FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

# Hodnocení vedoucího závěrečné práce

| | |
|---|---|
| **Student:** | Bc. Tomáš Balihar |
| **Vedoucí: práce:** | Dr.-Ing. Martin Novotný |
| **Název práce:** | Influence of Synthesis Parameters on Vulnerability to Side-Channel Attacks |
| **Obor:** | Návrh a programování vestavných systémů |

**Datum vytvoření:** 24. 8. 2020

| *Hodnotící kritérium:* | *Způsob hodnocení – následující škálou 1 až 4:* |
|---|---|
| **1. Splnění zadání** | ***1=zadání splněno,***<br>*2=zadání splněno s menšími výhradami,*<br>*3=zadání splněno s většími výhradami,*<br>*4=zadání nesplněno* |

*Popis kritéria:*
Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

*Komentář:*

Práce splňuje zadání ve všech bodech. Práce byla zejména časově velmi náročná (měření trvala několik týdnů). S dnešním vybavením, jímž disponujeme od června, bychom byli schopni tato měření provést ve zlomku tohoto času.

| *Hodnotící kritérium:* | *Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **2. Písemná část práce** | *78 (C)* |

*Popis kritéria:*
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti. Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3. Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

*Komentář:*

Práce navazuje na diplovou práci Ing. Jana Brejníka "Obrany proti útokům postranními kanály založené na dynamické rekonfiguraci FPGA ". Přivítal bych proto detailnější souhrn předchozí diplomové práce. Zejména mi schází blokové schéma zkoumané šifry (AES) s implementovanými ochranami. Z tohoto schématu by bylo zřejmé rozmístění jednotlivých částí obvodu (poloha registrů, S-boxů, apod.) a poté by bylo možné provést i toretickou úvahu o tom, jaký vliv na ochrany může mít například Register Balancing. Rešeršní část by mohla být obsáhlejší a obsahovat více odkazů na aktuální publikace, avšak na druhou stranu, text obsahuje odkazy na všechny publikace skutečně nezbytné pro tuto práci.

| *Hodnotící kritérium:* | *Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **3. Nepísemná část, přílohy** | *95 (A)* |

*Popis kritéria:*
Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce
– opakovatelnost experimentů

*Komentář:*

Nepísemná část představuje úpravu stávajícího měřícího softwaru a zejména pak 108 syntéz a implementací pro 108 různých nastavení parametrů, následovaných analýzou bitstreamů a časově rozsáhlými měřeními. Pro prvních osm konfigurací parametrů autor naměřil po 1.000.000 průběhů spotřeby, pro zbývajích 46 unikátních bitstreamů naměřil po 300.000 průbězích.

| *Hodnotící kritérium:* | *Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **4. Hodnocení výsledků, jejich využitelnost** | *95 (A)* |

*Popis kritéria:*
Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

*Komentář:*

Provedená měření dávají nahlédnout, jaké syntézní parametry jsou kritické z hlediska ochrany proti útokům postranními kanály. Získané výsledky plánujeme publikovat. Bylo by zajímavé zanalyzovat, jakým způsobem se změnilo zapojení obvodu, pokud byly optimalizace zapnuté (Zejména pokud bylo Keep Hierarchy vypnuté a Register Balancing povolený).

| *Hodnotící kritérium:* | *Způsob hodnocení – následující škálou 1 až 5:* |
|---|---|
| **5. Aktivita a samostatnost studenta** | 5a:<br>***1=výborná aktivita,***<br>*2=velmi dobrá aktivita,*<br>*3=průměrná aktivita,*<br>*4=slabší, ale ještě dostatečná aktivita,*<br>*5=nedostatečná aktivita*<br>5b:<br>***1=výborná samostatnost,***<br>*2=velmi dobrá samostatnost,*<br>*3=průměrná samostatnost,*<br>*4=slabší, ale ještě dostatečná samostatnost,*<br>*5=nedostatečná samostatnost* |

*Popis kritéria:*
V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

*Komentář:*

Student pravidelně konzultoval postup prací. Mírnou překážkou byla koronavirová karanténa, která způsobila drobné zpoždění prací.

| *Hodnotící kritérium:* | *Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **6. Celkové hodnocení** | *89 (B)* |

*Popis kritéria:*
Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.

*Text hodnocení:*

Zadání práce bylo splněno beze zbytku. Postrádám však detailnější popis analyzovaného obvodu, formou například blokového schématu. Do budoucna by bylo zajímavé zanalyzovat, jak konkrétně se mění zapojení obvodu při zapnutých optimalizacích a dovodit, proč zapnuté optimalizace mají tak významný vliv na odolnost obvodu proti útokům postranními kanály. Dále by bylo zajímavé zanalyzovat i jiné obvody (např. šifru PRESENT) s implementovanými ochranami, a rovněž tak by bylo možné zanalyzovat vliv nastavení syntézních parametrů i na jiné typy ochran, například Threshold Implementations, aj.

Podpis vedoucího práce: