Hodnocení vedoucího závěrečné práce

České vysoké učení technické v Praze **Fakulta informačních technologií**

Student: Bc. Lukáš Mazur
Vedoucí práce: Dr.-Ing. Martin Novotný
Název práce: Side channel analysis of cryptographic algorithms implementations
Obor: Počítačové inženýrství

Datum vytvoření: 27. 1. 2017

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	*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:
Jednalo se průzkumnou/výzkumnou práci s nejistým výsledkem. Přestože jsme měli zkušenosti s aplikací rozdílové odběrové anlýzy (DPA) na čipové karty, s její aplikací na číslicové obvody implementované v FPGA jsme dosud žádné zkušenosti neměli.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. 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 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.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	***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:
Zpráva pokrývá problematiku a neobsahuje žádné zbytné pasáže.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*95 (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 logicky a přehledně členěna.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*95 (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 ja psaná v angličtině, takže se neodvažuji hodnotit pravopis ani stylistiku. Nicméně, na základě mých znalostí se zdá být vše po gramatické a stylistické stránce v pořádku. Formální zápisy se zdají rovněž být v pořádku.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*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 úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
Autor cituje 34 zdrojů. Nanarazil jsem na to, že by autor porušil citační etiku - všechny převzaté prameny se zdají být řádně ocitovány. Bibliografické citace se zdají být úplné.

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:
Po řadě neúspěšných cest, které autor důkladně zdokumentoval, se mu nakonec (po návštěvě dr. Amira Moradiho z Ruhr-University Bochum v srpnu 2016) podařilo aplikovat metodu DPA i na kryptografický systém realizovaný v FPGA. Poté provedl ještě několik pokusů ve zhoršených měřících podmínkách (např s neodstraněnými blokovacími kondenzátory nebo s napájením ze spínaného zdroje), aby zjistil, jaký mají tyto nepříznivé faktory vliv na kvalitu útoku. Tato měření rovněž zdokumentoval. Práce slouží jako užitečný podklad pro další průzkumníky v této oblasti.

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:
Práce slouží jako podklad pro další výzkum, ve kterém pokračujeme.

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 samostatné tvůrčí práce (9b).

Komentář:
Autor průběžně konzultoval dosažené výsledky s vedoucím práce. Na práci pracoval jak v hardwarové laboratoři fakulty, tak doma.

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 práce dokumentuje výzkumné aktivity studenta v průběhu tří semestrů, od října 2015 až těsně po odevzdání textu práce v lednu 2017. Během prvních dvou semestrů student provedl řadu neúspěšných pokusů. Po návštěvě dr. Amira Moradiho z Ruhr-University Bochum a konzultaci s ním se mu následně podařilo provést úspěšný útok. Následně testoval několik variant měřícího prostředí a jeho vliv na úspěšnost útoku. Všechny slepé cesty i úspěšné pokusy jsou zdokumentovány a práce tak slouží jako podklad budoucím průzkumníkům.

Zadání bylo zcela splněno, ba překročeno, protože provedení úspěšného útoku nebylo požadováno v zadání práce. Množství odvedené práce přesahuje rámec běžné bakalářské práce.

Doporučuji, aby komise navrhla předloženou práci na cenu děkana.

Podpis vedoucího práce: