# Hodnocení oponenta diplomové práce

Autor práce: **Bc. Jessica FENCLOVÁ**

Název práce: **Odběrová analýza na platformě FPGA**

## Splnění zadání

splněno

## Zhodnocení odborné úrovně práce

Studentka velmi zdařile představuje možnosti hardwarových útoků na šifrovací zařízení. Velmi dobře obhajuje motivaci a aktuálnost dané problematiky. V teoretickém úvodu autorka seznamuje čtenáře se základními postuláty a terminologií.
Bohužel praktická část práce je příliš stručná. Obsahuje simulaci v MATLAB a implementaci AES Sbox procedury spolu s podpůrnými moduly pro řízení experimentu a interface založený na UARTu. V závěru je nastíněn CPA/DPA experiment, který může být s takto implementovaným systémem proveden. Je velká škoda, že se nepodařilo ukázkový experiment realizovat (bylo to součástí původního zadání). Není též zřejmé, zda ověření činnosti proběhlo při reálném provozu zařízení či jen pomocí VHDL simulací. Implementace algoritmu je možná až příliš atomizována do velkého počtu entit, nicméně to nemá na výslednou funkci vliv.
Je nutné konstatovat, že práce obecně splňuje redukované zadání práce dle dodatku z 16.3.2021.

## Zhodnocení formální úrovně a práce s literaturou

Formální úroveň práce hodnotím nadprůměrně. Je psána dobrou angličtinou a rozumně strukturována. V úvodu studentka popisuje hlavní motivaci a představuje jednotlivé typy hardwarových útoků na šifrovací algoritmy. Dále se pak věnuje hlavnímu předmětu práce, a to jsou útoky pomocí odběrové analýzy. V krátkosti představuje i obvody FPGA. Druhá část práce se věnuje praktickému přínosu a popisuje simulace a implementaci části šifrovacího algoritmu v FPGA. Nutno zmínit, že tato část je velmi stručná. Text je dostatečně prokládám citacemi na použité zdroje. Možná by práci prospělo více obrázků a diagramů místo slovního popisu. Práce je psána řádkováním 1 (či 1.15) a tak se celkový počet stránek může zdát nižší, než je obvyklé.
Příloha práce odkazuje na Git repozitář se zdrojovými kódy, kterou jsou výsledkem diplomové práce.

## Doporučení k obhajobě

Doporučuji k obhajobě

## Dotazy k práci

- Má výběr konkrétního FPGA obvodu vliv na provedení CPA/DPA?
- Uvádíte, že výsledný FPGA design umožňuje běh až na 170MHz. Je možné tento kmitočet zvýšit? Popřípadě uveďte, co jsou limitující faktory.

---

V ---------- dne ---------- Ing. Petr Burian, Ph.D.