POSUDEK VEDOUCÍHO 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
Vedoucí práce:	prof. Ing. Pavel Hazdra, CSc.
Pracoviště vedoucího práce:	Katedra mikroelektroniky FEL ČVUT v Praze

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání **náročnější**

Hodnocení náročnosti zadání závěrečné práce.

Cílem diplomové práce byla hardwarové implementace SHA-3 hashovací funkce využívající algoritmus KECCAK v programovatelném hradlovém poli Artix 7 firmy Xilinx. Diplomant musel prostudovat způsoby realizace SHA-3 hashovací funkce s využitím KECCAK algoritmu, implementovat jej na úrovni RTL, ověřit návrh simulací i hardwarovou implementací v systému na čipu (SoC) využívajícím soft processor MicroBlaze v programovatelném hradlovém poli Artix 7. Součástí práce bylo ověření efektivity hardwarového akcelerátoru srovnáním s čistě softwarovým řešením. Diplomant zadané téma zpracovával od základů a hodnotím jej jako náročné.

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.

Diplomant, dle mého názoru, bezezbytku splnil všechny požadavky zadání. Diplomová práce a její přílohy dokumentují, že detailně prostudoval možnosti realizace SHA-3 hashovací funkce algoritmem KECCAK, provedl jeho analýzu a implementoval jej na úrovni RTL v jazyce Verilog generovaném Python skriptem. Vlastní návrh koprocesoru ověřil simulací i hardwarovou implementací v SoC se soft processorem MicroBlaze na vývojové desce Digilent Nexys Video FPGA Board vybavené programovatelném hradlovém poli Artix 7. Vytvořil nezbytný firmware pro akcelerátor a detailně ověřil efektivitu hardwarového akcelerátoru srovnáním s čistě softwarovým výpočtem prováděným processorem MicroBlaze.

Aktivita a samostatnost při zpracování práce **A - výborně**

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

Diplomant pracoval na své práci samostatně a iniciativně. Postup na své práci průběžně konzultoval s vedoucím. Práce byla v úplnosti, včas a úspěšně dokončena.

Odborná úroveň **A - výborně**

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

Zpracování diplomové práce je, dle mého názoru, příkladné. Diplomant v detailu popisuje jak vlastní implementaci koprocesoru, tak všechny etapy návrhu i závěrečného zhodnocení. Práce je doplněna nezbytnými přílohami. Prokázal, že je schopen využívat nabytých znalostí i poznatků získaných z odborné literatury. Implementovaný koprocesor je plně funkční a přináší značné zrychlení výpočtu SHA-3 hashovací funkce.

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

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

Diplomová práce napsaná v angličtině je po formální, typografické i jazykové stránce na velmi dobré až vynikající úrovni.

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK VEDOUCÍHO 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.	
Diplomant ve své práci využil odpovídající a relevantní zdroje. Citované partie a vlastní úvahy diplomanta jsou řádně odlišeny.	

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.
Výstupem práce je funkční a otestovaný koprocesor implementující SHA-3 funkci algoritmem KECCAK. Diplomant prokázal při řešení práce svou odbornost, důslednost i experimentální zručnost.

III. CELKOVÉ HODNOCENÍ A NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení.

Diplomová práce Nikity Litvishka se zabývá hardwarovou implementací SHA-3 hashovací funkce využívající algoritmus KECCAK v programovatelném hradlovém poli Artix 7 firmy Xilinx. Dokladuje, že detailně prostudoval možnosti realizace SHA-3 hashovací funkce algoritmem KECCAK, provedl jeho analýzu a implementoval jej na úrovni RTL v jazyce Verilog generovaném Python skriptem. Vlastní návrh koprocesoru ověřil simulací i hardwarovou implementací v SoC se soft processorem MicroBlaze na vývojové desce Digilent Nexys Video FPGA Board vybavené programovatelném hradlovém poli Artix 7. Vytvořil nezbytný firmware pro akcelerátor a detailně ověřil efektivitu hardwarového akcelerátoru srovnáním s čistě softwarovým výpočtem prováděným processorem MicroBlaze. Výstupem práce je funkční a otestovaný koprocesor implementující SHA-3 funkci algoritmem KECCAK. Zpracování diplomové práce je, dle mého názoru, příkladné. Diplomant v detailu popisuje jak vlastní implementaci koprocesoru, tak všechny etapy návrhu i závěrečnou kvantifikaci akcelerace.

Diplomant bezezbytku splnil všechny požadavky zadání a podařilo se mu realizovat plně funkční zařízení, které v praxi vyzkoušel. Vlastní text diplomové práce výstižně charakterizuje postup řešení a je technicky na velmi dobré úrovni. Diplomová práce je důkazem toho, že je diplomant schopen samostatně tvořivě pracovat a uplatňovat studiem nabyté poznatky v inženýrské praxi.

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

Datum: 15.6.2020 Podpis: prof. Ing. Pavel Hazdra, CSc. v.r.