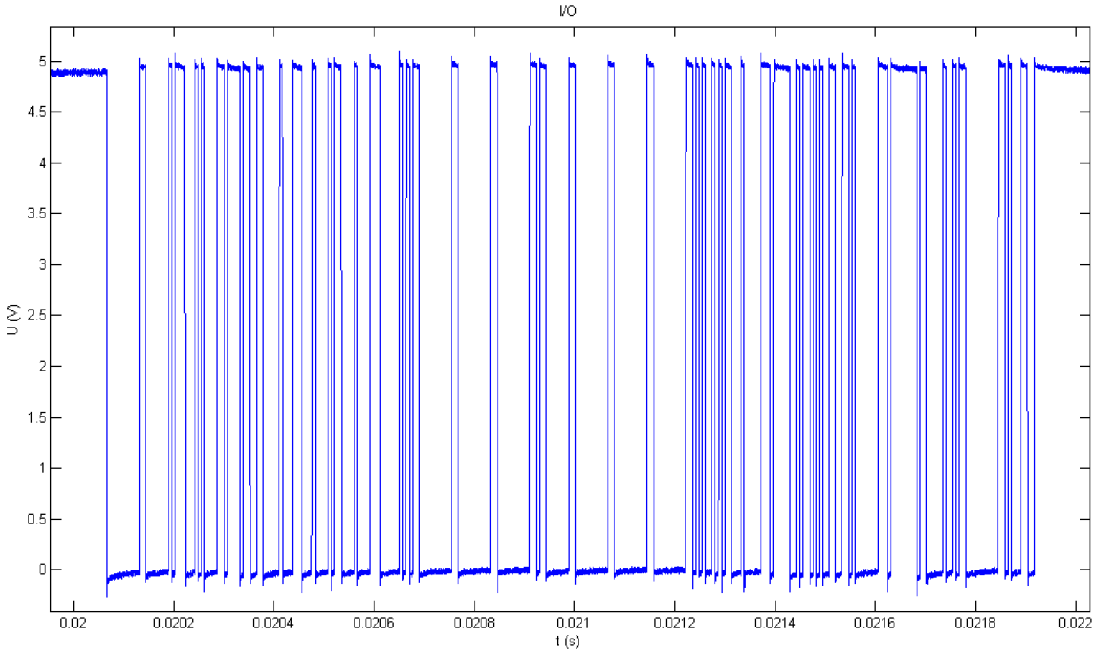
Obr. 6.15: Závislost napěťových změn na I/O portu čipové karty na čase - první příkaz.

Pro lepší názornost je zachycena pouze příkazová část prvního APDU příkazu. Jak je ze zachycených dat patrné, vzorkovací frekvence je dostatečná. Nejlépe jsou rozpoznatelné zaslané nulové bajty. Pro celkové odvození jednotlivých bitů přenosu není obrázek dost přesný, proto bude nutné využít přesnější analýzu probíhající komunikace.



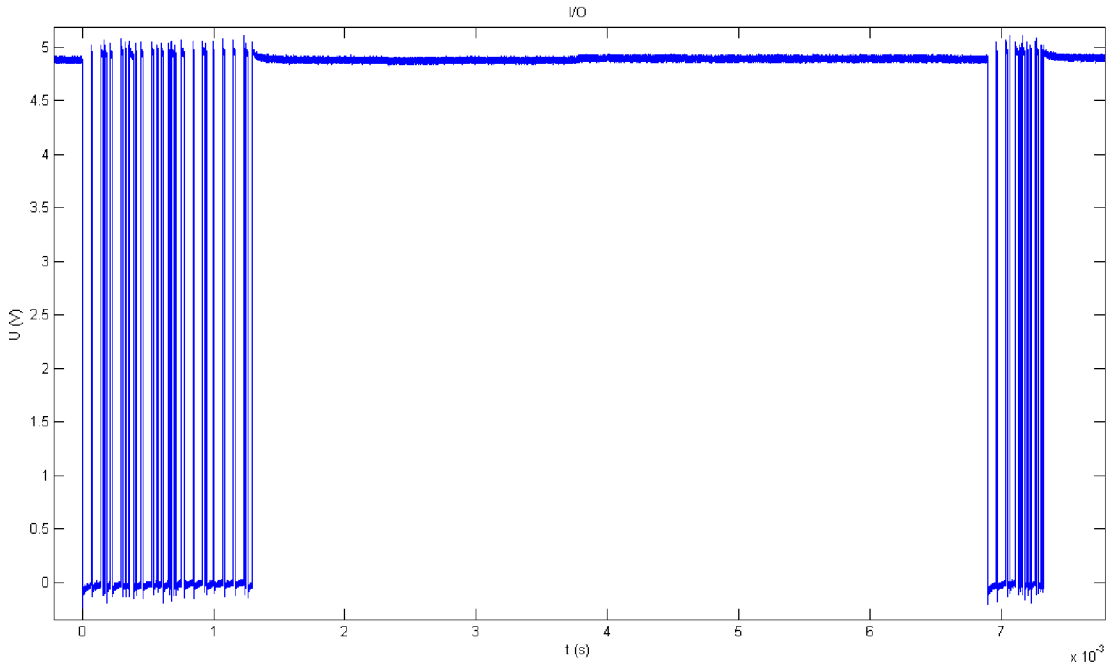
Obr. 6.16: První APDU příkaz - příkaz zaslaný kartě v detailnějším pohledu.

Pro lepší názornost je zachycena pouze část odpovědi prvního APDU příkazu. Je patrné při porovnání pouhým okem, že v odpovědi je přenášeno větší množství dat než u příkazu.



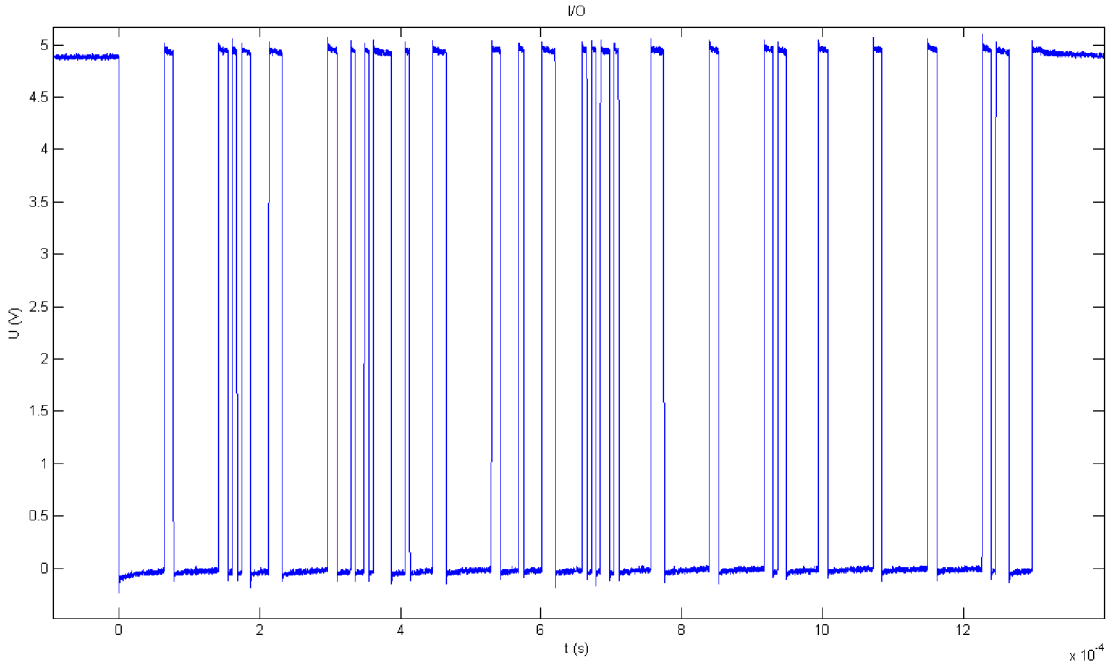
Obr. 6.17: První APDU příkaz - odpověď zaslaná kartě v detailnějším pohledu.

Zaslaný druhý APDU příkaz je předán přes I/O port z čtečky do karty viz obr. 6.18. V příkazové části byla pozměněna jedna položka dat, je patrné, že kartě stačí menší čas při zpracování příkazu. Zaslaná odpověď je menší než u prvního APDU příkazu.



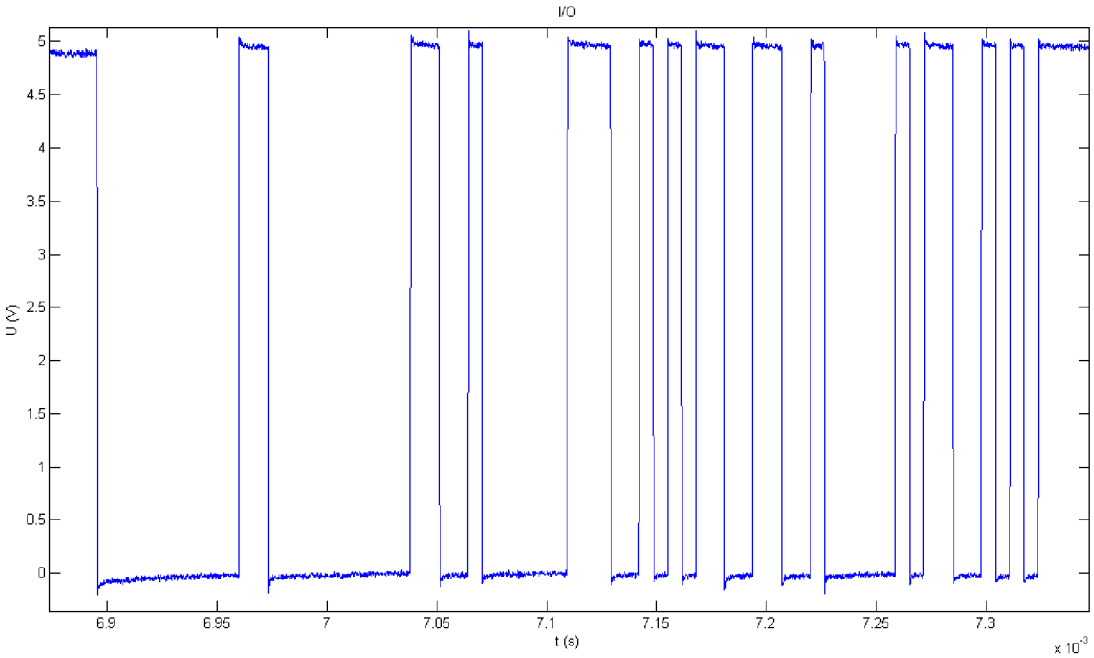
Obr. 6.18: Závislost napěťových změn na I/O portu čipové karty na čase - druhý příkaz.

Pro lepší názornost je zachycena opět pouze příkazová část druhého APDU příkazu.



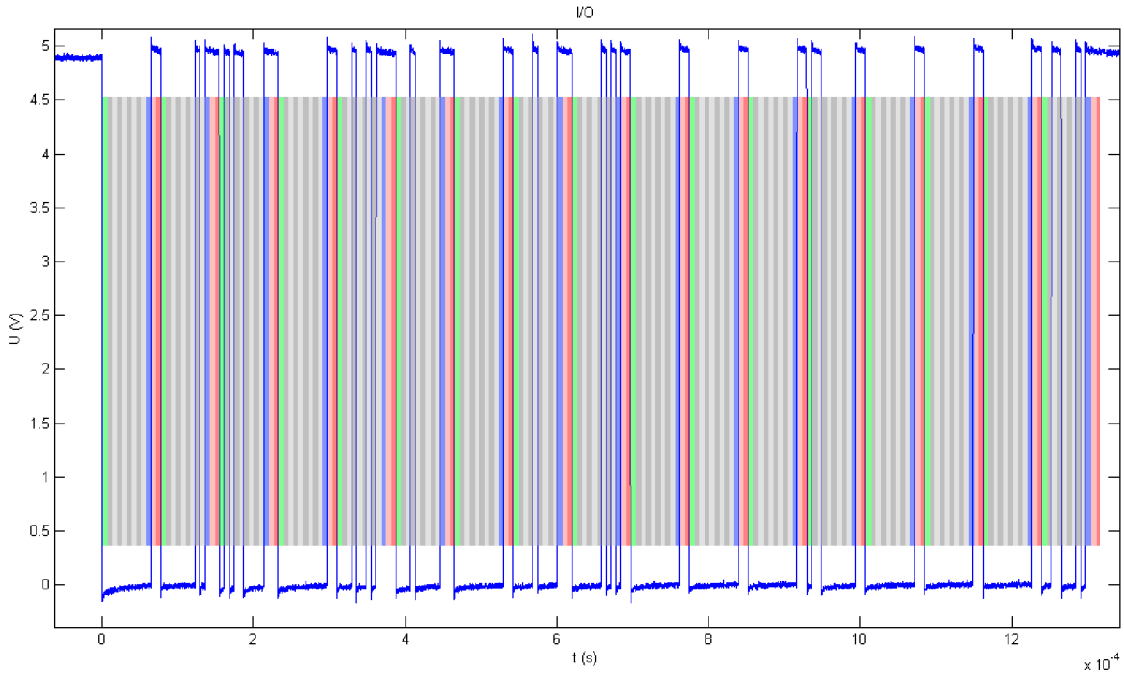
Obr. 6.19: Druhý APDU příkaz - příkaz zaslaný kartě v detailnějším pohledu.

Pro lepší názornost je opět zachycena pouze část odpovědi druhého APDU příkazu.



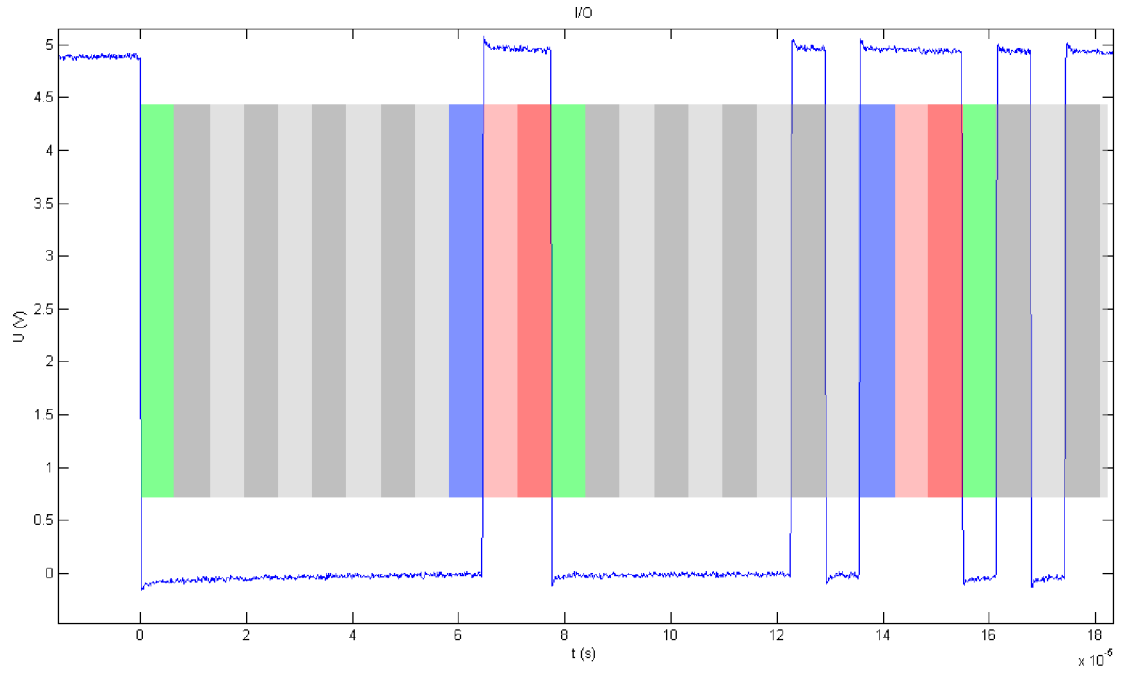
Obr. 6.20: Druhý APDU příkaz - odpověď zaslaná kartě v detailnějším pohledu.

Obrázek byl vytvořen z naměřených dat uložených do csv. Při zpracování byl použit Matlab. Grafy byly uloženy do formátu png (Portable Network Graphics). Obrázky byly vloženy do programu Paint.NET, který dokáže upravovat fotografie a nabízí inovativní uživatelské prostředí a podporuje vrstvy. Do obrázku byla přidána další vrstva s barevným rozdělením jednoho bajtu na jednotlivé bity pro názorné zobrazení.



Obr. 6.21: První APDU příkaz - příkaz po analýze komunikace.

Vrstva barevného rozdělení jednoho bajtu na jednotlivé bity označuje start bit zelenou barvou, přenášený bajt je označen tmavě a světle šedou pro lepší rozeznání. Paritní bit má modrou barvu. První stop bit má světle červenou a druhý stop bit tmavě červenou.



Obr. 6.22: Detailní výřez analýzy komunikace s barevným odlišením jednotlivých bitů.

Na detailním výřezu je snadno pozorovatelná hodnota komunikace. V čase 0 sekund začíná komunikace start bitem 0, dále následuje osm datových bitů 8 až 1 a všechny nabývají hodnoty 0. Desátý v pořadí je bit sudé parity s hodnotou 0. Po paritě následují dva stop bity a oba nabývají hodnoty 1. Druhý bajt se liší v 8 a 10 bitu, kde nabývá hodnoty 1.

Zachycená komunikace byla pro přehlednost zpracována do čtyř tabulek. V první tabulce je zaznamenán první APDU příkazu část příkazu viz tab. 6.4. Ve druhé je zaznamenán první APDU příkaz část odpovědi viz tab. 6.5. Ve třetí je zaznamenán druhý APDU příkaz, část příkazu viz tab. 6.6. Ve čtvrté je zaznamenán druhý APDU příkaz, část odpovědi viz tab. 6.7.

Tab. 6.4: Zachycená komunikace prvního APDU příkazu - příkaz.

Číslo bajtu	Start bit	8. bit	7. bit	6. bit	5. bit	4. bit	3. bit	2. bit	1. bit	Paritní bit	Stop bit 1	Stop bit 2	Hex.
1	0	0	0	0	0	0	0	0	0	0	1	1	00
2	0	0	0	0	0	0	0	1	0	1	1	1	40
3	0	1	0	1	1	0	0	0	0	1	1	1	0D
4	0	0	0	0	0	0	0	0	0	0	1	1	00
5	0	0	0	1	0	0	1	0	1	1	1	1	A4
6	0	0	0	1	0	0	0	0	0	1	1	1	04
7	0	0	0	0	0	0	0	0	0	0	1	1	00
8	0	0	0	0	1	0	0	0	0	1	1	1	08
9	0	0	0	0	0	0	1	0	1	0	1	1	A0
10	0	0	0	0	0	0	0	0	0	0	1	1	00
11	0	0	0	0	0	0	0	0	0	0	1	1	00
12	0	0	0	0	0	0	0	0	0	0	1	1	00
13	0	1	1	0	0	0	0	0	0	0	1	1	03
14	0	0	0	0	0	0	0	0	0	0	1	1	00
15	0	0	0	0	0	0	0	0	0	0	1	1	00
16	0	0	0	0	0	0	0	0	0	0	1	1	00
17	0	0	1	1	0	0	0	1	0	1	1	1	46

Tab. 6.5: Zachycená komunikace prvního APDU příkazu - odpověď.

Číslo bajtu	Start bit	8. bit	7. bit	6. bit	5. bit	4. bit	3. bit	2. bit	1. bit	Paritní bit	Stop bit 1	Stop bit 2	Hex.
1	0	0	0	0	0	0	0	0	0	0	1	1	00
2	0	0	0	0	0	0	0	1	0	1	1	1	40
3	0	0	0	1	0	1	0	0	0	0	1	1	14
4	0	1	1	1	1	0	1	1	0	0	1	1	6F
5	0	0	0	0	0	1	0	0	0	1	1	1	10
6	0	0	0	1	0	0	0	0	1	0	1	1	84
7	0	0	0	0	1	0	0	0	0	1	1	1	08
8	0	0	0	0	0	0	1	0	1	0	1	1	A0
9	0	0	0	0	0	0	0	0	0	0	1	1	00
10	0	0	0	0	0	0	0	0	0	0	1	1	00
11	0	0	0	0	0	0	0	0	0	0	1	1	00
12	0	1	1	0	0	0	0	0	0	0	1	1	03
13	0	0	0	0	0	0	0	0	0	0	1	1	00
14	0	0	0	0	0	0	0	0	0	0	1	1	00
15	0	0	0	0	0	0	0	0	0	0	1	1	00
16	0	1	0	1	0	0	1	0	1	0	1	1	A5
17	0	0	0	1	0	0	0	0	0	1	1	1	04
18	0	1	1	1	1	1	0	0	1	0	1	1	9F
19	0	1	0	1	0	0	1	1	0	0	1	1	65
20	0	1	0	0	0	0	0	0	0	1	1	1	01
21	0	1	1	1	1	1	1	1	1	0	1	1	FF
22	0	0	0	0	0	1	0	0	1	0	1	1	90
23	0	0	0	0	0	0	0	0	0	0	1	1	00
24	0	1	0	0	0	1	1	0	0	1	1	1	31

Tab. 6.6: Zachycená komunikace druhého APDU příkazu - příkaz.

Číslo bajtu	Start bit	8. bit	7. bit	6. bit	5. bit	4. bit	3. bit	2. bit	1. bit	Paritní bit	Stop bit 1	Stop bit 2	Hex.
1	0	0	0	0	0	0	0	0	0	0	1	1	00
2	0	0	0	0	0	0	0	0	0	0	1	1	00
3	0	1	0	1	1	0	0	0	0	1	1	1	0D
4	0	0	0	0	0	0	0	0	0	0	1	1	00
5	0	0	0	1	0	0	1	0	1	1	1	1	A4
6	0	0	0	1	0	0	0	0	0	1	1	1	04
7	0	0	0	0	0	0	0	0	0	0	1	1	00
8	0	0	0	0	1	0	0	0	0	1	1	1	08
9	0	0	0	0	0	0	1	0	1	0	1	1	A0
10	0	1	0	0	0	0	0	0	0	1	1	1	01
11	0	0	0	0	0	0	0	0	0	0	1	1	00
12	0	0	0	0	0	0	0	0	0	0	1	1	00
13	0	1	1	0	0	0	0	0	0	0	1	1	03
14	0	0	0	0	0	0	0	0	0	0	1	1	00
15	0	0	0	0	0	0	0	0	0	0	1	1	00
16	0	0	0	0	0	0	0	0	0	0	1	1	00
17	0	1	1	1	0	0	0	0	0	1	1	1	07

Tab. 6.7: Zachycená komunikace druhého APDU příkazu - odpověď.

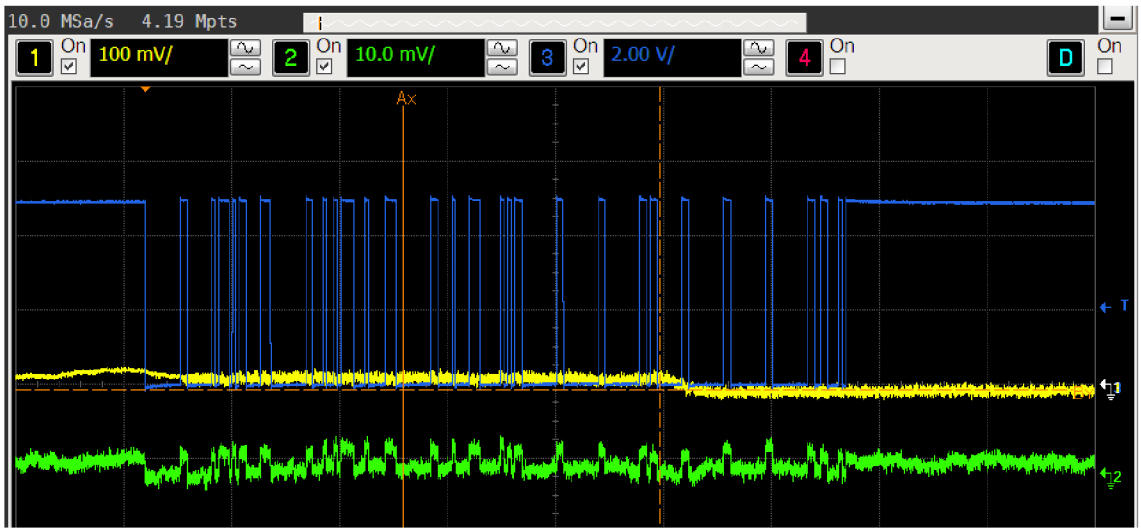
Číslo bajtu	Start bit	8. bit	7. bit	6. bit	5. bit	4. bit	3. bit	2. bit	1. bit	Paritní bit	Stop bit 1	Stop bit 2	Hex.
1	0	0	0	0	0	0	0	0	0	0	1	1	00
2	0	0	0	0	0	0	0	0	0	0	1	1	00
3	0	0	1	0	0	0	0	0	0	1	1	1	02
4	0	0	1	0	1	0	1	1	0	1	1	1	6A
5	0	0	1	0	0	0	0	0	1	0	1	1	82
6	0	0	1	0	1	0	1	1	1	1	1	1	EA

Ze zachycené a následně analyzované komunikace je jasně patrné, že analýza dat byla úspěšná. Získaná data odpovídají zaslaným APDU příkazům a odpovědím co obdržel použitý software. Komunikace navíc obsahuje na začátku 3 bajty a na konci jeden bajt u každého příkazu.

6.3 Změny napájení pří probíhajících výpočtech

Při měření pomocí měřící karty AD622 bylo zachyceno více stejných APDU příkazů. Příkazy byly od sebe odděleny na základně začínající a končící komunikace na I/O portu. Ze zachycené proudové spotřeby byly v odpovídajících časech získány hodnoty spotřeby pro konkrétní příkaz a tyto spotřeby byly následně porovnány. Odpovídající časy byly získány z grafů. Z celkových dat byly vyčteny pouze potřebné informace a ty uloženy do nového souboru mat. Pro tyto opakující se operace byly vytvořeny skripty a funkce, které následně ulehčily zpracování naměřených dat. Spotřeby vzorků prvního APDU příkazu jsou zachyceny, viz obr. 6.24 a 6.25. Spotřeby vzorků druhého APDU příkazu jsou zachyceny, viz obr. 6.26 a 6.27. Zaslaná data a odpovědi jsou stejné. Čipová karta zpracovává první APDU příkaz pokaždé 22 ms a druhý příkaz 7 ms. Z porovnaných dat je patrné, že spotřeby nejsou pro stejný příkaz totožné.

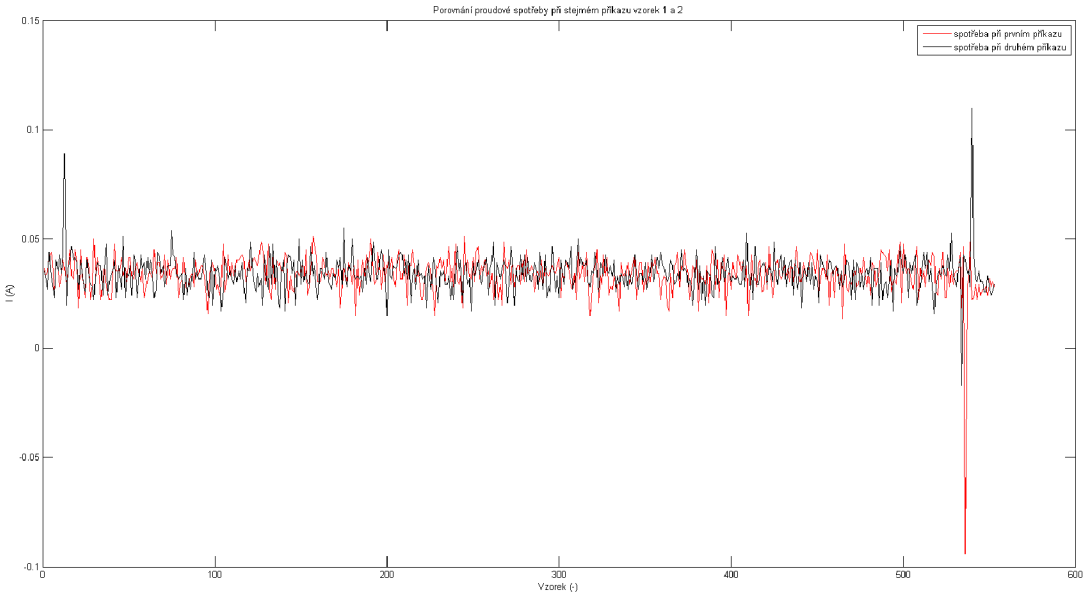
Při prvním měření na osciloskopu MSO9104A se nejpravděpodobněji nedopatřením při měření podařilo zachytit uniklé informace z I/O portu elektromagnetickým kanálem. Všechny kanály byly osazeny citlivou napěťovou sondou. První kanál má žlutou barvu a měří napětí před rezistorem. Druhý kanál má zelenou barvu a měří napětí za rezistorem v mV, při měření nebyla sonda správně zachycena a dokázala zachytit unikající informace z I/O portu (ze vzduchu) viz obr. 6.23. Třetí kanál má modrou barvu a měří změny napětí ve V při probíhající komunikaci na I/O portu. Unikající informace přesně odpovídají komunikaci, která byla změřena třetím kanálem. S poklesem napětí na třetím kanálu, což odpovídá přenosu bitů s hodnotou 0, se projeví i pokles napětí na druhém kanálu. Taktéž při nárůstu napětí na třetím kanálu, což odpovídá přenosu bitů s hodnotou 1, se projeví nárůst napětí i na druhém kanálu.



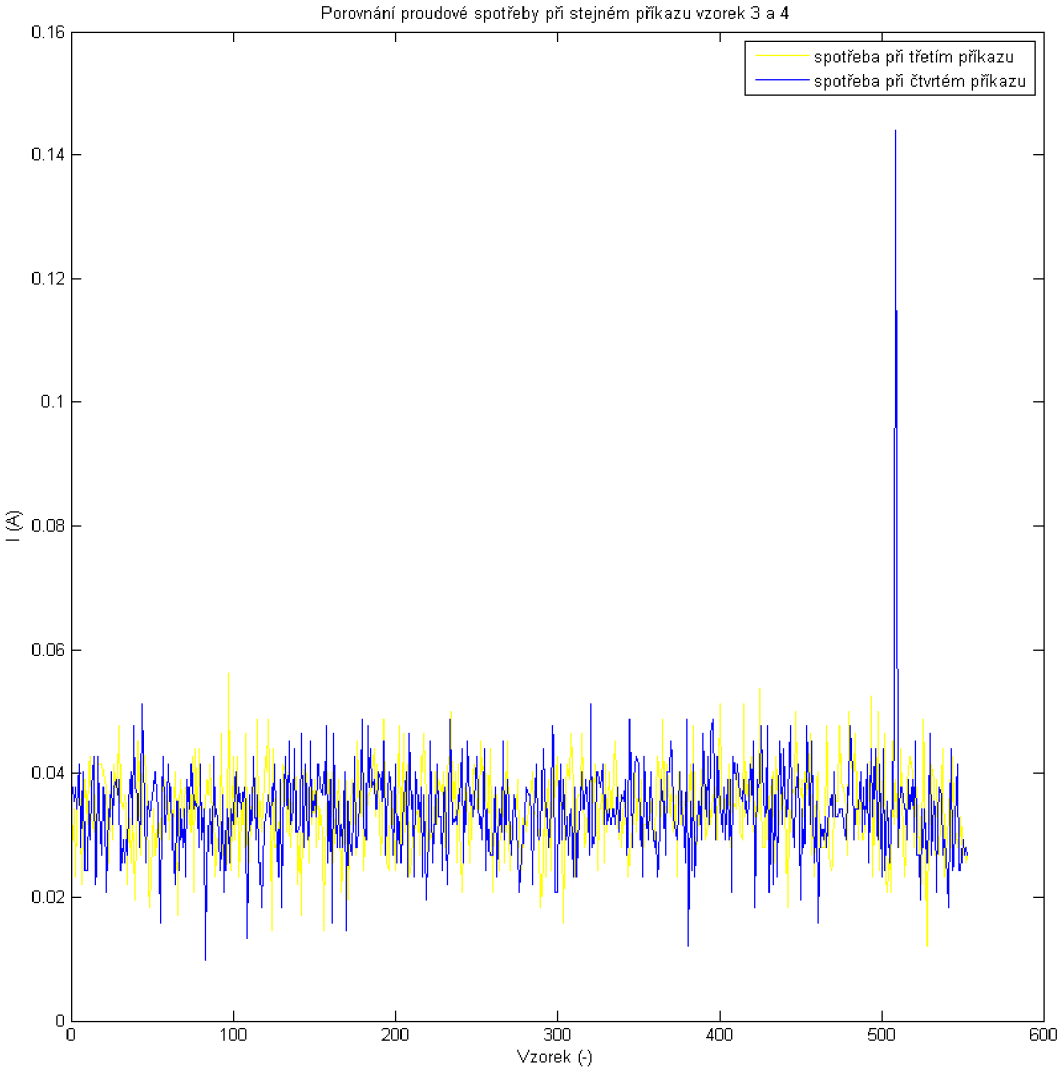
Obr. 6.23: Únik elektromagnetickým kanálem z I/O portu.

Při měření pomocí osciloskopu byla vzorkovací frekvence natolik dostatečná, aby bylo možné pozorovat závislosti spotřeby čipové karty při zpracování i jednotlivý bitů během celé komunikace viz obr. 6.28 a 6.29. Výsledné grafy byly upraveny podle vlastního uvážení pomocí změn rozsahu souřadnic, protože rozsah byl vybírán automaticky a často nebyl přehledný. Grafy se v Matlabu i přes velké množství naměřených hodnot vykreslovaly rychle a bez větších problémů.

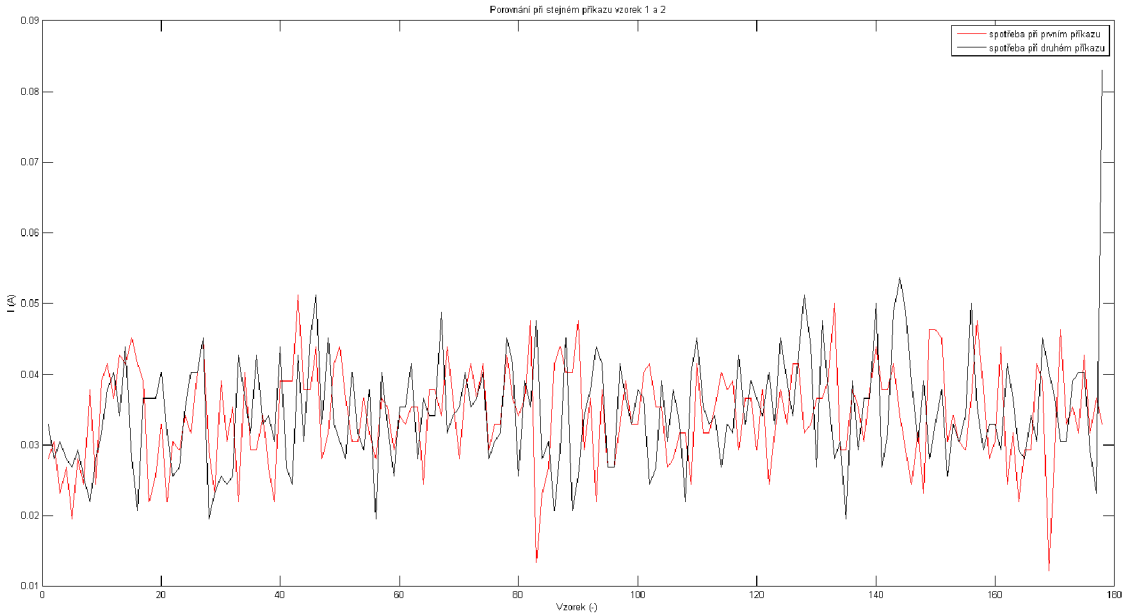
Porovnání bylo provedeno pro dva používané APDU příkazy. Spotřeba jednotlivý vzorků je barevně odlišena. Při detailním zkoumání spotřeby jednotlivých bajtů a bitů nebyla zjištěna žádná souvislost. Pro lepší a přehlednější sledování závislostí a určení jednotlivých bitů ve spotřebě bylo využito podobného principu jako v části analýzy komunikace. Data spotřeby byla rozdělena svislými černými čarami na jednotlivé bity a nový bajt je vykreslen červenou čarou. Podobnost se neprojevila ani u stejných bajtů, které obsahovaly samé nuly krom dvou stop bitů. Pouze na začátku komunikace při začátcích nových bajtů se projeví opakovaně růst spotřeby.



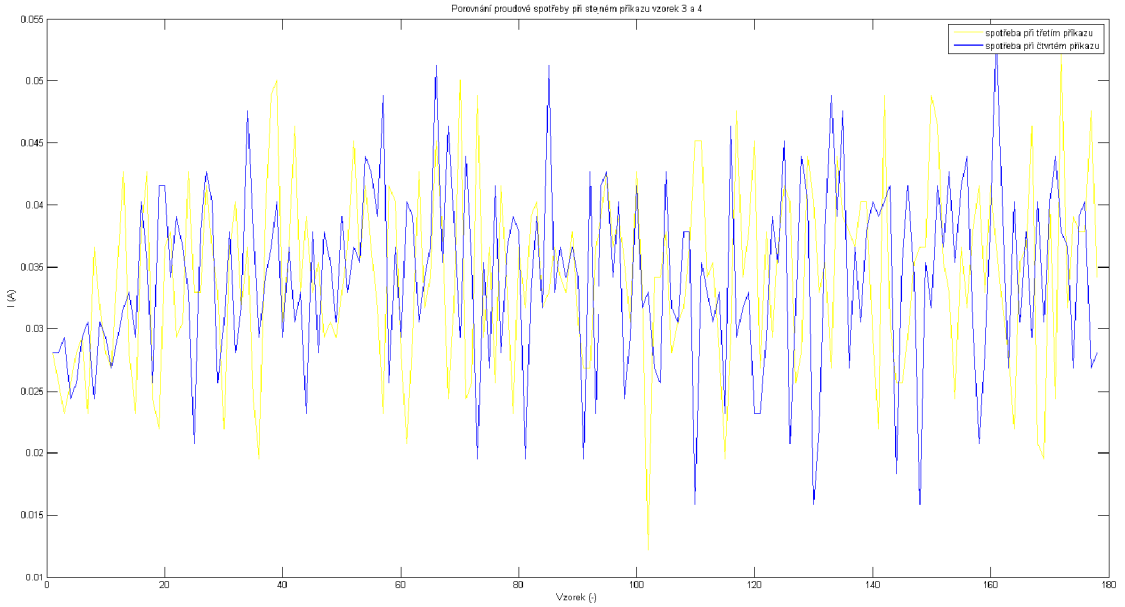
Obr. 6.24: Porovnání proudové spotřeby prvního příkazu - vzorky 1 a 2.



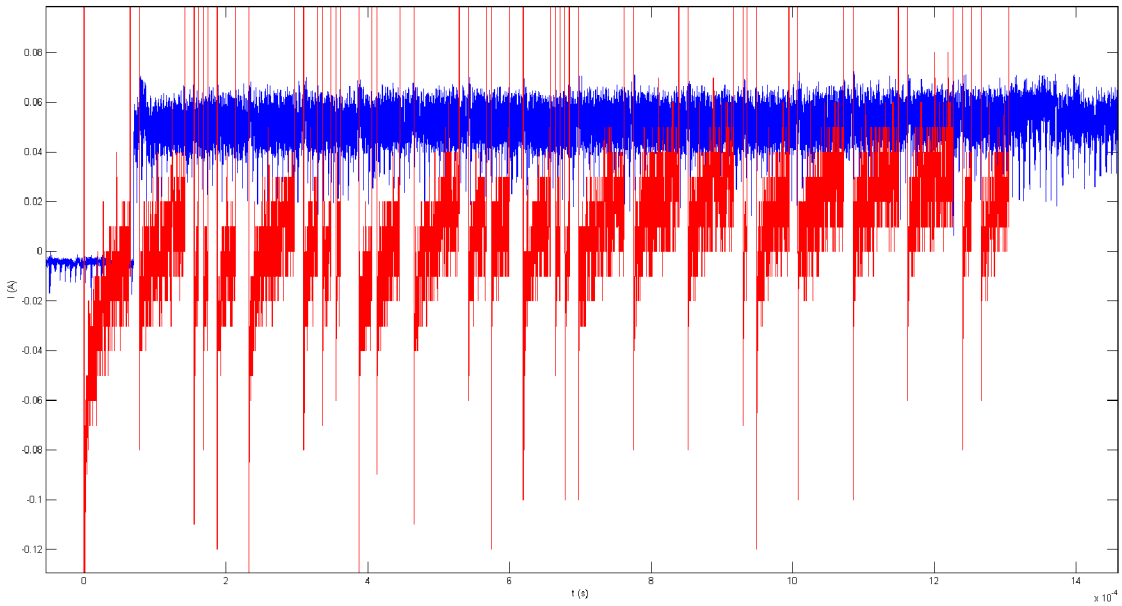
Obr. 6.25: Porovnání proudové spotřeby prvního příkazu - vzorky 3 a 4.



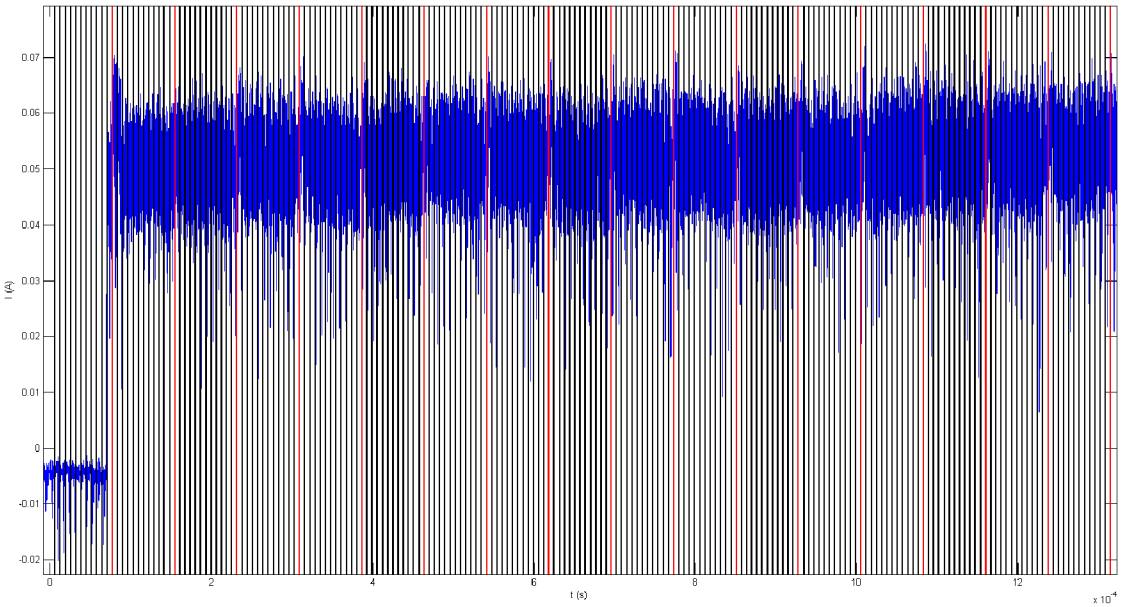
Obr. 6.26: Porovnání proudové spotřeby druhého příkazu - vzorky 1 a 2.



Obr. 6.27: Porovnání proudové spotřeby druhého příkazu - vzorky 3 a 4.



Obr. 6.28: Závislost proudové spotřeby a komunikace.

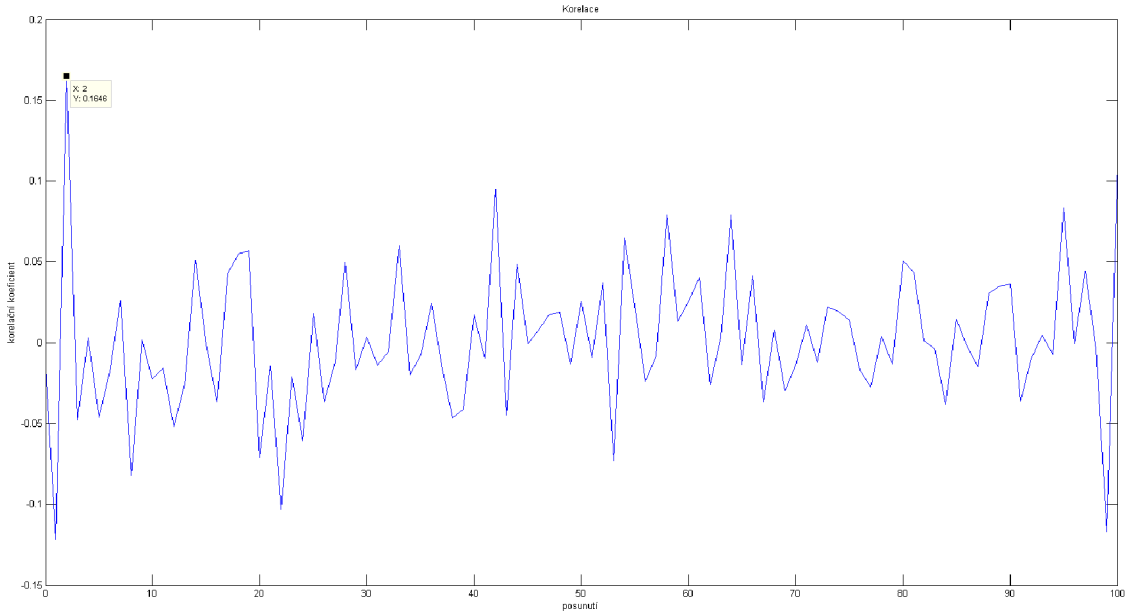


Obr. 6.29: Závislost proudové spotřeby a komunikace s rozdělením po bitu a bajtu.

Při zjišťování podobnosti a možného posunutí vzorků byla použita korelační analýza. Pokud se mezi dvěma vzorky ukáže korelace, je pravděpodobné, že jsou na sobě závislé. Korelace je míra lineární závislosti vzorku. Míru korelace pak vyjadřuje korelační koeficient, který může nabývat hodnot od mínus 1 do plus 1.

Naměřená data jsou korelována mezi původním a posunutým vzorkem. Data musela být před použitím upravena. Ze všech naměřených dat byly vybrány jen potřebné hodnoty vzorků. Rozmezí hodnot bylo určeno z dat získaných na I/O portu. K tomu byla použita funkce *korelace* [8]. Která vyžaduje 4 vstupní parametry. První a druhý je porovnávaný vzorek. Třetí a čtvrtý parametr je číslo nejmenšího a největšího posunu. Testováno od 0 do 100. Pro data z osciloskopu testováno od -100 do 100.

Funkce vrací na výstupu dva vektory R a D. Vektor R určuje délku posunutí a D korelace. Získané hodnoty byly přehledně vykresleny do grafu a z nich získány hodnoty, které jsou zaznamenány, viz tab. 6.8 a 6.9.



Obr. 6.30: Funkce korelace prvního příkazu pro vzorek 1 a 2.

Získané hodnoty s posunem udávají krok posunutí a tomu odpovídající hodnotu korelačního koeficientu. Hodnoty bez posunu jsou přímo získané korelační koeficienty s nulovým posunem. Kde je hodnota funkce korelace blízko jedné, je silná lineární závislost.

Tab. 6.8: Hodnoty korelace příkazů porovnávaných vzorků-data AD622.

	vzorek 1 a 2	vzorek 1 a 3	vzorek 1 a 4	vzorek 2 a 3	vzorek 2 a 4	vzorek 3 a 4
příkaz 1 s posunem	(2; 0.1646)	(37; 0.1485)	(2; 0.1172)	(6; 0.0840)	(31; 0.1959)	(45; 0.1127)
příkaz 1 bez posunu	-0.0120	0.0518	-0.0389	-0.0133	0.0498	0.0465
příkaz 2 s posunem	(78; 0.2215)	(98; 0.3184)	(71; 0.2287)	(6; 0.2365)	(90; 0.2335)	(11; 0.2092)
příkaz 2 bez posunu	0.0474	0.0394	0.0851	-0.0533	-0.0476	-0.0202

V závislosti na provedeném šetření bylo zjištěno, že se jednotlivé pokusy neshodují a jejich průběh je zcela nahodilý. Jednotlivé pokusy odhalily nesouvislé hodnoty korelačních koeficientů, které se vždy blížily k 0. Tyto výsledky byly potvrzeny jak v rámci posouzení pokusů s posunu (tj. příkaz 1 a příkaz 2 s posunem z tab. 6.8), stejně tak po zhodnocení statistiky zjištěných hodnot korelačních koeficientů v rámci pokusů bez posunu (tj. příkaz 1 a 2 bez posunu). Na základě tohoto statistického šetření tedy můžeme konstatovat, že mezi těmito daty nebyla nalezena žádná lineární závislost. Tímto byl tedy potvrzen prvotní předpoklad o neexistenci jakékoli korelace mezi zkoumanými daty.

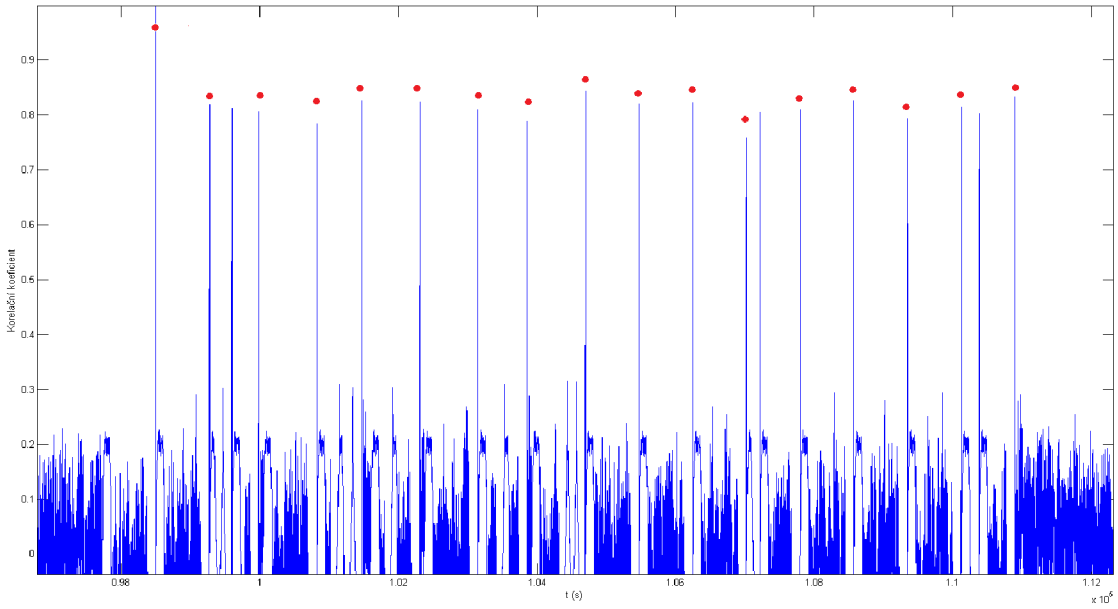
Tab. 6.9: Hodnoty korelace prvního příkazu-data osciloskop.

	celý příkaz 1 s posuvem	celý příkaz 1 bez posuvu	část příkazu 1 s posuvem	část příkazu 1 bez posuvu
vzorek 1 a 2	(70; 0.6178)	0.5919	(-10; 0.0701)	0.0637

Mezi daty získanými z osciloskopu se projevila větší závislost korelačních koeficientů, což bylo způsobeno především zvýšením počtu naměřených dat. V šetření pro celý příkaz 1 byla nalezena určitá závislost mezi porovnávanými daty. U šetření části příkazu, což odpovídá hodnotám pouze zpracovávaných dat bez příkazu a odpovědi, nebyla mezi daty nalezena opět žádná lineární závislost.

Korelace byla zjišťována také u části spotřeby, která byla opakovaně obsažena v datech APDU příkazu. Část začíná deseti bity s hodnotou 0 a končí dvěma bity s hodnotou 1. Další pokus byl proveden pouze s dvěma bity s hodnotou 1. Jsou to dva po sobě jdoucí stop bity. Po testování velkého množství možností můžu konstatovat, že mezi těmito daty nebyla nalezena žádná lineární závislost. Tímto byl tedy potvrzen prvotní předpoklad o neexistenci jakékoli korelace mezi zkoumanými daty.

Podobný postup byl aplikován i na data naměřená na I/O portu. Z dat byla vybrána část celé komunikace a část, kdy je zasílán příkaz. Tato data byla porovnávána s částí, která odpovídala dvěma po sobě jdoucím stop bitům. Závislost dat byla ověřena upravenou korelační funkcí, viz obr. 6.31. Označené korelační koeficienty červenou tečkou odpovídají hodnotám, kdy se v každém přenášeném bajtu na konci nachází dva ukončující stop bity. V zachycené komunikaci je zasláno 17 bajtů a to odpovídá 17 zachyceným a označeným koeficientům, které mají stejný časový odstup. Na těchto datech podrobených analýze se projevila existence silné závislosti, která byla očekávána. Tím byla ověřena správnost použité korelační funkce.



Obr. 6.31: Upravená funkce korelace pro závislost v komunikaci.

Výsledky ukázaly, že nebyla nalezena žádná závislost mezi daty, které byly odposlechnuty přes napěťově proudový postranní kanál testované čipové karty. Karta používá velmi dobrá protiopatření, která jí zajišťují bezpečnost před útoky využívajících postranních kanálů. Testovaný čip karty je určen pro použití ve zvláště bezpečných aplikacích, přičemž vlastní protiopatření proti SPA, DPA, EMA a DFA útokům. Implementované protiopatření se mi s dostupným vybavením, ke kterému jsem měl přístup v průběhu zpracování diplomové práce, nepodařilo narušit.

Nejlepším softwarovým protiopatřením proti jednoduché výkonové analýze se zdá být co možná nejvíce konstantní běh výpočtu anebo zajištění, že nebude výpočet ovlivňován daty, se kterými se při výpočtu pracuje. Byly použity implementace instrukce, jejichž výkonové charakteristiky nejsou tak snadno patrné. Dalším možným protiopatřením je použití algoritmů, které obsahují náhodné prvky, jež ovlivňují náhodně prováděný výpočet. Což ztížilo potřebné odstraňování šumu, které se provádí průměrováním při analýze napěťově proudového postranního kanálu.

Hardwarová protiopatření jsou často nedostatečně popsána. Výrobci čipových karet neradi poskytují detaily o těchto hardwarových protiopatřeních, které využívají u svých produktů. Jednou z možností ochran je zajistit dostatečné vyvážení spotřeby nebo také desynchronizace vnitřních hodin čipu, to znamená, že cykly budou prováděny různou dobu. Tyto opatření lze narušit měřícím zařízením o dostatečné velké vzorkovací frekvenci. Cílem opatření není většinou útok úplně znemožnit, ale znesnadnit a to do takové míry, aby se cena řádově posunula na vyšší úroveň než je cena utajovaných informací na čipové kartě.

K dosažení přesnějších a více vypovídajících výsledků je nutné mít přístup k měřicím přístrojům, které umožní signál vzorkovat s vysokou frekvencí nebo mít k dispozici výkonnější pracovní stanici a lepší měřící kartu. Bylo by zajímavé hledat v měřených datech předpřipravené instrukce o známém časovém průběhu, které se cyklicky opakují nebo otestovat aplikace nahrané na čipovou kartu, které vyžadují manipulaci s pinem, jako je např. elektronická peněženka. Použít čtečku, která komunikuje s počítačem pomaleji přes sériový port COM (RS232), protože k zachycení přenášených dat bude dostačovat nižší vzorkovací frekvence. Mít přístup k placeným verzím softwaru, který je určen k práci s čipovými kartami. Softwarové vybavení vyvíjené výrobcem karty JCS Suite v 3.0 umožňovalo provádět více operací automaticky s čipovou kartou než použitý software JSmart Card Explorer, ale k dispozici byla pouze jedna licence na pracovní stanici v laboratoři. To nedovolilo využít JCS Suite v 3.0 při měření na osciloskopu.

7 Závěr

Cílem diplomové práce bylo seznámit se s používanými čipovými kartami a s kryptografickými algoritmy. Prostudovat a popsat známé metody útoků na čipové karty pomocí postranních kanálů a poukázat na tyto formy úniku informací. Při měření napájecích charakteristik čipové karty během komunikace bylo zapotřebí také odvodit změny napájení v závislosti na probíhajících výpočtech. Navrhnout formu monitorování komunikace karty a čtečky, postup odposlechu a analýzy zpracovávaných informací.

Teoretická část se postupně věnuje typům, vlastnostem, komunikaci, bezpečnosti a postranním kanálům čipových karet. Dále se zabývá vznikem a měřením napěťově proudového postranního kanálu a v neposlední řadě popisuje použité laboratorní pracoviště. Byly vytvořeny laboratorní pracoviště, které umožňovaly měření napěťově proudového postranního kanálu čipové karty a monitorovali probíhající komunikaci mezi čipovou kartou a terminálem. Pro potřeby měření byla využita modifikovaná čtečka OMNIKEY. Pracovní stanice s měřící kartou AD622 a osciloskop MSO9104A. Pro umožnění měření a zpracování naměřených dat byl použit matematický program Matlab a Simulink. V Simulinku byl následně navržen model, který umožnil měření a sběr dat. Analýza dat je velmi účinným nástrojem při útocích na čipové karty, protože někdy dokáže odhalit některé unikající informace, které nejsou hned na první pohled viditelné. Pro analýzu byl vybrán matematický software Matlab, protože je přehledný, rychlý, podporuje uživatelské M-soubory a v neposlední řadě umožňuje také snadnou manipulaci s naměřenými daty a grafy. Z důvodů nekorektního chování pracovní stanice s měřící kartou AD622 nebylo možné se přiblížit maximálním technickým parametrům měřící karty, které by byly pro potřeby měření komunikace dostačující. Maximum udávané výrobcem je pro čtyři A/D vstupy 400 KHz a 625 KHz pro jeden A/D vstup. Měření bylo úspěšné pro hodnoty 25 a 50 KHz při použití tří A/D vstupů. Komunikace byla zachycena při použití pouze jediného A/D vstupu při vzorkovací frekvenci 100 KHz. Dosažené hodnoty však nejsou pro přesné měření dostačující, proto byl k měření použit osciloskop MSO9104A. Ze zachycené a následně analyzované komunikace osciloskopem je jasně patrné, že analýza přenášených dat byla úspěšná. Získaná data odpovídají zaslaným APDU příkazům a odpovědím, co obdržel použitý software.

Detailním zkoumáním spotřeby karty při zpracování jednotlivých APDU příkazů pomocí grafických závislostí a korelačních koeficientů nebyla zjištěna žádná souvislost. Závislost se neprojevila ani u vybraných částí spotřeby při zpracování dat. Pouze na začátku komunikace se při zpracování nově příchozího bajtu se opakovaně projevil mírný nárůst spotřeby.

Implementace všech kryptografických algoritmů jak symetrických, tak asymetrických, jsou náchylné na SPA a DPA útok. Napěťově proudovou analýzou lze napadnout běžně používané kryptografické algoritmy. Úspěch útoku se odvíjí od použité implementace. SPA a DPA útoky se zakládají na měření spotřeby zařízení, které poskytne potřebné informace k odvození vzájemných vztahů, čímž poruší předpoklady a záruky bezpečných algoritmů. Při zkoumání napěťově proudového kanálu čipové karty byla testována karta od firmy G&D, typ Sm@rtCafe Expert 4.0. Čip karty je určen pro použití ve zvláště bezpečných aplikacích a vlastní protiopatření proti SPA, DPA, EMA a DFA útokům. Tohle protiopatření se mi s dostupným vybavením, ke kterému jsem měl přístup, nepodařilo narušit. Karta používá velmi dobré protiopatření, které jí zajišťují bezpečnost před útoky využívajících postranních kanálů.

Literatura

[1] A cryptovision whitepaper. In *Side Channel Attacks on Smart Cards* [online]. Gelsenkirchen : [s.n.], 2009 [cit. 2010-12-04]. Dostupné z WWW: <http://www.cryptovision.com/fileadmin/media/documents/Whitepaper_Produkte/01-Whitepaper-Technical-Side-Channel_EN.pdf>.

[2] BEJČEK, Ludvík. *Měření v elektrotechnice* [online]. Brno : Vysoké učení technické v Brně, 200?. 241 s. Skripta. Vysoké učení technické v Brně, FEKT . Dostupné z WWW: <http://wwwo.utee.feec.vutbr.cz/CZ/Predmety/BMVA/bmva.htm>.

[3] BILLY, Billy. Http://www.tcs.hut.fi/Studies/T-79.514/slides/S5.Brumley-*comp128.pdf* [online]. 2004 [cit. 2011-03-01]. A3/A8 & COMP128 . Dostupné z WWW:<http://www.tcs.hut.fi/Studies/T-79.514/slides/S5.Brumley-omp128.pdf>.

[4] BUCHMÜLLER, H.-U. *Infineon Technologies AG Security and Chipcard ICs* [online]. [s.l.] : Infineon Technologies AG, 2006 [cit. 2011-04-22]. Dostupné z WWW: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte03/0399b_pdf.pdf?__blob=publicationFile>.

[5] ČÍŽEK, Jakub. *Www.zive.cz* [online]. 2009-09-06 [cit. 2011-03-01]. Superpočítače způsobují kryptografům problémy. Dostupné z WWW: <http://www.zive.cz/clanky/superpocitace-zpusobuji-kryptografum-problemy/sc-3-a-145121/default.aspx>.

[6] Differential Power Analysis. In KOCHER, Paul ; JAFFE, Joshua; JUN, Benjamin. *Differential Power Analysis*[online]. San Francisco : [s.n.], [1998] [cit. 2010-12-04]. Dostupné z WWW: <http://www.cryptography.com/public/pdf/DPA.pdf>.

[7] FIPS 140. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, last modified on 24 únor 2011 [cit. 2011-03-01]. Dostupné z WWW: <http://en.wikipedia.org/wiki/FIPS_140>.

[8] FRANO, Petr. *Zpracování dat při časové a výkonové analýze čipových karet* [online]. Brno : Masarykova univerzita, 2006. 39 s. Diplomová práce. Masarykova univerzita v Brně Fakulta informatiky. Dostupné z WWW: <http://is.muni.cz/th/39349/fi_b/Bakalarska_prace-tcq.pdf>.

[9] HAGHIR, Yahya; TARANTINO, Thomas. *Smart Card Manufacturing*. Munich : John Wiley & Sons, 2002. 221 s. ISBN 0471497673.

[10] *Http://primianotucci.com* [online]. 2007 [cit. 2011-03-01]. JSmartCardExplorer : Cross-platform, low level APDU smart card development. Dostupné z WWW: <http://primianotucci.com/default.php?view=113>.

[11] *Http://www.hidglobal.com* [online]. 2011 [cit. 2011-03-01]. OMNIKEY 3121 USB. Dostupné z WWW: <http://www.hidglobal.com /prod_detail.php?prod_id=188>.

[12] *Http://www.humusoft.cz* [online]. 2011 [cit. 2011-03-01]. Simulace a modelování dynamických systémů, Model-Based Design. Dostupné z WWW: <http://www.humusoft.cz/produkty/matlab/simulink/>.

[13] *Http://www.humusoft.cz* [online]. 2011 [cit. 2011-03-01]. Real Time Toolbox. Dostupné z WWW: <http://www.humusoft.cz/produkty/rtt/>.

[14] *Http://www.humusoft.cz* [online]. 2011 [cit. 2011-03-01]. Měřicí karty. Dostupné z WWW: <http://www.humusoft.cz/produkty/datacq/>.

[15] *Http://www.humusoft.cz* [online]. 2011 [cit. 2011-03-01]. AD622. Dostupné z WWW: <http://www.humusoft.cz/produkty/datacq/ad622/>.

[16] *Http://www.humusoft.cz* [online]. 2011 [cit. 2011-03-01]. AD 622 DATA ACQUISITION CARD USER'S MANUAL. Dostupné z WWW: <http://www2.humusoft.cz/www/datacq/manuals/ad622um.pdf>.

[17] *Http://www.mathworks.com* [online]. 2011 [cit. 2011-03-01]. MATLAB - The Language Of Technical Computing. Dostupné z WWW: <http://www.mathworks.com/products/matlab/>.

[18] KARBAN, Pavel . *Výpočty a simulace v programech Matlab a Simulink*. Brno : Computer Press, 2006. 220 s. ISBN 978-80-251-1448-3.

[19] KOC, Cetin Kaya. *Cryptographic Engineering* [online]. Tophane : Springer, 2009 [cit. 2010-12-03]. Dostupné z WWW: <http://www.springerlink.com/content/978-0-387-71816-3#section=131769&page=1>. ISBN 978-0-387-71817-0.

[20] Low Cost Attacks on Smart Cards. In MATTHEWS, Adam. *The Electromagnetic Side-Channel* [online]. [s.l.] : [s.n.], 2006 [cit. 2010-12-04]. Dostupné z WWW: <http://www.ngssoftware.com/Libraries/Documents/09_06_Low_Cost_Attacks_on_Smart_Cards_-_The_Electromagnetic_Side-Channel.sflb.ashx>.

[21] MANGARD, Stefan; OSWALD, Elisabeth; POPP, Thomas. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. GRAZ : Springer, 2007. 337 s. ISBN 978-0-387-30857-9.

[22] MATĚJKA, Jiří . *Útoky postranními kanály na čipové karty* [online]. Brno : Vysoké učení technické v Brně, 2010. 88 s. Diplomová práce. Vysoké učení technické v Brně, FEKT . Dostupné z WWW: <http://www.vutbr.cz/www_base /zav_prace_soubor_verejne.php?file_id=28101>.

[23] MAYES, Keith E.; MARKANTONAKIS, Konstantinos. *Smart Cards, Tokens, Security and Applications*. London : Springer, 2008. 392 s. ISBN 978-0-387-72197-2.

[24] NOUZÁK, Josef. *Postranní kanály mikroprocesorů* [online]. Praha : České vysoké učení technické v Praze, 2007. 48 s. Bakalářská práce. České vysoké učení technické v Praze, Fakulta elektrotechnická. Dostupné z WWW: <https://dip.felk.cvut.cz/browse/pdfcache/nouzaj1_2007bach.pdf>.

[25] RANKL, Wolfgang; EFFING, Wolfgang. *Smart Card Handbook*. Fourth Edition. Munich : John Wiley & Sons, 2010. 1088 s. ISBN 978-0-470-74367-6.

[26] RANKL, Wolfgang. *Smart Card Applications*. Chichester : John Wiley & Sons, 2007. 217 s. ISBN 978-0-470-05882-4.

[27] RANKL, Wolfgang Overview about Attacks on Smart Cards. In *Smart Card Handbook* [online]. 3rd edition. Munich : John Wiley & Sons, 2003 [cit. 2010-12-04]. Dostupné z WWW: http://www.wrankl.de/SCH/Attacks.pdf

[28] Rozšířený abstrakt. In HANÁČEK, Petr; MATYÁŠ, Vašek. *Čipové karty v informačních systémech* [online]. Brno : [s.n.], 2003 [cit. 2010-12-04]. Dostupné z WWW: <http://www.fit.vutbr.cz/~hanacek/papers/Datakon03.pdf>.

[29] *Sm@rtCafé® Expert 4.0* [online]. Munchen : Giesecke & Devrient GmbH, 2008 [cit. 2011-04-15]. Dostupné z WWW: <http://www.gi-de.com>.

[30] WEIKMANN, Franz Smartcards and Side Channels Attacks. In *How do Side Channel Attacks Affect the Software Development Process?* [online]. Bochum : [s.n.], 2003 [cit. 2010-12-04]. Dostupné z WWW:http://eref.uqu.edu.sa/files/Others/Elliptic%20Curves/Scalar%20Multiplication/How%20do%20Side%20Channel%20Attacks%20Affect%20the%20Software%20Development.pdf

[31] White Paper. In BAR-EL, Hagai. *Ntroduction to SideChannel Attacks* [online]. Netanya : [s.n.], [200?] [cit. 2010-12-04]. Dostupné z WWW:<http://www.discretix.com/PDF/Introduction%20to%20Side%20Channel%20Attacks.pdf>.

Seznam použitých zkratek a symbolů

ABS	acrylonitrile butadiene styrene
AES	Advanced Encryption Standard
AID	Application Identifier
APDU	application protocol data unit
ATR	answer to reset
BGT	Blok Guard Time
BIO API	Biometric Application Programming Interface
BWT	Block Waiting Time
CISC	complex instruction set computer
CLA	class
CLK	clock
CMOS	Complementary Metal-Oxide-Semiconductor
CPU	central processing unit
CRC	cyclic redundancy check
CSV	Comma-separated values
CT-API	CardTerminal Application Programming Interface
CWT	Character Waiting Time
DAP	Data Authentication Pattern
DEMA	Differential electromagnetic analysis
DES	Data Encryption Standard
DMA	direct memory access
DPA	Differential power analysis
EC2	Amazon Elastic Compute Cloud
EEPROM	electrically erasable programmable read-only memory
EMA	Electromagnetic analysis
ETU	elementary time unit
FIPS	Federal Information Processing Standards
G&D	Giesecke & Devrient
GSM	Global System for Mobile Communications
HO-DPA	High Oder DPA
I/O	input/output
I^2C	inter-integrated circuit
ID	identifier
IEC	International Electrotechnical Commission
INS	instruction
ISO	International Organization for Standardization
LACAL	Laboratory for cryptologic algorithms
Lc	length command
Le	expected length
MAT	soubor Matlabu pro ukládání dat
MD5	Message-Digest algorithm 5
MMC	MultiMediaCard
NFC	near field communication
NIST	National Institute of Standards
NPU	numeric processing unit
NRZI	non return to zero inverted
OCF	Open Card Framework

OP	Open Platform
P1, P2, P3	parameter 1, 2, 3
PA	Power analysis attacks
PC	polycarbonate
PCI	Peripheral Component Interconnect
PC/SC	Personal Computer/Smart Card
PET	polyethylene terephthalate
PNG	Portable Network Graphics
PPS	protocol parameter selection
PVC	polyvinyl chloride
RAM	random access memory
R_i	vnitřní odpor
RISC	reduced instruction set computer
ROM	Read-Only Memory
RSA	Rivest, Shamir and Adleman Algorithm
SEMA	Simple electromagnetic analysis
SHA-1	Secure Hash Algorithm-1
SIM	subscriber identity module
SPA	Simple power analysis
SRAM	static random access memory
SW1, SW2	status word 1, 2
SWP	Single-wire Protocol
TA	Timing attack
TPDU	transmission protocol data unit
TTL	transistor-transistor-logic
UART	universal asynchronous receiver transmitter
UICC	universal integrated chip card
U_{CPU}	napětí na mikroprocesoru
U_{mer}	měřené elektrické napětí
U_{zdr}	napětí na zdroji
USB	Universal Serial Bus
UV	ultraviolet
V_{in}	napětí na vstupu
V_{out}	napětí na výstupu
V_{dd}	napájecí napětí

Přílohy

Obsah CD

DP.pdf – text diplomové práce ve formátu Adobe Acrobat Reader

Power smart card analysis final – model vytvořený v Simulinku

Naměřená data

- Data AD622
- Data osciloskop MSO9104A

Vybrané obrázky