FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Ondřej Semrád
Oponent práce:	Ing. Petr Socha
Název práce:	Fast data-acquisition tools for side-channel analysis in FPGA
Obor:	Návrh a programování vestavných systémů

Datum vytvoření: 7. 6. 2020

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:
Práce se zabývá hardwarovou i softwarovou podporou pro analýzu postranních kanálů kryptografických FPGA implementací. Student splnil zadání bez výhrad.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*89 (B)*

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:
Písemná práce je celkově jazykově na dobré úrovni, koherentní a čtivá. Úvodní kapitola práce, state-of-the-art, je velmi stručná a obsahuje drobné nepřesnosti. Navazující kapitoly, popisující návrh, implementaci a testování výsledného řešení, jsou věcné a informačně bohaté. Použité zdroje odpovídají povaze práce.

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:
Navržené řešení sestává z VHDL návrhu, umožňujícího zapouzdření testované kryptografické implementace a provedení definovaných testů/měření. Při tom využívá dvou FPGA na dedikované desce Sakura-G, kdy jedno FPGA slouží jako řídící, a druhé FPGA obsahuje testovanou implementaci. Dále řešení obsahuje sadu podpůrných scriptů v Pythonu, usnadňujících nasazení a verifikaci. Poslední částí řešení je C++ plug-in pro softwarový toolkit SICAK, zajišťující komunikaci s FPGA a řízení testovacího procesu z osobního počítače.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*90 (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:

Výstupem práce je univerzální řešení podporující testování odolnosti kryptografických FPGA implementací proti útokům postranními kanály. Navržené řešení urychluje specifické měření spotřeby, tradiční úzké hrdlo testování, natolik, že novým úzkým hrdlem se stává i v nejjednodušších případech až následné statistické zpracování naměřených dat. Využitelnost výsledků práce částečně snižuje pouze absence stručnějšího uživatelského manuálu, kdy uživatel je odkázán pouze na obsáhlý text diplomové práce.

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:

1) FPGA na Sakura-G nejsou vybavena chladiči. Zabýval jste se příkonem a termálními nároky FPGA při delším intenzivním měření?
2) Co obnáší změna hodinové frekvence pro testovaný obvod?
3) Co by obnášelo přenesení řešení na novější platformu Sakura-X?

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

6. Celkové hodnocení

95 (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:

Student při řešení prokázal schopnost samostatné kreativní práce, která vyžadovala znalost problematiky postranních kanálů a znalost číslicového i softwarového návrhu. Výsledky práce budou dále využívány při výzkumu na KČN. Práci navrhuji ohodnotit známkou A - výborně.

Podpis oponenta práce: