VĚDECKÉ SPISY VYSOKÉHO UČENÍ TECHNICKÉHO V BRNĚ

Edice PhD Thesis, sv. 445

ISSN 1213-4198

Ing. Petr Daněček

Útoky na kryptografické moduly

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

Ing. Petr Daněček

ÚTOKY NA KRYPTOGRAFICKÉ MODULY

ATTACKS ON CRYPTOGRAPHIC MODULES

ZKRÁCENÁ VERZE PH.D. THESIS

Obor:	Teleinformatika
Školitel:	Doc. Ing. Václav Zeman, Ph.D.
Oponenti:	Doc. Ing. Jiří Sýkora, CSc. Ing. Petr Hujka, Ph.D.
Datum obhajoby:	10. 1. 2008

Klíčová slova

Postranní kanál, kryptografický modul, jednoduchá výkonová analýza SPA, diferenční výkonová analýza DPA, kryptoanalýza.

Key words

Side Channel, Cryptographic Module, Simple Power Analysis SPA, Differential Power Analysis DPA, Crypto analysis.

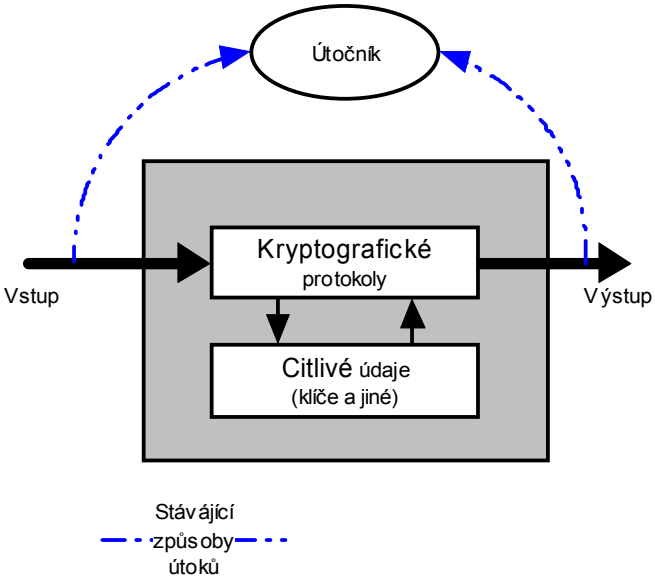
Dizertační práce je uložena na Vědeckém oddělení, Fakulta elektrotechniky a komunikačních technologií, Vysoké učení technické v Brně, Údolní 53, Brno.

ISBN 978-80-214-3484-4
ISSN 1213-4198

OBSAH

1 ÚVOD

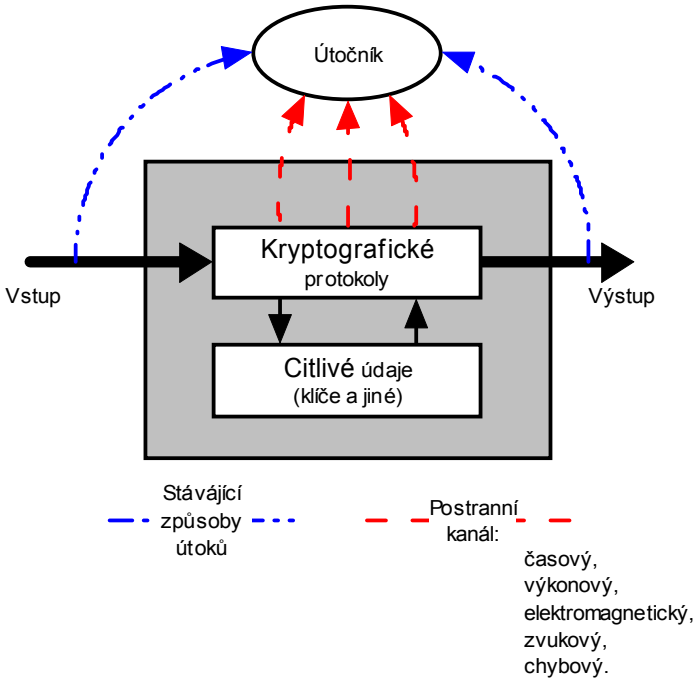
Vývoj bezpečných způsobů výměny informací probíhá nepřetržitě po řadu let. Byla navržena celá řada bezpečnostních norem, ve kterých byly aplikovány kvalitní šifrovací (symetrické a asymetrické) a další kryptografické algoritmy, jejichž bezpečnost je po teoretické stránce dostatečně ověřena a při použití šifrovacích klíčů o přiměřené délce je lze považovat za bezpečné. Dosavadní pohled na možná bezpečnostní rizika těchto systémů směřoval především k rozlomení šifrovacích protokolů a algoritmů. Proti v současnosti používaným šifrovacím algoritmům je tento způsob neefektivní a časově náročný. Model konvenčního způsobu vedení útoku na kryptografický modul je na obr. 1.



Obr. 1. Konvenční model útoku na kryptografický modul

Při reálném provozu kryptografický modul poskytuje své služby, a to za pomoci komunikace se svým okolím. Předpokladem správného návrhu modulu je, že veškeré citlivé informace zůstávají během této činnosti uvnitř kryptografického modulu. Komunikace s okolím smí probíhat pouze po přesně specifikovaných rozhraních a v rámci povolených komunikačních protokolů. Modul musí zamezit jakékoliv jiné komunikaci.

Operace probíhající uvnitř kryptografického modulu lze stručně nazvat jako činnost kryptografického modulu. Při své činnosti kryptografický modul produkuje tepelné a jiné záření, spotřebovává výkon ze zdroje atd. Tyto produkty mohou být provázány (korelovány) s průběhem operací uvnitř kryptografického modulu. Takto dochází k nežádoucímu vynesení citlivých informací mimo modul, jedná se tedy o nežádoucí komunikaci s okolím. Vznikají postranní kanály.



Obr. 2. Rozšířený model útoku na kryptografický modul zahrnující postranní kanály

Útoky postranním kanálem (*Side Channel Attacks*) jsou zcela novou koncepcí vedení útoku na kryptografický modul. Útok postranním kanálem je veden na chyby v implementaci šifrovacího algoritmu. Citlivé informace jsou získány ze zdánlivě bezvýznamných odezev systému jako jsou chybová hlášení, doby trvání výpočtů, proudové či napěťové poměry v systému, elektromagnetické vyzařování a případně i další odezvy, které mohou být i uměle vyvolané. Tyto útoky jsou založeny na korelaci vnitřních stavů vznikajících při zpracování kryptografických operací a údaji unikajícími z modulu na fyzické úrovni. Model útoku na kryptografický modul s využitím postranních kanálů je zobrazen na obr. 2. Běžně používaný je také termín útok na implementaci.

Postranní kanály zcela mění celkový pohled na bezpečnost systému. Již nestačí zvolit kvalitní šifru, ale je nezbytné velkou pozornost věnovat i její implementaci. Jakákoliv obecná metodika návrhu kryptografického modulu odolného vůči útokům postranním kanálem v současnosti v podstatě neexistuje.

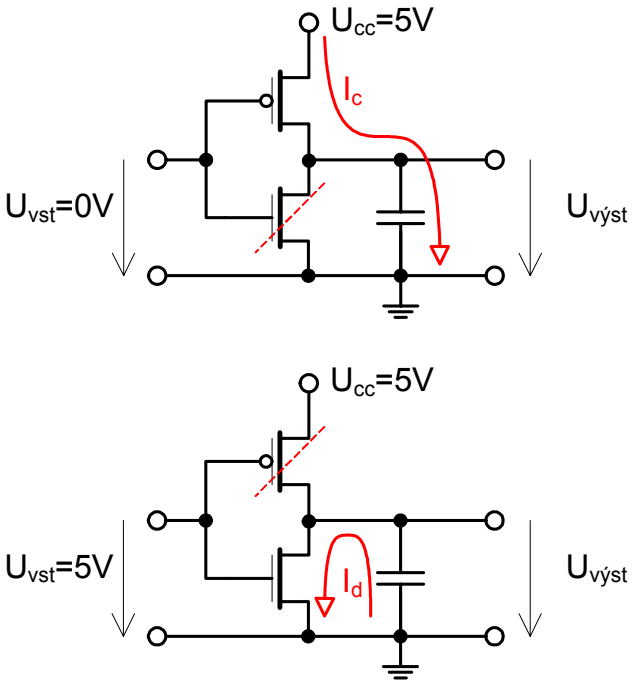
2 PŘEHLED SOUČASNÉHO STAVU PROBLEMATIKY

2.1 ÚTOK VÝKONOVÝM POSTRANNÍM KANÁLEM

Z detailního pozorování výkonové spotřeby elektronického zařízení je zřejmé, že jeho spotřeba není s časem konstantní. Na první pohled je patrné zvlnění podobné nahodilému šumu. Nahodilost je však pouze zdánlivá, neboť šum je závislý na změnách stavu elektronických součástek uvnitř zařízení. Vzhledem k velkému množství těchto součástek je pak výsledný průběh výkonové spotřeby zdánlivě

nahodilý šum. Změny výkonové spotřeby vznikají na úrovni elementárních elektronických součástek, jako je např. tranzistor.

Většina moderních kryptografických zařízení je založena na technologii CMOS (*Complementary Metal Oxide Semiconductor*). Základním stavebním prvkem logiky založené na CMOS technologii je invertující člen, viz obr. 3.



Obr. 3. Model invertoru logiky založené na CMOS
a) Nabíjení parazitní kapacity b) Vybíjení parazitní kapacity

Invertor obsahuje dva tranzistory zapojené jako spínače řízené napětím. Princip je zřejmý: pokud je vstupní napětí v logické úrovni „1“, je otevřen dolní tranzistor a horní uzavřen. Naopak je tomu, pokud je vstupní napětí v logické úrovni „0“. V obou těchto stabilních stavech je výkonová spotřeba malá, ale nestejná.

Výkonová špička nastává při přechodu mezi těmito stavy. V ten moment jsou na krátký čas otevřeny oba tranzistory a napájení je zkratováno proti zemi. Následně vzniká proudová špička. Dokonce i v klidovém stavu tranzistory odebírají malý proud ze zdroje a ten se mění v teplo a záření. Dominantní zdroj výkonových změn je vybíjení a nabíjení interní kapacitní zátěže připojené na výstupy. Zdroje výkonových změn jsou:

- tepelné vyzařování tranzistorů v klidovém stavu a příslušný proudový odběr (různý pro stav „otevřeno“ a „zavřeno“),
- proudové špičky při přechodech mezi těmito stavy,
- proudové změny při nabíjení a vybíjení parazitní kapacitní zátěže připojené sběrnice.

Všechny tři jsou diskutovány v literatuře [1].

2.2 KORELACE PRŮBĚHŮ VÝKONOVÉ SPOTŘEBY S OPERACEMI A OPERANDY ZPRACOVÁVANÝMI ŠIFROVACÍM ALGORITMEM

V kryptografických modulech vybavených mikroprocesory dochází při zpracování programu ke spínání řady tranzistorů. Tyto stavy „sepnuto“, „vypnuto“ a jejich změny jsou přímo závislé na prováděném programu. Tak dochází k nežádoucímu zanesení informace o vnitřním stavu programu do výkonové spotřeby. V případě zpracovávání nahodilých instrukcí by výkonová spotřeba byla nepravidelná.

Kryptografické algoritmy jsou založeny na pravidelných cyklech, ve kterých se pracuje s citlivými informacemi (jako např. rundy u DES algoritmu). To vnáší do výkonové spotřeby pravidelně se opakující vzory. Z nich je možno na základě obecné znalosti šifrovacích algoritmů přesně určit typ konkrétního pozorovaného algoritmu a sledovat jednotlivé fáze průběhu zpracování. Z drobných odchylek v pravidelně se opakujících fázích je možné získat přímo citlivé informace. Této techniky útoku je použito při jednoduché výkonové analýze SPA (*Simple Power Analysis*).

V průběhu zpracování programu jsou pravidelně čtena a zapisována data z a do paměti. Přenášena jsou po datové sběrnici. Vzhledem ke kapacitním vlastnostem této sběrnice dochází k pravidelnému nabíjení a vybíjení cest datové sběrnice. Tyto jevy jsou opět zaneseny do výkonové spotřeby. Jsou mnohem méně patrné a jejich využití pro útok vyžaduje využití pravděpodobnostních výpočtů a jiných sofistikovaných matematických postupů. Tato technika útoku je pak použita při diferenční výkonové analýze DPA (*Differential power analysis*).

3 CÍLE DIZERTAČNÍ PRÁCE

Za jeden z nejvýznamnějších postranních kanálů lze považovat výkonový. Na něm je založena řada nebezpečných útoků zaměřených především proti menším kryptografickým modulům, jsou to například čipová karta nebo USB token. Dizertační práce je přímo zaměřena na studium výkonového postranního kanálu.

Útok výkonovým postranním kanálem je založen na průniku útočníka do napájecího systému kryptografického modulu. Tato skutečnost je zpravidla opomíjena a rozbor napájecího systému ve spojitosti s výkonovým postranním kanálem v dostupné literatuře chybí. Často je při popisu útoku mylně předpokládáno, že výkonový průběh je měřen přímo na napájecím vývodu pouzdra integrovaného obvodu. Vliv napájecího systému na získané výsledky není brán v potaz.

Hlavním cíle dizertační práce lze shrnout do tří etap: podrobné studium výkonového postranního kanálu, vytvoření experimentálního simulačního pracoviště a doplnění chybějících informací v opomíjené oblasti vlivu napájecích systémů na bezpečnost kryptografických modulů.

Naplnění hlavních cílů ústí v naplnění následujících bodů.

Podrobné studium výkonového postranního kanálu. Cíle této etapy řešení dizertační práce jsou.

- Vymezit pojem kryptografický modul, popsat problematiku jeho návrhu a také problematiku implementace kryptografických algoritmů a protokolů do tohoto modulu. V souvislosti s tím musí text práce obsahovat i popis těchto algoritmů a to z důvodu jak jejich implementace, tak i pochopení výkladu útoků postranním kanálem.
- Provést podrobnou analýzu známých útoků založených na výkonovém postraním kanálu, přičemž důraz bude kladen na diferenční výkonovou analýzu.

Vytvoření experimentálního simulačního pracoviště. Cíle této etapy řešení dizertační práce jsou.

- Vytvořit experimentální pracoviště pro simulaci útoků výkonovým postranním kanálem. Vytvoření tohoto pracoviště zahrnuje realizaci modelu kryptografického modulu, implementaci kryptografických protokolů, návrh a popis měřicího řetězce, vytvoření programového vybavení pro zpracování měřených výsledků atd. Součástí této etapy je i popis postupu měření.

Doplnění chybějících informací v opomíjené oblasti vlivu napájecích systémů na bezpečnost kryptografických modulů. Cíle této etapy řešení dizertační práce jsou.

- Provést rozbor napájecího systému kryptografických modulů.
- Prostudovat souvislost mezi napájecím systémem kryptografického modulu a uskutečnitelností útoku výkonovým postranním kanálem.
- Provést experimentální měření výkonových průběhů v klíčových místech napájecího systému modelu kryptografického modulu.
- Vyhodnotit dopad napájecího systému na průběhy získané měřením v klíčových místech.

4 JEDNODUCHÁ VÝKONOVÁ ANALÝZA

Cílem kapitoly je prostudovat jednoduchou výkonovou analýzu. Kapitola popisuje typické příklady problematických částí algoritmů náchylných na útok touto analýzou. Naznačena jsou protiopatření vedoucí ke ztížení útoku tohoto typu.

Jednoduchá výkonová analýza SPA (Simple Power Analysis) je technika útoku výkonovým postranním kanálem založená na přímém pozorování průběhu výkonové spotřeby kryptografického modulu. Tato technika nevyužívá statistických metod nebo jiných matematických postupů [2], [3], [4].

Útok jednoduchou výkonovou analýzou je vhodný proti kryptografickým protokolům, ve kterých je průběh prováděného programu silně závislý na zpracovávaných datech (obsahuje řadu podmíněných operací závislých na datech). Provedení či neprovedení řady instrukcí vykonávaného programu je tak přímo závislé na zpracovávaných datech. Každá instrukce má charakteristický průběh

výkonové spotřeby. Pozorováním výkonové spotřeby je určen sled provedených instrukcí závislých na zpracovávaných datech. Typické příklady takovýchto algoritmů s popisem jejich problematických částí obsahuje následující text.

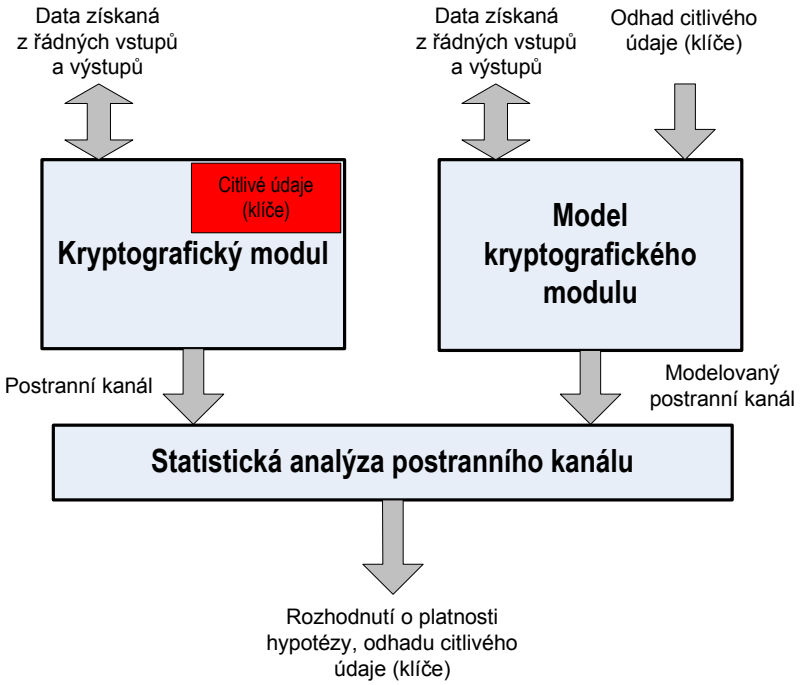
- Klíčové hospodářství. Řada algoritmů, např. šifrovací algoritmus DES, připravuje pro každou iteraci rundovní šifrovací klíče. Konkrétně u šifrovacího algoritmu DES je to ve dvou 28bitových posuvných registrech. Při rotaci v daném registru je poslední bit vysunut mimo registr a na základě jeho hodnoty je rozhodnuto o nastavení prvního bitu v registru (cyklický registr). Tato podmíněná operace má výraznou charakteristiku v průběhu výkonové spotřeby.
- Permutace. Šifrovací algoritmus DES, ale i řada jiných algoritmů, je založena na řadě permutací. Programový kód permutací přeložený do instrukčních sad cílových mikroprocesorů vnáší do průběhů výkonové spotřeby značné charakteristiky v závislosti na datech do permutací vstupujících.
- Porovnávání. Řada algoritmů obsahuje programový kód pro porovnávání řetězců nebo částí operační paměti. Tyto porovnání jsou opět založena na podmíněných větveních programu, která způsobují významné změny nejen ve výkonovém postranním kanálu, ale také v časovém a dalších kanálech.
- Násobení. Různé typy modulárního násobení jsou jedním z nejvýznamnějších zdrojů informací unikajících řadou postranních kanálů. Informace v kanálu jsou silně korelovány s hodnotami zpracovávaných dat a způsob úniku těchto dat je závislý na konkrétní realizaci procesu násobení.
- Umocňování. Principiálně jednoduché funkce modulárního umocňování jsou založeny na postupném procházení exponentu v iteračních krocích. V závislosti na hodnotě bitu exponentu příslušného dané iteraci jsou nebo nejsou provedeny požadované operace a následné násobení. Na základě hodnoty exponentu je tak program větven v každé iteraci do zcela jiné cesty, je zpracován jiný kód s charakteristickou dobou výpočtu a podpisem v průběhu výkonové spotřeby. Množství prosakující informace roste s počtem exponentů.

Zvláštním případ jednoduché výkonové analýzy je založen na nalezení silné závislosti mezi průběhem výkonové spotřeby a Hammingovou váhou zpracovávaných dat (Hammingova váha reprezentuje počet nenulových bitů ve slově) [5]. Z informace o Hammingově váze zpracovávaných dat, která uniká výkonovým postranním kanálem, je možné tato data rekonstruovat. Tento způsob jednoduché výkonové analýzy je efektivní proti systémům zpracovávajícím data v menších jednotkách, například bajtech. Tuto metodu lze využít v kombinaci s diferenční výkonovou analýzou proti systémům, jejichž ochrana je založena na maskování zpracovávaných dat. V tomto případě totiž nelze diferenční výkonovou analýzu použít samotnou.

5 DIFERENČNÍ VÝKONOVÁ ANALÝZA

Cílem kapitoly je prostudovat techniku útoku diferenční výkonovou analýzou. Základem útoku je sestavení hypotetického modelu kryptografického modulu. Tento model musí zahrnovat simulovaný postranní kanál. Vyhodnocení získaných výsledků z reálného a hypotetického modulu je provedeno za pomocí statistických metod.

Útok za pomoci diferenční výkonové analýzy DPA (*Differential Power Analysis*) je jedním z nejnebezpečnějších druhů útoku výkonovým postranním kanálem [2], [3], [6]. Tento typ analýzy je založen na sledování korelace mezi výkonovým průběhem a programem zpracovávanými daty. Tato vazba je většinou slabá a je nutné použít statistických metod k jejímu nalezení. Na obr. 4 je zobrazen obecný model diferenční analýzy. Základem je model reálného kryptografického modulu. Předpokladem jsou stejná data zpracovávaná jak na reálném modulu, tak na jeho modelu. Následně jsou analyzovány výstupy získané postranním kanálem jak reálného modulu, tak i hypotetického modelu. Pouze pro správný odhad citlivého údaje dochází ke korelaci mezi oběma postranními kanály. V případě, že jsou získána a analyzována data z jednorozměrného postranního kanálu (jeden typ kanálu, získána jedna hodnota pro každý časový okamžik), je diferenční analýza nazývána diferenční analýza prvního řádu. V případě vícerozměrného postranního kanálu (více typů postranních kanálů, je získána řada hodnot pro každý z časových okamžiků) se jedná o diferenční analýzu vyšších řádů.



Obr. 4. Model diferenční analýzy [7]

5.1 ÚTOK VÝKONOVÝM POSTRANNÍM KANÁLEM S DIFERENČNÍ ANALÝZOU ZALOŽENOU NA ROZDÍLU STŘEDNÍCH HODNOT

Pro úspěšné provedení útoku diferenční výkonovou analýzou je nutné získat řadu průběhů výkonové spotřeby (řádově 1000) a současně jim příslušných vstupů nebo výstupů kryptografického modulu. Cílem útoku je odvodit bity tajného klíče, který je opakovaně použit při všech operacích. Do souvislosti je dán výkonový průběh a změny stavů na datových sběrnicích. Ty jsou odvozeny ze vstupů nebo výstupů kryptografického modulu. V případě, že naměřené průběhy výkonové spotřeby nebudou vůbec závislé na vnitřních stavech, nelze tento typ útoku realizovat.

Nashromážděné průběhy výkonové spotřeby měřené v diskrétním čase lze chápat jako vektory náhodných veličin $\mathbf{T}_1..\mathbf{T}_n$, kde n je počet změřených průběhů (viz [5], [14] a [15]). Každý vektor z $\mathbf{T}_1..\mathbf{T}_n$ obsahuje k naměřených hodnot $\mathbf{T}_i = (T_{i[1]}..T_{i[k]})$, kde $i \in 1..n$. Počet naměřených hodnot v každém vektoru závisí na vybavení útočníka, tedy vzorkovací frekvenci snímacího zařízení a kapacitě paměti určené pro záznam (obvykle $10^4 \leq k \leq 10^6$).

Naměřené průběhy lze rozdělit do dvou podmnožin, a to na základě hodnoty bitu b. Bit b je závislý na vnitřních stavech kryptografického modulu a je získán z otevřeného či šifrovaného textu.

Předpokladem je, že bit b jednoznačně zařazuje naměřený výkonový průběh do jedné ze dvou podmnožin a má vliv na probíhající operace v kryptografickém modulu. Získány jsou dvě podmnožiny, které lze matematicky popsat následujícími vztahy

$$\mathbf{T}_0 = \{\mathbf{T}_i : b = 0\},\ \mathbf{T}_1 = \{\mathbf{T}_i : b = 1\}. \qquad (5.1), (5.2)$$

V případě, že otevřený text je náhodný, je rozložení průběhů v obou podmnožinách rovnoměrné. Každou podmnožinu bude dále reprezentovat průměr všech průběhů (vektorů) v ní. Průměrný průběh pro každou podmnožinu pro $j = 1..k$ lze zapsat jako

$$\overline{A}_{0[j]} = \frac{1}{|\mathbf{T}_0|} \sum_{\mathbf{T}_i \in \mathbf{T}_0} T_{i[j]},\ \overline{A}_{1[j]} = \frac{1}{|\mathbf{T}_1|} \sum_{\mathbf{T}_i \in \mathbf{T}_1} T_{i[j]}, \qquad (5.3), (5.4)$$

kde $|\mathbf{T}_1| + |\mathbf{T}_0| = n$ a $T_{i[j]}$ představuje j-tou hodnotu z vektoru měřené výkonové spotřeby T_i. Diferenční průběh je získán jako rozdíl obou průměrných průběhů reprezentujících každou podmnožinu. Pro $j = 1..k$ lze tento průběh zapsat jako

$$\Delta_{[j]} = \overline{A}_{1[j]} - \overline{A}_{0[j]}. \qquad (5.5)$$

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

$$\mathrm{E}[T_{i[j^*]} \mid b = 1] - \mathrm{E}[T_{i[j^*]} \mid b = 0] = \varepsilon. \qquad (5.6)$$

V časových okamžicích $j \neq j^*$, kdy výkonová spotřeba je na bitu b nezávislá, pak platí

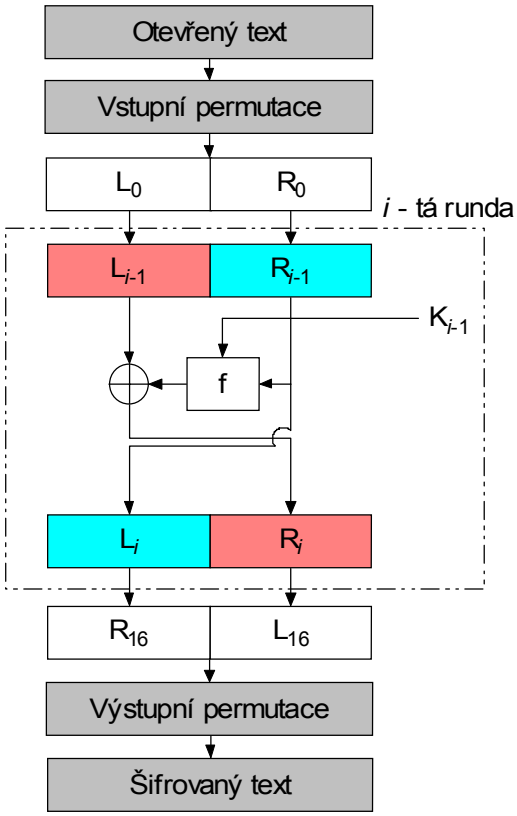
$$\mathrm{E}\left[T_{i[j]} \mid b=1\right] - \mathrm{E}\left[T_{i[j]} \mid b=0\right] = 0 . \qquad (5.7)$$

V případě, že jsou k dispozici velké počty naměřených výkonových průběhů, tak $\overline{A}_{1[j]}$ a $\overline{A}_{0[j]}$ konverguje k $\mathrm{E}\left[T_{i[j]} \mid b=1\right]$ a $\mathrm{E}\left[T_{i[j]} \mid b=0\right]$. Pak lze psát

$$\lim_{n\to\infty} \Delta_{[j]} = \lim_{n\to\infty} \overline{A}_{1[j]} - \lim_{n\to\infty} \overline{A}_{0[j]} = \begin{cases} \varepsilon, \text{pro } j = j^*, \\ 0, \text{ostatní}. \end{cases} \qquad (5.8)$$

5.2 PRAKTICKÁ REALIZACE ÚTOKU ZA POMOCÍ DIFERENČNÍ VÝKONOVÉ ANALÝZY NA ŠIFROVACÍ ALGORITMUS DES

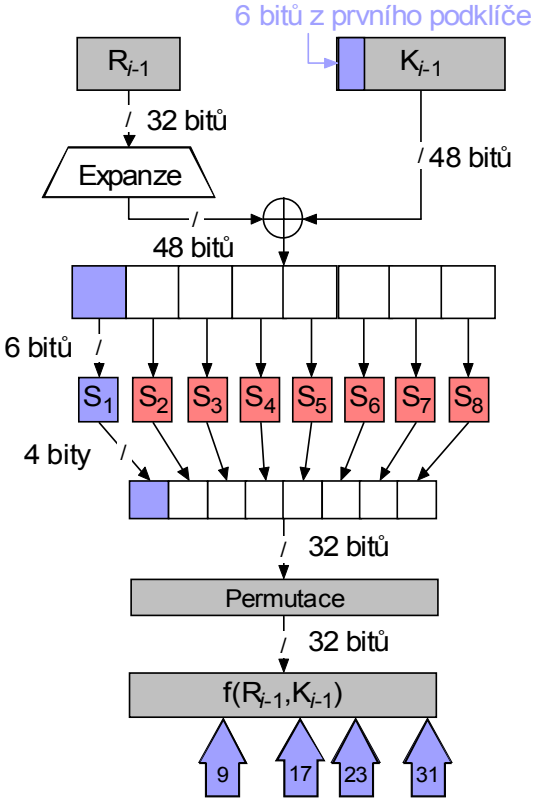
Praktická ilustrace útoku DPA bude prezentována na šifrovacím algoritmu DES (viz obr. 5). Základem pro rozdělení měřených průběhů výkonové spotřeby do dvou podmnožin je hodnota rozdělujícího bitu b. V případě šifry DES lze rozdělující bit získat buď z otevřeného textu a nebo z textu šifrovaného. Nejprve bude popsán postup útoku na základě znalosti otevřeného textu a následně naznačen postup pro znalost textu šifrovaného.



Obr. 5. Schéma šifrovacího algoritmu DES

5.2.1 Znalost otevřeného textu

Předpokladem je znalost otevřeného textu. Z otevřeného textu jsou odvozeny bity bloku R_0 první rundy. V prvním kroku je zjišťováno prvních 6 bitů ze 48 bitového rundovního klíče (viz obr. 6). Tyto bity mají vliv na první S-box. První S-box po příslušné permutaci ovlivňuje 9., 17., 23. a 31. bit ve výsledku Fiestelovy rundovní funkce. Na základě Fiestelovy rundovní funkce užité u algoritmu DES lze vypočítat blok $R_1 = L_0 \oplus f(R_0, K_1)$.

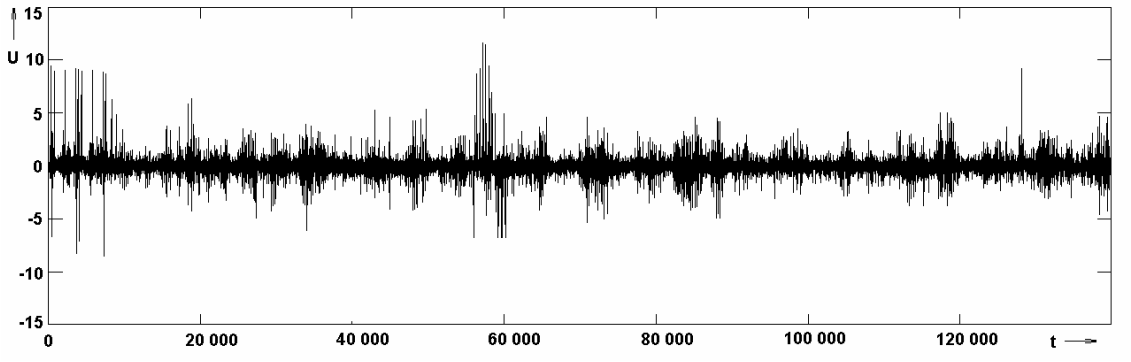


Obr. 6. Základní schéma Fiestelovy rundovní funkce u algoritmu DES [8]

Bity 9, 17, 23 a 31 z bloku R_1 jsou tedy ovlivněny prvním S-boxem a jeden z nich lze užít jako rozdělující bit pro rozdělení průběhů výkonové spotřeby. Bity bloků R_0 a L_0 jsou známy na základě provedení počáteční permutace otevřeného textu. Jedinou neznámou jsou bity K_1 reprezentující 6 bitů z 48 bitového rundovního klíče. Těchto 6 bitů je odhadnuto a na jejich základě jsou provedeny výpočty příslušného rozdělujícího bitu bloku R_1 každého výkonového průběhu. Následné dělení a získaný diferenční průběh rozhodne, zda jsou bity K_1 odhadnuty správně či špatně. Správným odhadem je získán diferenční průběh s několika zákmity o odchylce ε (viz obr. 7), nesprávným odhadem diferenční průběh s přibližně konstantním průběhem o výchylkách nulové hodnoty. Pouze jeden ze 2^6 odhadů je správným rundovním klíčem na jehož základě je získán správný diferenční průběh.

Stejným postupem se v dalším kroku zjišťuje další 6 bitová část rundovního klíče. Nejprve jsou určeni kandidáti na rozdělující bit z bitů bloku R_1. Jsou to ty bity, které

jsou ovlivněny druhým S-boxem. Je získán diferenční průběh a rozhodnuto o správnosti odhadu 6 bitové části klíče. Postupně je tak v dalších krocích získáno celých 48 bitů rundovního klíče. Na základě znalostí o nakládání s 56 bitovým klíčem algoritmu DES lze ze získaných 48 bitů rundovních klíčů určit 48 bitů z 56 bitového klíče. Zbývajících 8 bitů lze určit útokem hrubou silou a nebo provedením diferenční analýzy pro druhou rundu algoritmu DES. Hodnoty bitů v blocích L_1 ,R_1 jsou vypočteny na základě získaného 48 bitového rundovního klíče.



Obr. 7. Diferenční průběh získaný při DPA za použití správného odhadu rozdělovacího bitu *b* [5]

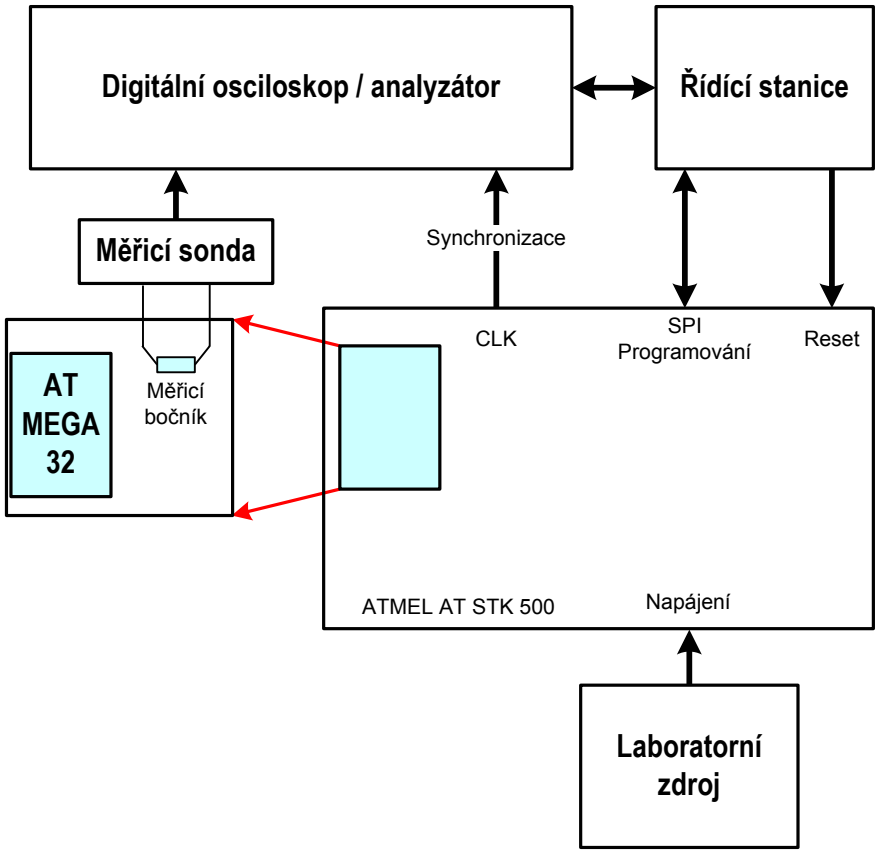
5.2.2 Znalost šifrovaného textu

Z příslušného bitu šifrovaného textu lze odvodit bity z bloku L_{16} poslední rundy. Útok je veden od poslední rundy stejným způsobem. Je vybrán rozdělující bit z bloku $L_{16.}$ Bity bloku L_{16} lze získat výpočtem z bloku L_{15} dle vztahu $L_{15} = R_{16} \oplus f(L_{16}, K_{16})$. Šestice bitů z rundovního klíče K_{16} je odhadnuta a následně ověřena správnost odhadu. Postup je opakován po 6 bitových částech až do získání správného 48 bitového rundovního klíče. Postup získání celého hlavního klíče je popsán v závěru předchozího odstavce.

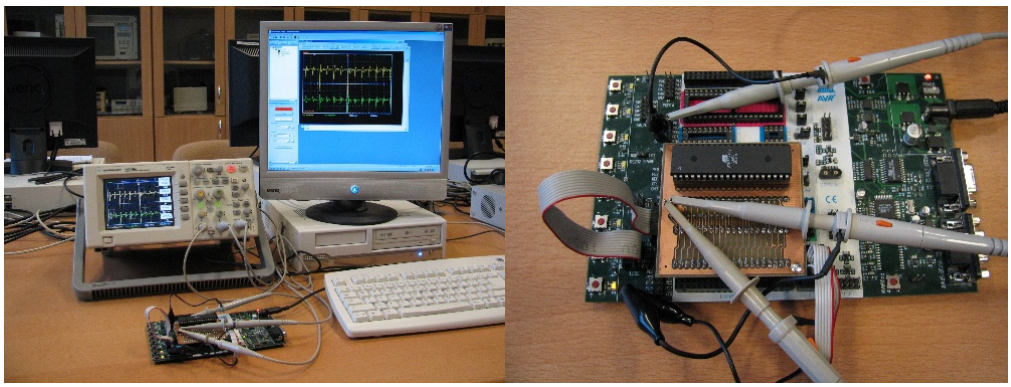
6 EXPERIMENTÁLNÍ PRACOVIŠTĚ PRO SIMULACI ÚTOKŮ VÝKONOVÝM POSTRANNÍM KANÁLEM

Cílem kapitoly je popsat bloky experimentálního pracoviště vytvořeného za účelem studia postranních kanálů a ověření vlivu napájecího systému na výkonový postranní kanál. Blokové schéma experimentálního pracoviště je na obr. 8, jeho skutečná podoba je zobrazena na obr. 9. Toto pracoviště sestává z následujících prvků:

- model kryptografického modulu (vývojový kit ATMEL AT STK 500 a mikroprocesor AVR MEGA 32) s implementovanou kryptografickou knihovnou,
- měřicí řetězec (měřicí bočník, sonda, jednotka pro záznam a zpracování dat),
- řídicí stanice (osobní počítač doplněný o vyvinuté programové vybaveni).



Obr. 8. Blokové schéma experimentálního pracoviště



Obr. 9. Experimentální pracoviště

Následující text obsahuje podrobnější popis dílčích bloků a použitého vybavení.

6.1 KRYPTOGRAFICKÝ MODUL

Před praktickým ověřením útoku výkonovým postranním kanálem byl navržen model kryptografického modulu. Jako cílová platforma byla vybrána rodina mikroprocesorů firmy AVR firmy Atmel. Mikroprocesory AVR jsou 8-bitové procesory založené na RISC (*Reducion Instruction Set Computer*) architektuře. Dosahují výpočetních výkonů typických pro 16-bitové procesory. Charakteristické

rysy jsou jednocyklové instrukce, vyšší taktovací frekvence spojená s vyšším pracovním výkonem a efektivní optimalizace překladu. Důvodů volby řady AVR, je celá řada. Především jsou tyto procesory často použity jako základ čipových karet a USB tokenů. Model kryptografického modulu se tím výrazně blíží realitě. Další výhodou je návrh modulu přizpůsobený pro snadný přístup k požadovanému výkonovému postrannímu kanálu. Cílem práce totiž není zahrnout do koncepce způsoby odstraňování fyzických zábran u reálných kryptografických zařízení, cílem je studovat samotný postranní kanál. Model kryptografického modulu již byl ověřen a využit v rámci projektů řešených na fakultě telekomunikací, např. projektů Akademie Věd ČR [9], [10].

Součástí modelu kryptografického modulu je kromě hardwarové platformy také softwarové vybavení. Do modulu byly implementovány kryptografické algoritmy nezbytné k simulacím útoku postranním kanálem. Jedním z implementovaných je i šifrovací algoritmus DES. DES již není v současnosti považován za bezpečný. Důvodem jeho implementace je názornost útoku výkonovým postranním kanálem proti němu. DES se tak stává pomyslně „odrazovým můstkem“. Algoritmus DES je bohatě dokumentován a lze jej čerpat např. v knihovně OpenSSL. Bohužel je OpenSSL určena pro komplexní operační systémy a jiné hardwarové platformy. Návrh vlastní knihovny kryptografických protokolů zahrnující charakteristické rysy mikroprocesorů AVR byl tedy nezbytný. Knihovna byla vytvořena v jazyce C ve vývojovém prostředí Codevision.

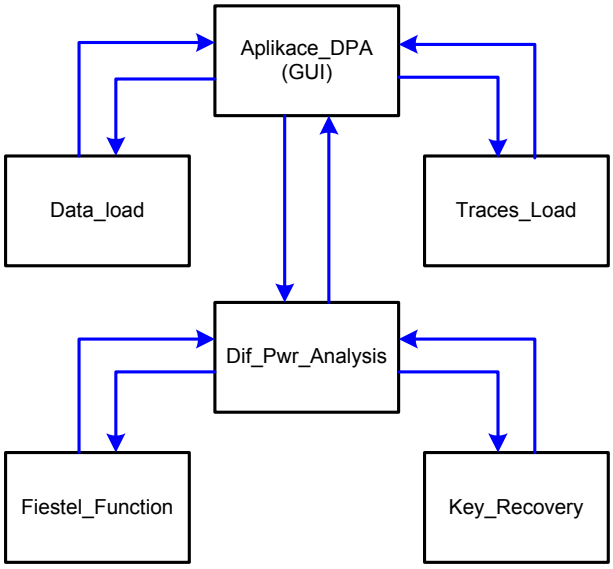
6.2 PROGRAMOVÉ VYBAVENÍ PRO DIFERENČNÍ VÝKONOVOU ANALÝZU

Pro zpracování výsledků získaných z výkonového postranního kanálu bylo zvoleno prostředí MATLAB. Pro potřeby diferenční výkonové analýzy byla vyvinuta aplikace v jazyce C s grafickou nadstavbou v prostředí MATLAB. Blokové schéma aplikace je na obr. 10 [11]. Aplikace je sestavena z dílčích bloků realizovaných samostatnými soubory (m-files). Aplikace umožňuje simulovat útok za pomocí diferenciální výkonové analýzy. Použita je statistická metoda založená na rozdílu středních hodnot.

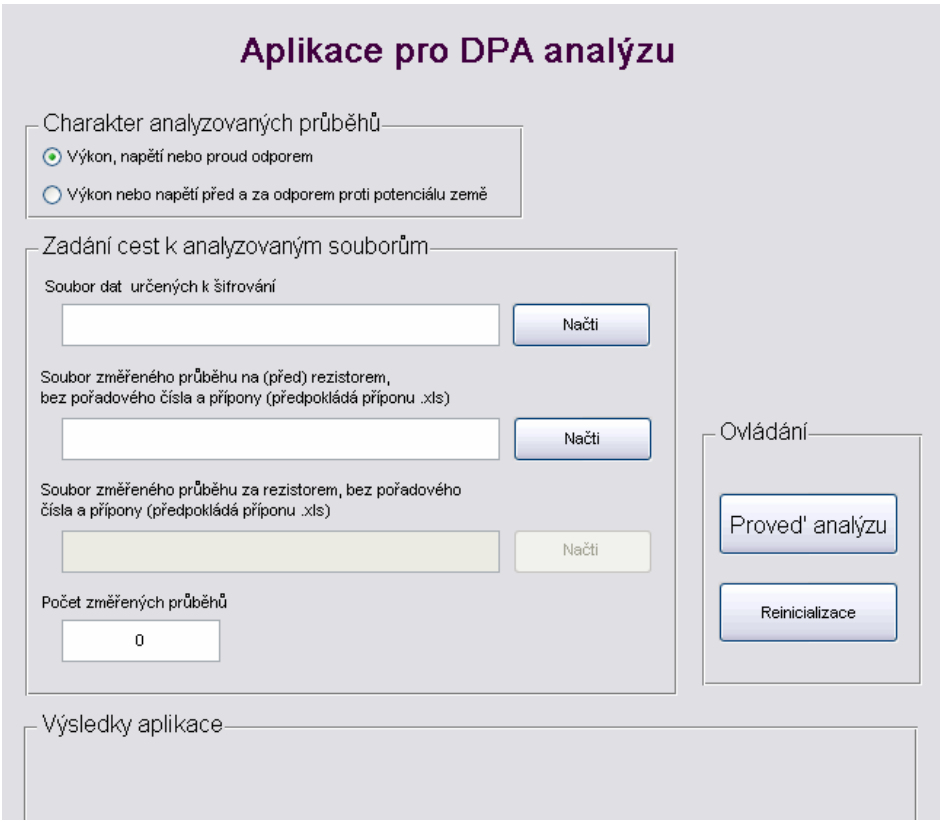
Blok *Data_Load* zajišťuje zavedení a konverzi dat určených ke zpracování šifrovacím algoritmem DES. Blok *Traces_Load* zajišťuje zavedení měřených výkonových průběhů příslušejícím k datům zavedeným v předchozím kroku.

Na zavedených a konvertovaných datech provede blok *Dif_Pwr_Analysis* samotnou diferenční výkonovou analýzu. Pro potřeby analýzy a simulace funkcí šifrovacího algoritmu DES blok *Dif_Pwr_Analysis* spolupracuje s bloky *Fiestel_Function* a *Key_Recovery*. Výsledkem této analýzy je odhad šifrovacího klíče.

Grafické rozhraní představuje prostředníka mezi uživatelem a funkcemi aplikace realizujícími analýzu. Vzhled základního ovládacího panelu je na obr. 11.



Obr. 10. Blokové schéma aplikace pro diferenční výkonovou analýzu

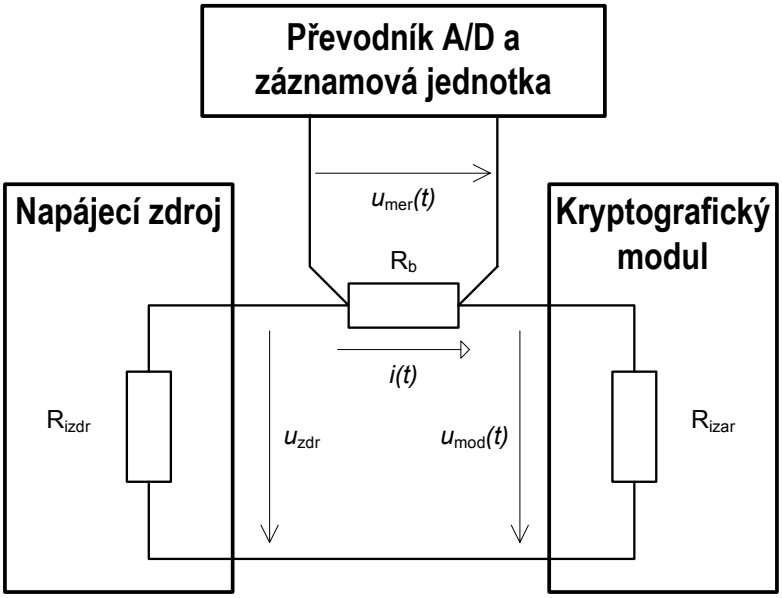


Obr. 11. Grafické uživatelské rozhraní [11]

6.3 MĚŘENÍ VÝKONOVÝCH PRŮBĚHŮ

Výkonová analýza je založena na sledování výkonové spotřeby kryptografického modulu. Za předpokladu, že je kryptografický modul napájen konstantním napětím, je aktuální výkonová spotřeba přímo úměrná proudové dle $p(t) = U \cdot i(t)$. Ve skutečnosti lze tedy měřit proudovou spotřebu.

Zatímco je napětí konstantní, proud se mění dle zákonitostí popsaných v kapitolách pojednávajících o výkonovém postranním kanále. Měřicí metoda je založena na snímání a zaznamenávání odebírané proudové spotřeby ze zdroje. Základem měřicího řetězce je bočník vřazený mezi zdroj a kryptografický modul (viz obr. 12). Na bočníku je okamžitá hodnota proměnného proudu $i(t)$ převedena na okamžitou hodnotu proměnného napětí $u(t)$, dle Ohmova zákona $u(t) = R \cdot i(t)$. Okamžitá hodnota získaného napětí $u(t)$ je převedena A/D převodníkem do digitální podoby a zaznamenána.



Obr. 12. Zapojení měřicího řetězce

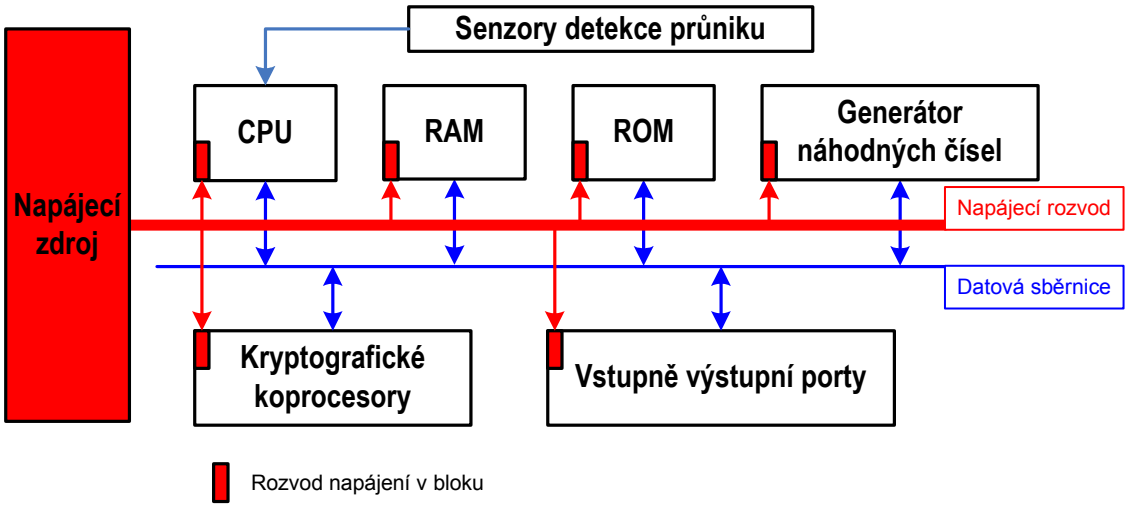
Snímací zařízení je zpravidla osciloskop nebo číslicový analyzátor. Ekvivalentní vstupní impedance běžných osciloskopů je tvořena paralelní kombinací odporu $R_i = 1$ MΩ a kapacity $C_i = 20$ až 50 pF. Osciloskop je do obvodu připojen pomocí napěťové sondy. Ta zpravidla umožňuje kompenzaci vstupních impedancí a zvyšuje vstupní odpor osciloskopu za cenu snížení napětí přiváděného na vstup osciloskopu. Osciloskopy těchto parametrů nezpůsobí chybu měření.

7 NAPÁJECÍ SYSTÉM KRYPTOGRAFICKÉHO MODULU

Napájecí systém je nedílnou součástí každého elektronického zařízení. Primárním úkolem napájecího systému bylo zajistit zdroj elektrické energie a její rozvod po zařízení. Požadavkem každého elektronického prvku je stálé napájení o přesně

definovaných hodnotách. Z pohledu napájecích svorek součástky tak vedení zpravidla představuje zdroj konstantního napětí s dostatečnou proudovou rezervou (tvrdý zdroj napětí). Dalším požadavkem je zamezení šíření rušivých jevů (impulzů) mezi zdrojem a napájenými prvky a dále mezi prvky samotnými.

Kryptografický modul je konkrétní realizací elektronického zařízení (viz obr. 13). V případě kryptografického modulu se požadavky na napájecí systém výrazně zvyšují. Zvláště pak na základě znalosti problematiky výkonového postranního kanálu se návrh napájecího systému stává velmi komplikovaným úkolem. Kromě obecných požadavků na elektronické zařízení je do návrhu napájecího systému kryptografického modulu nezbytné zahrnout i techniky zamezující útokům výkonovým postranním kanálem. Tento způsob ochrany spadá do kategorie hardwarových protiopatření.



Obr. 13. Blokové schéma rozvodu napájení v kryptografickém modulu

Útočník musí při útoku výkonovou analýzou vzít v potaz všechny prvky napájecího systému. Jeho cílem je získat průběhy výkonové spotřeby přímo v místech napájecích svorek integrovaných obvodů. S rostoucí vzdáleností měření od těchto míst roste počet napájených prvků a počet filtračních prvků napájecího systému. S tím také roste množství šumu ve sledovaném výkonovém postranním kanále.

7.1 ROZVOD NAPÁJENÍ V ELEKTRONICKÉM ZAŘÍZENÍ

Rozvod napájení v rámci elektronického zařízení lze rozdělit na dva úseky [12]. Prvním z nich je rozvod napájecí energie od zdroje k jednotlivým napájeným blokům. Tyto bloky jsou většinou představovány deskou plošných spojů. Dalším úsekem je rozvod napájení v rámci samotného bloku.

7.1.1 Úsek mezi napájecím zdrojem a funkčními bloky

Úsek mezi napájecím zdrojem a jednotlivými funkčními bloky je krátký (do půl metru). Dle proudového odběru bloků jsou voleny vodiče z vhodného materiálu a o takovém průřezu, aby nedošlo k proudovému přetížení. Problematické je zamezení kapacitním vazbám se signálovými a ostatními vodiči. Žádoucí je umístění napájecího a zemnícího vodiče blízko sebe. Je tím zajištěna malá indukčnost a dochází ke vzniku příznivé přídavné kapacity mezi vodiči.

7.1.2 Úsek v rámci bloku

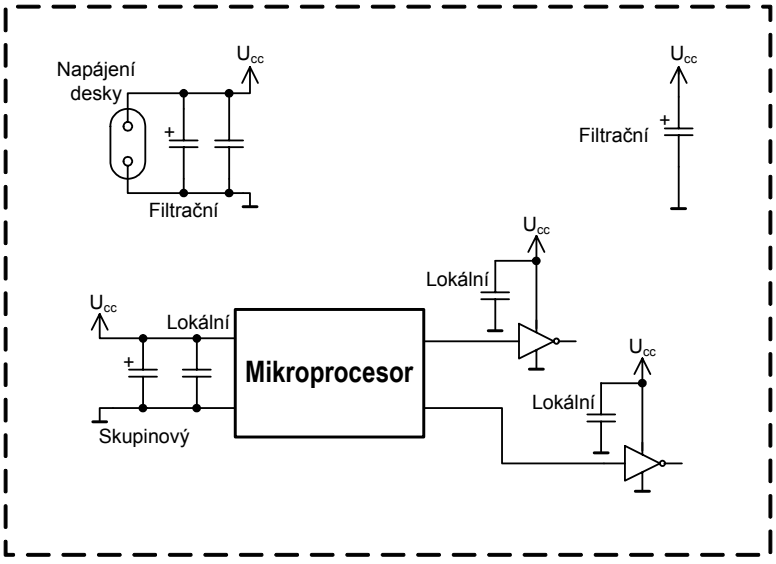
Úkolem napájecího systému v rámci bloku (jedné desky plošných spojů) je rozvod elektrické energie od napájecích svorek bloku k jednotlivým elektronickým součástkám. Rozvod napájecího a zemního spoje je nejkomplikovanějším a co do plochy největším uzlovým spojem na desce plošných spojů. Jeho návrh je náročný. Zjednodušení přináší vícevrstvý plošný spoj, kdy jsou pro rozvod napájení vyhrazeny samostatné vnitřní vrstvy. Dochází mezi nimi ke vzniku přídavné kapacity.

Napájecí soustava musí v rámci bloku zajistit:

- minimální ovlivňování signálových cest,
- zamezení šíření impulzního rušení,
- vytvoření lokálního zdroje elektrické energie pro rychlé děje v integrovaných obvodech.

Pro realizaci posledních dvou úkolů používá napájecí systém filtračních prvků. Konkrétně jsou to blokovací kondenzátory, které jsou někdy doplněné o přídavné indukční prvky.

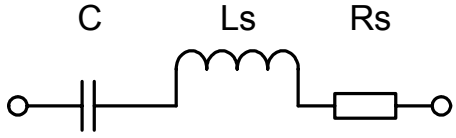
Dle účelu, typu a kapacity jsou blokovací kondenzátory členěny na filtrační, skupinové a lokální, viz obr. 14.



Obr. 14. Blokovací kondenzátory a jejich umístění na desce plošných spojů [13]

7.2 BLOKOVACÍ KONDENZÁTORY

Klíčové místo napájecího systému je v přípojném bodě filtračního prvku. Filtrační prvek je většinou realizován blokovacím kondenzátorem. V elektronických zařízeních, sestavených z mikroprocesoru a na jeho výstupy připojených a jím ovládaných elektronických prvků, dochází během činnosti k rychlým změnám energie. Úkolem lokálního a skupinového blokovacího kondenzátoru je tuto energii zajistit. Z množství požadované energie a rychlosti změn je odvozena vhodná kapacita a typ kondenzátoru. Vzhledem k rychlosti změn energie je vhodným typem kondenzátor s dobrými vysokofrekvenčními parametry, tedy zpravidla keramický kondenzátor. Parametry kondenzátoru se mění s frekvencí a výrobce poskytuje jejich frekvenční závislosti. Nad mezní frekvenci se u kondenzátoru projevují parazitní vlastnosti (postupně převládá parazitní indukčnost). Často není blokovací kondenzátor jen jeden, ale je jich několik o různých kapacitách. Je to dáno právě jejich mezním kmitočtem, kdy každý z nich zajišťuje energii pro různě rychlé změny energie (různé frekvence). Model kondenzátoru je na obr. 15.



Obr. 15. Model parazitních vlastností kondenzátoru, C – vlastní kapacita, Rs – součet všech sériových odporů (elektrolytu, anodové a katodové fólie a přívodů), Ls – součet všech sériových indikčností

Za předpokladu, že po nabití kondenzátoru se na jeho elektrodách nachází stejně velký náboj opačné polarity (platí $Q = Q_1 = -Q_2$), pak energie akumulovaná kondenzátorem je

$$E = \frac{1}{2}QU = \frac{1}{2}QU^2 . \qquad (7.1)$$

kde Q je náboj a U napětí na elektrodách kondenzátoru.
Pro nabíjení kondenzátoru platí následující vztah

$$I = \frac{\mathrm{d}Q}{\mathrm{d}t} = C\frac{\mathrm{d}U}{\mathrm{d}t} . \qquad (7.2)$$

kde I je proud nabíjející kondenzátor, $\frac{\mathrm{d}Q}{\mathrm{d}t}$ je změna náboje na elektrodách kondenzátoru, C je kapacita kondenzátoru a $\frac{\mathrm{d}U}{\mathrm{d}t}$ je změna napětí na elektrodách kondenzátoru.

7.2.1 Lokální blokovací kondenzátor

Kapacitu lokálního blokovacího kondenzátoru lze určit podle následujícího vztahu

$$C_P = \frac{I_p}{\frac{\Delta U_{cc}}{\Delta t}} \qquad (7.3)$$

kde I_p je impulzní proudová spotřeba integrovaného obvodu (odráží změnu energie), ΔU_{cc} je přípustná změna napájecího napětí (zpravidla 5%) po dobu proudového impulzu a Δt je doba trvání proudového impulzu.

7.2.2 Skupinový blokovací kondenzátor

Kapacitu skupinového blokovacího kondenzátoru lze určit podle následujícího vztahu

$$C_B = C_L\left(\frac{\Delta U_{CL}}{\Delta U_{CC}}\right) \qquad (7.4)$$

kde C_L je celková zatěžovací kapacita, ΔU_{CL} napěťový rozkmit na kapacitní zátěži C_L a ΔU_{cc} je přípustná změna napájecího napětí (zpravidla 5%).

8 VÝSLEDKY MĚŘENÍ VÝKONOVÝCH PRŮBĚHŮ V KLÍČOVÝCH MÍSTECH NAPÁJECÍHO SYSTÉMU

Cílem kapitoly je naznačit způsob, jakým byly publikovány výsledky měření výkonové spotřeby v klíčových místech napájecího systému kryptografického modulu v textu dizertační práce. Dizertační práce obsahuje kompletní soubor výsledků, v textu této kapitoly je pouze jejich příklad.

8.1 POPIS MĚŘENÍ

Měřicím řetězcem není měřena přímo výkonová spotřeba kryptografického modulu (viz text předchozích kapitol). Měřena je proudová spotřeba, která je za předpokladu konstantního napájecího napětí úměrná výkonové. Proudová spotřeba je měřena na předřadném bočníku. Proměnná proudová spotřeba $i(t)$ je dle Ohmova zákona $u(t) = R \cdot i(t)$ na bočníku převedena na proměnné napětí $u(t)$. Toto proměnné napětí $u(t)$ je následně zaznamenáváno a zpracováváno. To je také důvod, proč jsou veškeré měřené výsledky v podobě proměnného napětí a ne výkonu. Důležitá je poznámka, že všechna měření jsou prováděna na měřicím bočníku vloženém do cesty napájení. Měřicí bočník je vložen na klíčové místo napájecího systému a na něm je provedeno měření napěťového průběhu.

Nejvýraznějším prvkem ovlivňujícím napěťové průběhy v úseku rozvodu napájení jsou blokovací kondenzátory. Umístění blokovacích kondenzátorů představuje klíčová místa pro měření napěťových průběhů.

Konkrétní parametry blokovacích kondenzátorů obsažených v modulu jsou:

- keramický kondenzátor 100 nF – provedení SMD,
- tantalový elektrolytický kondenzátor 47 μF, provedení SMD,
- elektrolytický kondenzátor 220 μF , provedení radiální.

První měření napěťového průběhu je provedeno bez blokovacích kondenzátorů, tedy přímo na napájecím vývodu mikroprocesoru AVR MEGA 32. Získaný průběh je považován za referenční. Následně jsou měřeny napěťové průběhy na jednotlivých kondenzátorech nebo jejich kombinacích. Každé provedené měření je dokumentováno obrazovkou sejmutou z osciloskopu. Tato obrazovka obsahuje referenční průběh získaný při prvním měření (bez blokovacích kondenzátorů), dále pak napěťový průběh měřený na klíčovém místě napájecího systému (na daném blokovacím kondenzátoru/ech) a hodinový signál CLK měřený na svorce CLK mikroprocesoru. Měření jsou synchronizována za pomocí signálu získaného na jednom z portů mikroprocesoru. Tento signál je vytvářen programově. Obrazovky sejmuté z osciloskopu jsou obsahem textu dizertační práce samotné, zde nejsou uvedeny.

Mikroprocesorem je v cyklu zpracováván jednoduchý programový kód. Každá z instrukcí je provedena v jednom hodinovém cyklu. V úvodní fázi jsou do registrů r16 a r17 předpřipraveny hodnoty r16 = 0x00 a r17 = 0xFF (tyto instrukce nejsou obsahem obr. 16).

Na obr. 16 je ve smyčce prováděný programový kód o 4 instrukcích. Pozorování a hodnocení průběhů je založeno na principu jednoduché výkonové analýzy, tedy průběhy jsou pozorovány a vyhodnocovány přímo. Opakovaně prováděný kód sestává z následujících instrukcí.

- výstupní port A je nastaven do úrovně logické jedničky a tím je odeslán synchronizační impulz pro aktivaci měření,
- následují dva hodinové takty obsahují sledované instrukce, u kterých bude vyhodnocován průběh výkonové spotřeby,
- výstupní port A je nastaven do úrovně logické nuly a tím se deaktivuje měření.

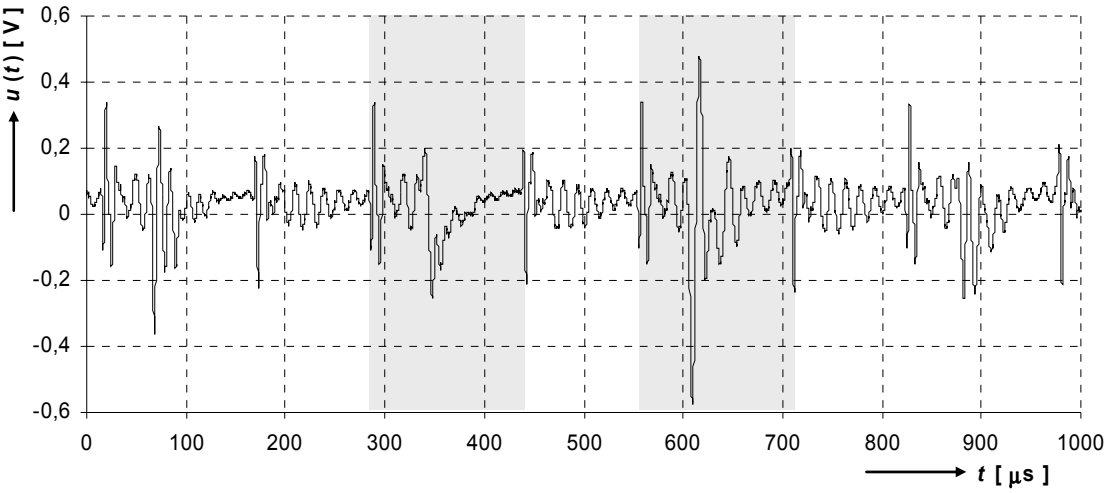
Opakovaný cyklus má délku 4 hodinových taktů.

```
1. out $1B,r17
2. out $18,r16
3. out $18,r17
4. out $1B,r16
```

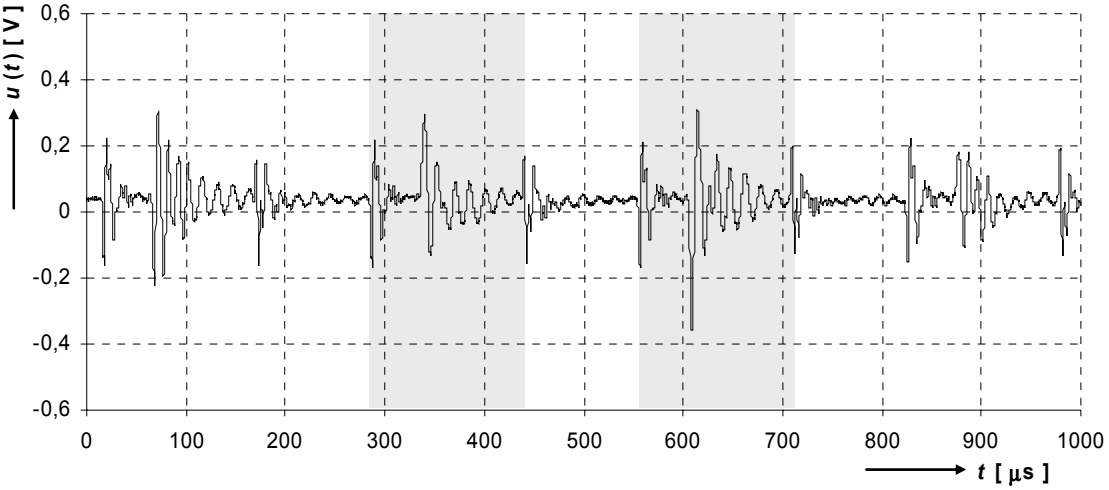
Obr. 16. Programový kód opakovaně zpracovávaný mikroprocesorem při měřeních

8.2 SHRNUTÍ A VYHODNOCENÍ ZÍSKANÝCH VÝSLEDKŮ

Příklad výsledků získaných měřením napěťových průběhů je v následujících grafech na obr. 17 a obr. 18. Kompletní soubor výsledků je obsahem samotné dizertační práce



Obr. 17. Měřený průběh bez blokovacích kondenzátorů



Obr. 18. Měřený průběh s keramickým blokovacím kondenzátorem 100 nF

V každém grafu je zanesen měřený napěťový průběh pro čtyři takty hodinového signálu. Pro posouzení jsou rozhodující druhý a třetí hodinový takt. Napěťový průběh je pro tyto dva takty zvýrazněn. Na každé straně je jako první umístěn graf s referenčním průběhem měřeným bezprostředně na napájecím vývodu mikroprocesoru. To je vhodné pro snadnější posouzení rozdílů mezi měřením u pouzdra a měřeními získanými v klíčových místech napájecího systému.

Obr. 18 je získán měřením průběhu napětí na blokovacím kondenzátoru 100 nF. Patrné jsou výrazné změny oproti referenčnímu průběhu. V časovém rozmezí 350 až

400 μs je dokonce degradace průběhu kritická. Celkově je pozorovatelné výrazné snížení špiček a vyhlazení průběhu. Blokovací kondenzátor 100 nF má na měřený průběh výrazný vliv. Plyne to i z podstaty jeho určení, protože je používán jako lokální blokovací kondenzátor.

Ze získaných výsledků, které jsou obsahem dizertační práce, jednoznačně vyplývá výrazný vliv blokovacího kondenzátoru 100 nF. Tento kondenzátor ve srovnání s ostatními degraduje průběh nejvíce. Všechny kondenzátory výrazně ovlivnili průběh druhého hodinového taktu v rozmezí časů 350 až 400 μs. Charakteristický podpis je zde zcela ztracen.

9 ZÁVĚR

V souladu s cíly stanovenými v kapitole 3 je text dizertační práce zaměřen na problematiku bezpečnosti kryptografických modulů vůči útokům postranním kanálem. Práce je zaměřena konkrétně na studium výkonového postranního kanálu.

Podrobná studie výkonového postranního kanálu byla rozčleněna do dvou částí, jednoduché a diferenční výkonové analýzy. Oba typy analýz byly ilustrovány na šifrovacích algoritmech DES a AES. Tyto algoritmy byly nejprve popsány a na jejich popisu bylo následně poukázáno na jejich slabiny. Rozebrána byla jejich slabá místa využitelná k útoku výkonovým postranním kanálem. Závěrem byl popsán Kocherův útok diferenční výkonovou analýzou založenou na statistické metodě rozdílu středních hodnot.

V přípravné fázi na praktické simulace útoku výkonovým postranním kanálem bylo autorem dizertační práce navrženo a realizováno experimentální pracoviště. Pracoviště sestává z modelu kryptografického modulu, měřicího řetězce a řídicí stanice. Řídicí stanice byla vybavena softwarem vytvořeným za účelem ověření diferenční výkonové analýzy Software je realizován v prostředí MATLAB. Data pro analýzu byla získána měřicím řetězcem založeným na odporovém bočníku. Tento bočník je vložen do napájecí cesty mezi vývojový kit a autorem vytvořenou měřicí redukcí osazenou mikroprocesorem AT MEGA 32. Do procesoru je zavedena autorem vytvořená kryptografická knihovna.

Stěžejním přínosem dizertační práce je také posouzení vlivu napájecího systému kryptografického modulu na informace (měřené průběhy) získané z výkonového postranního kanálu. V dostupné literatuře a odborných článcích je tento vliv zcela ignorován a jeho studie neexistuje. Zpravidla je mylně předpokládáno, že informace unikající výkonovým postranním kanálem jsou získávány přímo na napájecím vývodu integrovaného obvodu. Toto nelze v praxi vždy zajistit. Útočníkovi je přístup do napájecího systému zpravidla omezen.

Studie napájecího systému kryptografického modulu a jeho vlivu na výkonovou analýzu a následné experimentální ověření tohoto vlivu jsou jedinečným a dosud nepublikovaným přínosem této dizertační práce a byly vytvořeny autorem práce. Stejně tak i metody pro posouzení tohoto vlivu. Ověření tohoto vlivu je provedeno na navrženém a realizovaném experimentálním pracovišti.

Nejkomplikovanějším, a co do plochy největším uzlovým spojem na desce plošných spojů, je rozvod napájení a země. Ze studie napájecího systému kryptografického modulu vyplývá, že místa připojení filtračních prvků jsou klíčová pro posuzování vlivu tohoto systému na průběh výkonové spotřeby. Úkolem filtračních prvků je zamezení šíření impulsního rušení a zajištění lokálního zdroje energie pro rychlé děje probíhající v integrovaném obvodu. Filtrační prvek je zpravidla realizován pomocí blokovacího kondenzátoru, popř. kombinací kondenzátoru a cívky.

Předchozí odstavec shrnuje poznatky, ze kterých autor práce vycházel při stanovení metodiky pro posouzení vlivu napájecího systému kryptografického modulu na průběh výkonové spotřeby. Metodika je založena na sledování rozdílů v průbězích měřených před a za klíčovým místem napájecího systému, tedy místem připojení filtračního prvku, zpravidla blokovacího kondenzátoru. Napájecí systém rozlišuje tři základní druhy blokovacího kondenzátoru. Jsou to filtrační, skupinový a lokální blokovací kondenzátor.

Experimentálně získané výsledky měření průběhů před a za blokovacími kondenzátory a stejně tak jejich hodnocení je obsahem poslední kapitoly dizertační práce. Nejvýraznější vliv na průběh výkonové spotřeby má lokální keramický kondenzátor o hodnotě 100 nF. Způsobuje pokles úrovně ve sledovaném průběhu a výrazně degraduje charakteristické otisky instrukcí. Zbylé typy analyzovaných blokovacích kondenzátorů méně ovlivňují sledovaný průběh.

Konečným výsledkem bylo publikování získaných poznatků ve formě dizertační práce vhodné pro vlastní obhajobu. Řada dílčích výsledků již byla publikována na mezinárodních konferencích v průběhu doktorského studia autora práce. Na tyto publikace je v textu mnohokrát odkazováno.

LITERATURA

[1] WESTE, N., ESHRAGHIAN, K. Principles of CMOS VLSI Design: A System Perspective. Addison-Wesley, 2nd edition, N.Y.: McGraw-Hill, 1993, ISBN 0-201-533-766.

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

[3] KOCHER, P., JAFFE, J., JUN, B.: Differential Power Analysis: Leaking Secrets, In Proc. of CRYPTO '99, pp. 388-397, Santa Barbara, CA. Springer Berlin / Heidelberg, LNCS vol. 1666, 1999, ISSN 0302-9743.

[4] DANĚČEK, P., BŘEZINA, M. Simple power analysis In Research in telecommunication technology. Research in Telecommunication Technology 2006. Brno: Brno, 2006, s. 1 – 4.

[5] MUIR, J., A.: Techniques of Side Channel Cryptanalysis. Master Thesis, University of Waterloo, Waterloo, Ontario, Canada, 2001.

[6] DANĚČEK, P.: Power Side Channel Attacks to Cryptographic Modules. In Research in telecommunication technology. Ostrava: VŠB-Technická univerzita Ostrava, 2005, ISBN 80-248-0897-8.

[7] OSWALD, E, PRENEEL, B: A Theoretical Evaluation of some NESSIE Candidates regarding their Susceptibility towards Power Analysis Attacks, Katholieke Universiteit Leuven, Dept. ESAT, Belgium October 4, 2002.

[8] BIHAM, E., SHAMIR, A.: Differential Cryptanalysis of the Data Encryption Standard. Springer Berlin/Heidelberg, LNCS vol. 537, p.2, 1991, ISSN 0302-9743.

[9] DANĚČEK, P., BŘEZINA, M., MIŠUREC, J.: Data secure multiple colection of lastest network types. In Research in telecommunication technology. Research in Telecommunication Technology. Ostrava: VŠB-Technická univerzita Ostrava, 2005, pp. 1-6, ISBN 80-248-0897-8.

[10] MIŠUREC, J., DANĚČEK, P., BŘEZINA, M.: Bezpečná vzdálená správa a sběr dat. Elektrorevue - Internetový časopis (http://www.elektrorevue.cz), č. 5, s. 10-24, 2005, ISSN 1213-1539.

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

[12] VRBA, K., HERMAN, I., KUBÁNEK, D.: Konstrukce elektronických zařízení. [skripta k výuce předmětu]. [.pdf dokument]. Dostupný z WWW: <https://www.feec.vutbr.cz/et/skripta/utko/Konstrukce_elektronickych_zarizeni_S.pdf>

[13] ŠANDERA, J.: Návrh plošných spojů pro povrchovou montáž. BEN, Praha 2006, 272 stran. ISBN 80-7300-181-0.

[14] DANĚČEK, P., BODEČEK, K. Safety of Cryptographic Modules In International Conference on Signals and Electronic Systems. ICSES '06 International Conference on Signals and Electronic Systems. Poland, Lodz: NEUVEDEN, 2006, s. 1 - 1, ISBN 83-921172-6-3.

[15] DANĚČEK, P., BŘEZINA, M. Útok výkonovým postranním kanálem na hardwarový kryptografický modul.. Elektrorevue - Internetový časopis (http://www.elektrorevue.cz), ISSN 1213-1539, 2006, roč. 2006/08, č. 1, s. 1 - 1.

Další publikace autora dizertační práce

[16] DANĚČEK, P. Control system for GSM modem In Telecommunications and Signal Processing. Telecommunications and Signal processing TSP 2004. Brno: Brno, 2004, s. 292 - 295, ISBN 80-214-2684-5.

[17] DANĚČEK, P. Přenosy dat v sítích GSM, možnosti využití. Elektrorevue - Internetový časopis (http://www.elektrorevue.cz), ISSN 1213-1539, 2005, roč. 2005/5, č. 01, s. 1 - 1.

[18] SMÉKAL, Z., DANĚČEK, P. Testování multimediálních datových přenosů. Opnovaná výzkumná zpráva pro MPO projekt FD-K3/045 (výzkumná zpráva).

[19] ZEMAN, V., UCHYTIL, S., DANĚČEK, P. Zavedení nových poznatků z oblasti počítačové bezpečnosti do výuky. Oponovaná zpráva k projektu IS1572 (výzkumná zpráva).

[20] SÝKORA, M., DANĚČEK, P., CVRK, L., UCHYTIL, S. Výzkum uživatelsky přátelských videokonferenčních technologií. Roční oponovaná výzkumná zpráva MPO projektu FD-K3/045 (výzkumná zpráva).

[21] MIŠUREC, J., DANĚČEK, P., CVRK, L. Decentralized Secure Communication across NAT. International Transaction on Computer Science and Engineering, ISSN 1738-6438, 2005, roč. 1, č. 23, s. 121 - 134.

[22] MIŠUREC, J., CVRK, L., DANĚČEK, P. Decentralized Secure Communication across NAT In Proceedings 2nd International Conference on Electronics, Hardware, Wireless and Optical Communications. 2nd International Conference on Electronics, Hardware, Wireless and Optical Communications EHWOC 2005. 2005, s. 10 - 23, ISBN 89-953729-5-8.

[23] ZEMAN, V., DANĚČEK, P., SÝKORA, M. Cable references models for simulating metallic access networks In Telecommunications and Signal Processing TSP 2005. Telecommunications and Signal Processing TSP-2005. Brno: , 2005, s. 172 - 174, ISBN 80-214-2972-0.

[24] ZEMAN, V., DANĚČEK, P. Testovací provoz videokonferenčního systému. Oponovaná výzkumná zpráva projektu FD-K3/045 (výzkumná zpráva).

[25] LATTENBERG, I., DANĚČEK, P. Inovace a podpora výuky předmětu "Konstrukce elektronických zařízení". Oponovaná zpráva projektu č. 3189 (výzkumná zpráva).

[26] DANĚČEK, P., ŠILHAVÝ, P. Bezpečná autentizace In Research in telecommunication technology. Research in Telecommunication Technology 2006. Brno: Brno, 2006, s. 1 – 4.

[27] BURDA, K., BURŠÍK, F., DANĚČEK, P. Výzkum a ověření systému pro záznam a dlouhodobou archivaci multimediálních dat s inteligentním vyhledáváním - stanovení koncepce. Oponovaná výzkumná zpráva I. etapy řešení projektu MPO, 2006, reg. č. projektu FT-TA3/121. (výzkumná zpráva).

[28] ŠILHAVÝ, P., DANĚČEK, P. Vyšší techniky datových přenosů - laboratorní cvičení. ISBN TKO606. (skripta).

CURRICULUM VITAE

Jméno a příjmení:	Petr Daněček
Narozen:	18. 1. 1981 v Kyjově
Kontaktní spojení:	danecek.petr@email.cz

Dosažené vzdělání

2004 – současnost	Doktorské studium v oboru Teleinformatika. Téma dizertační práce je zaměřeno na útoky postranními kanály. Ústav Telekomunikací, Fakulta elektrotechniky a komunikačních technologií, Vysoké učení technické Brno
1999 – 2004	Magisterské studium v oboru Elektrotechnika a sdělovací technika. Vypracována diplomová práce s názvem Řídicí ústředna pro GSM modem. Ústav Telekomunikací, Fakulta elektrotechniky a komunikačních technologií, Vysoké učení technické Brno
1995 – 1999	Střední průmyslová škola v Uherském Hradišti, obor slaboproudá elektrotechnika

Účast na řešení projektů

2006

- Bezpečnost hardwarových kryptografických modulů.
- Výzkum nové generace infuzních pump s centrálním dispečinkem.
- Výzkum a ověření systému pro záznam a dlouhodobou archivaci multimediálních dat s inteligentním vyhledáváním.
- Výzkum a vývoj systému zabezpečené datové komunikace GPRS pro dálkový sběr energetických dat.
- Aplikovaný výzkum zabezpečené internetové komunikace se vzdálenými koncovými zařízeními v energetice.

2005

- Výzkum uživatelsky přátelských videokonferenčních technologií.

Zahraniční stáže

2007	Odborná stáž na vysoké škole University of Halmstad, Halmstad, Švédsko. V rámci stáže zpracována část dizertační práce. Program Free mover.
2005	Odborná stáž na vysoké škole KHLIM, Hasselt, Belgie. V rámci stáže řešen projekt TRNG generálů do programovatelných logických obvodů. Program Sokrates/Erasmus.

ANOTACE

Konvenční způsob kryptoanalýzy je založen na studiu slabin kryptografických algoritmů. Model útoku konvenční kryptoanalýzou zahrnuje pouze matematický popis použitých kryptografických algoritmů. Tento model je bez vazeb na fyzickou implementaci modelu a bez vazeb na reálné provozní podmínky. V současnosti používané kryptografické algoritmy jsou při použití dostatečně dlouhých šifrovacích klíčů v podstatě neprolomitelné a konvenční kryptoanalýza je neefektivní.

Nový způsob kryptoanalýzy přináší využití postranních kanálů. Model útoku za použití postranních kanálů je rozšířen o fyzické projevy modulu během průběhu kryptografických operací.

Tato dizertační práce obsahuje popis kryptografických modulů a zkoumá vliv postranních kanálů na bezpečnost těchto modulů.

ABSTRACT

The conventional way of cryptanalysis is based on the cryptographic algorithms weak points examine. The attack model of conventional cryptanalysis covers mathematical description of the cryptographic algorithm used. This model is without any relation to the physical model implementation and without any relation to the real environment. Cryptographic algorithms currently used in the combination with strong cipher keys are almost unbreakable and the conventional cryptanalysis is ineffective.

The new way of cryptanalysis employs the side channels. The model of cryptanalysis using side channels is enhanced with physical behavior of the module performing the cryptographic operations.

This dissertation thesis deals with cryptographic module description and studies influence of these side channels on the security of this module.