FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Jan Brejník
Oponent práce:	Dr.-Ing. Martin Novotný
Název práce:	Obrany proti útokům postranními kanály založené na dynamické rekonfiguraci FPGA
Obor:	Návrh a programování vestavných systémů

Datum vytvoření: 18. 1. 2019

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *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:
Předložená diplomová práce svým rozsahem a zejména objemem a kvalitou provedených prací odpovídá zhruba třem (možná i více) standardním diplomovým pracím.
- Úkolem autora bylo reimplementovat šifru PRESENT s ochranami proti útokům postranními kanály a poté tyto ochrany aplikovat na šifru AES. Autor však nejenom implementoval šifru PRESENT a AES, ale navíc tyto ochrany aplikoval i na šifru SERPENT a na variantu šifry AES, v které se výpočet S-boxu provádí prostřednictvím transformace do kompozitního tělesa. Tuto variantu šifry AES navíc implementoval ve dvou verzích a v kapitole Budoucí práce navrhuje ještě třetí verzi. Pro transformaci do kompozitního tělesa musel navíc autor nastudovat náročný matematický aparát. Toto by vystačilo na více jak jednu diplomovou práci.
- Úkolem autora bylo "provést alespoň několik pokusných měření". Autor provedl minimálně 83 měření, když pro každou variantu hardwaru vyzkoušel vliv jednotlivých ochran a jejich kombinací. Každé měření přitom trvalo cca 1,5 hodiny v případě méně důležitých měření (kdy měřil pouze 300.000 průběhů spotřeby) až cca 5 hodin v případě důležitých měření, kdy měřil 1.000.000 průběhů spotřeby. Toto by vystačilo na druhou práci.
- Dále autor vytvořil dva automatické generátory VHDL kódu, které značí jako DynReconfGen a DynReconfGen3. Toto by vystačilo na třetí práci.
- Dále autor vytvořil rozsáhlou dokumentaci na přiloženém DVD. Stačí nahlédnout do adresářů GfReports a Results.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*99 (A)*

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 je členěná přehledně a napsána srozumitelně. Obsahově je více než bohatá. Kromě samotné práce, která má 119 stran, autor vytvořil rozsáhlou dokumentaci i na přiloženém DVD. Pokud se týče nedostatků v textu práce, jedná se pouze o drobnosti. Například, autor se v textu neodkazuje na některé obrázky (např. obrázek 1.1 či 1.11; z popisku obrázku je ale jasné, ke které části textu se obrázek vztahuje), občas autor místo slova "prvek" (tělesa) používá termín "element" nebo místo slova "zobrazení" občas používá slovo "mapování", a v malé míře se v textu také vyskytují překlepy. Věřím, že tyto drobnosti by se odstranily po kontrole třetí osobou.

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

Jak bylo řečeno výše, autor navrhl dva generátory VHDL kódů. Generátory použil pro implementaci celkem pěti obvodů (PRESENT, SERPENT, AES základní, AES s kompozitním tělesem, AES s kompozitním tělsem pokročilý). Navržené obvody proměřil. Vše zdokumentoval. Doporovodná dokumentace na DVD zabírá váce jak 2 GB.

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

Z diplomové práce plánujeme vytvořit několik publikací.

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*
5. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:

V tento moment mě žádný dotaz nenapadá.

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

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:

Vytvořená diplomová práce svojí kvalitou i kvantitou výrazně převyšuje běžné diplomové práce. Nezbývá mi než hodnotit práci nejvyšším stupněm. Zároveň si dovoluji doporučit komisi, aby předloženou diplomovou práci nominovala na cenu děkana.

Podpis oponenta práce: