POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Návrh HW akcelerátoru Keccak hashovacího algoritmu pro SoC platformu**
Jméno autora:	**Nikita Litvishko**
Typ práce:	diplomová
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra mikroelektroniky
Oponent práce:	Ing. Jan Kovalský
Pracoviště oponenta práce:	Adesto Technologies

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání **náročnější**

Hodnocení náročnosti zadání závěrečné práce.

Zadání diplomové práce vyžadovalo od studenta velké množství samostudia v přípravě na samotné řešení. Student si musel nejprve osvojit teoretické základy Keccak algoritmu, nastudovat syntaxi Verilog 2001 jazyka, ve kterém bylo nutné HW akcelerátor naimplementovat, připravit simulaci k ověření správné funkcionality HW akcelerátoru, nalézt SW implementaci Keccak algoritmu vhodnou pro požadovaný MicroBlaze procesor, nadefinovat metodu porovnání výkonu obou řešení a provést porovnání získaných výsledků. Celkový záběr těchto aktivit vyžadoval značné úsilí studenta, proto zadání hodnotím jako náročnější.

Splnění zadání **splněno**

Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Zadání diplomové práce bylo splněno v plném rozsahu.

Zvolený postup řešení **vynikající**

Posuďte, zda student zvolil správný postup nebo metody řešení.

Student Litvishko zvolil při návrhu HW akcelerátoru správný postup, který mu umožnil jak otestovat samotný blok a algoritmus on úrovni FPGA tak jej připravit pro snadnou integraci do SoC obvodu na úrovni ASIC. Pro porovnání výhodnosti použití HW akcelerátoru v SoC architekturách byla také využita SW implementace tohoto algoritmu od třetí strany, která umožnila snadné řízení a tedy i porovnání rychlosti zpracování vstupních dat.

Odborná úroveň **A - výborně**

Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.

Práce byla zpracována velice pečlivě na teoretické úrovni ještě před samotným započetím praktického řešení. Student strávil dostatečné množství času studiem principů Keccak algoritmu a také hledáním vhodného SW řešení, které by mohlo být použito k porovnání s výkonem HW akcelerátoru. Při samotné implementaci HW akcelerátoru a testovací SoC architektury student také řešil typické problémy jako jsou například přechody hodinových domén, které bylo nutné správně implementovat. Implementované řešení ukazuje správné použití metodologií, které se v praxi používají.

Formální a jazyková úroveň, rozsah práce **A - výborně**

Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.

Po formální stránce je práce velice zdařilá. Student si zvolil jako jazyk diplomové práce angličtinu, což hodnotím velice kladně. I když se v textu někdy objevují překlepy, nijak to nesnižuje kvalitu samotné práce. V některých odstavcích jsou věty zapsány trochu kostrbatě a mohly by být zjednodušeny pro zachování lepší srozumitelnosti. Jazyková úroveň i rozsah práce jsou na dobré úrovni.

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

Výběr zdrojů, korektnost citací	**A - výborně**
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. 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.	
Výběr literatury byl vhodně zvolen. Student čerpal z odborné literatury jak teoretické znalosti k principům Keccak algoritmů tak technické detaily k použitým blokům FPGA obvodů firmy Xilinx nebo SW implementacím Keccak algoritmů.	

Další komentáře a hodnocení
Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.
Výsledné technické řešení na úrovni RTL včetně dodatečných podpůrných SW skriptů odpovídá zvyklostem a postupům, které se standardně používají v praxi. Student si při řešení zadání osvojil mnoho nových praktických zkušeností, které se budou hodit v jeho další profesní kariéře.

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Uveďte případné otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.

Samotné zadání diplomové práce vyžadovalo zodpovědný přístup jak během teoretické přípravy tak při praktické realizaci. Student se s tímto úkolem vypořádal na vysoké úrovni a nabídnuté výsledné řešení IP bloku HW akcelerátoru lze považovat za připravené k využití v praxi.

Velice oceňuji také snahu studenta dodat společně s RTL zdrojovými kódy sadu podpůrných python skriptů, které umožňují automatickou generaci RTL kódu implementující strukturu SHA-3 funkce.

V neposlední řadě pak chci vyzdvihnout komplexnost výsledného řešení a šíři záběru nových znalostí a praktik, které si student musel během řešení zadání osvojit.

Výsledné porovnání rychlosti zpracování vstupních dat HW akcelerátorem a SW řešením, stejně tak úroveň RTL a ostatních zdrojových kódů společně s textem diplomové práce hodnotím jako velice zdařilé.

Otázky k obhajobě:

1. Pokud bychom chtěli výsledné řešení optimalizované pro platformu FPGA použít v ASIC obvodu, které bloky nebo části návrhu by bylo nutné upravit pro ASIC implementaci?
2. Existují v předloženém řešení nějaké části, které by se daly dále vylepšit nebo rozšířit?

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **A - výborně.**

Datum: 15.6.2020 Podpis: