

# Posudek oponenta závěrečné práce

České vysoké učení technické v Praze

Fakulta informačních technologií

**Student:** Jan Říha  
**Oponent práce:** Ing. Vojtěch Miškovský  
**Název práce:** Útok postranními kanály na implementaci algoritmu AES na platformě Altera  
**Obor:** Počítačové inženýrství

**Datum vytvoření:** 9. 6. 2017

<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení - následující škálou 1 až 5:</b>
<b>1. Náročnost a další komentář k zadání</b>	<b>1=mimořádně náročné zadání, 2=náročnější zadání, 3=průměrně náročné zadání, 4=lehčí, ale ještě dostatečně náročné zadání, 5=nedostatečně náročné zadání</b>
<b>Popis kritéria:</b> 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.)	
<b>Komentář:</b> Tato práce navazuje na dřívější práce věnující se rozdílové odběrové analýze a dále na práci věnující se spolehlivostním variantám šifry AES. Ačkoli byla nemalá část implementace převzata z těchto prací, autor musel pro splnění zadání skloubit znalosti návrhu hardware i software a také další znalosti vyučované až v magisterském studiu. Proto považuji zadání za nadprůměrně náročné.	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení - následující škálou 1 až 4:</b>
<b>2. Splnění zadání</b>	<b>1=zadání splněno, 2=zadání splněno s menšími výhradami, 3=zadání splněno s většími výhradami, 4=zadání nesplněno</b>
<b>Popis kritéria:</b> 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.	
<b>Komentář:</b> Zadání bylo bez výhrad splněno.	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení - následující škálou 1 až 4:</b>
<b>3. Rozsah písemné zprávy</b>	<b>1=splňuje požadavky, 2=splňuje požadavky s menšími výhradami, 3=splňuje požadavky s většími výhradami, 4=nesplňuje požadavky</b>
<b>Popis kritéria:</b> Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.	
<b>Komentář:</b> Rozsah práce je vysoce nadprůměrný. Práce je informačně bohatá a neobsahuje nadbytečné informace.	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):</b>
<b>4. Věcná a logická úroveň práce</b>	<b>96 (A)</b>
<b>Popis kritéria:</b> 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.	
<b>Komentář:</b> Věcná i logická úroveň práce je velmi vysoká. Upozornil bych pouze na střídání slov průběh a stopa (kapitola 5), která jsou zde používána ve stejném významu a jejichž střídání může čtenáře mást. Dále v sekci 3.2.3 došlo k záměně funkce or za xor.	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):</b>
<b>5. Formální úroveň práce</b>	<b>99 (A)</b>
<b>Popis kritéria:</b> Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 14/2015, článek 3.	
<b>Komentář:</b> Práce obsahuje jen velice malé množství překlepů, jinak není co vytknout.	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):</b>
<b>6. Práce se zdroji</b>	<b>100 (A)</b>

**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 využívá relevantní zdroje, korektně je cituje a jejich výsledky jasně odděluje od vlastních.

**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:**

Tato práce je součástí rozsáhlejšího výzkumu na KČN. Autorovy výsledky byly zpracovány do vědeckého článku, který prošel recenzním řízením a byl úspěšně přijat na konferenci DSD 2017.

**Hodnotící kritérium:**

*Způsob hodnocení - nehodnotí se*

**8. Komentář o využitelnosti výsledků**

**Popis kritéria:**

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

**Komentář:**

Výsledky jsou součástí širšího výzkumu, nicméně autorovy závěry by mohly být již nyní uplatňovány v praxi.

**Hodnotící kritérium:**

*Způsob hodnocení - nehodnotí se*

**9. Otázky k obhajobě**

**Popis kritéria:**

Uvedte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

**Otázky:**

Výsledky uvedené v [15] ukazují, že metody zabezpečení proti chybám mají negativní dopad na odolnost proti DPA, což je v rozporu s autorovými výsledky. Mohl by se autor pokusit odůvodnit tento rozpor?

**Hodnotící kritérium:**

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

**10. Celkové hodnocení**

99 (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:**

Zadání práce bylo nadprůměrně náročné a autor se dopracoval k požadovaným výsledkům. Práce je zpracována velice kvalitně. Výsledky práce byly přijaty jako příspěvek na mezinárodní konferenci. S ohledem na tato fakta nelze než doporučit práci k obhajobě a ohodnocení stupněm A.

Podpis oponenta práce: