

Hodnocení vedoucího závěrečné práce

České vysoké učení technické v Praze

Fakulta informačních technologií

Student: Jan Říha
Vedoucí práce: Dr.-Ing. Martin Novotný
Název práce: Útok postranními kanály na implementaci algoritmu AES na platformě Altera
Obor: Počítačové inženýrství

Datum vytvoření: 9. 6. 2017

Hodnotící kritérium: 1. Náročnost a další komentář k zadání	Způsob hodnocení - následující škálou 1 až 5: 1=mimořádně náročné zadání, 2=náročnější zadání, 3=průměrně náročné zadání, 4=lehčí, ale ještě dostatečně náročné zadání, 5=nedostatečně náročné zadání
Popis kritéria: Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.) Komentář: Práce je výzkumného charakteru. Student si musel samostudiem osvojit problematiku vyučovanou až v rámci magisterského studia. Nad rámec magisterských znalostí si musel osvojit aplikaci rozdílové odběrové analýzy na obvody FPGA.	
Hodnotící kritérium: 2. Splnění zadání	Způsob hodnocení - následující škálou 1 až 4: 1=zadání splněno, 2=zadání splněno s menšími výhradami, 3=zadání splněno s většími výhradami, 4=zadání nesplněno
Popis kritéria: Posuďte, zda předložená ZP splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků. Komentář: Zadání bylo beze zbytku splněno. Na základě výsledků práce vznikl příspěvek na konferenci Euromicro DSD 2017.	
Hodnotící kritérium: 3. Rozsah písemné zprávy	Způsob hodnocení - následující škálou 1 až 4: 1=splňuje požadavky, 2=splňuje požadavky s menšími výhradami, 3=splňuje požadavky s většími výhradami, 4=nesplňuje požadavky
Popis kritéria: Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Komentář: Rozsahem 58 stran práce překračuje běžné bakalářské práce. Nezaznamenal jsem zbytečnosti ani chybějící informace.	
Hodnotící kritérium: 4. Věcná a logická úroveň práce	Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F): 100 (A)
Popis kritéria: 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. Komentář: Práce je strukturována logicky, autor systematicky postupuje k cíli. Práce je srozumitelná, jednotlivé kapitoly na sebe logicky navazují.	
Hodnotící kritérium: 5. Formální úroveň práce	Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F): 100 (A)
Popis kritéria: Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 14/2015, článek 3. Komentář: Práce možná obsahuje několik překlepů, já jsem je ale nezaznamenal.	
Hodnotící kritérium: 6. Práce se zdroji	Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F): 100 (A)
Popis kritéria: Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a uvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.	

Komentář:

Autor cituje 25 pramenů. Vzhledem k aktuálnosti tématu je nejstarší (prvotní) zdroj terpve z roku 1999.

Hodnotící kritérium:

Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):

7. Hodnocení výsledků, publikační výstupy a ocenění

100 (A)

Popis kritéria:

Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:

Jak jsem zmínil v úvodu, jednalo se o výzkumnou práci. Autor zkoumal problematiku, kterou se, podle našeho nejlepšího vědomí, nikdo doposud nezabýval. K dispozici byly pouze prameny, které se zabývaly podobnými tématy, např. kolega Francesco Regazzoni se zabýval vlivem obran proti tzv. fault-injection útokům na odolnost proti rozdílové odběrové analýze (DPA). Dlužno však podotknout, že rozdílů mezi jeho a naší prací je více: 1) Regazzoni se zabýval obranami proti fault-injection útokům, kdežto my jsme se zabývali fault-tolerant architekturami, 2) Regazzoni se zaměřil na ASIC, kdežto my na FPGA, 3) Regazzoni používal simulaci, kdežto my jsme požívali měření na reálném obvodu.

Hodnotící kritérium:

Způsob hodnocení - nehodnotí se

8. Komentář o využitelnosti výsledků

Popis kritéria:

Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:

Výsledky bakalářské práce byly zpracovány jako článek, který byl přijat k prezentaci na konferenci Euromicro DSD 2017, která se bude konat 30.8.-1.9.2017 ve Vídni.

Hodnotící kritérium:

Způsob hodnocení - následující škálou 1 až 5:

9. Aktivita a samostatnost studenta v průběhu řešení

9a:

1=výborná aktivita,
2=velmi dobrá aktivita,
3=průměrná aktivita,
4=slabší, ale ještě dostatečná aktivita,
5=nedostatečná aktivita

9b:

1=výborná samostatnost,
2=velmi dobrá samostatnost,
3=průměrná samostatnost,
4=slabší, ale ještě dostatečná samostatnost,
5=nedostatečná samostatnost

Popis kritéria:

Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (9a). Posuďte schopnost studenta samostatně tvůrčí práce (9b).

Komentář:

Student často konzultoval svoji práci. Text práce měl hotový minimálně dva týdny před uzávěrkou, takže zbylo ještě dost času na doladění detailů. Práci student odevzdal s týdenním předstihem, jako jeden z prvních.

Hodnotící kritérium:

Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):

10. Celkové hodnocení

100 (A)

Popis kritéria:

Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:

Předložená výzkumná práce je na vysoké úrovni. Na základě práce vzniknul příspěvek, který byl přijat na konferenci Euromicro DSD 2017. Doporučuji komisi, aby práci navrhla na cenu děkana.

Podpis vedoucího práce: