KOMISIJI ZA STUDIJE II STEPENA ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Komisija za studije II stepena, Elektrotehničkog fakulteta u Beogradu, na svojoj sednici održanoj 02.06.2015. godine imenovala nas je u Komisiju za pregled i ocenu master rada dipl. inž. Danila Šijačića pod naslovom „Hardverska implementacija PRIMATEs familije algoritama''. Nakon pregleda materijala Komisija podnosi sledeći

IZVEŠTAJ

1. Biografski podaci kandidata

Danilo Aleksandar Šijačić rođen je u Beogradu 3. aprila 1990. godine. Kao nosilac diplome „Vuk Karadžić''—zasluzene na prirodno-matematičkom smeru u Prvoj beogradskoj gimnaziji—upisao je osnovne akademske studije na Elektrotehničkom fakultetu u Beogradu, septembra 2009. godine. Godinu dana kasnije, Danilo se pridružio odseku za elektroniku, gde je uspešno položio sve ispite do 2013. Godine. Pre nego što će diplomirati, Danilo se odlučio za godinu dana rada u industriji, primenjujući znanja elektronike u oblasti zaštite podataka u uređajuma posebne namene. Konačno, Danilo je početkom oktobra 2014. Godine uspešno odbranio diplomski rad sa ocenom 10—završavajući osnovne studije sa prosečnom ocenom 9.5—stekavši znanje diplomiranog inženjera elektrotehnike i računarstva.

Nakon toga Danilo je upisao master studije na svom matičnom odseku u Beogradu, i do danas sarađuje sa odsekom za kriptografiju i zaštitu podataka na Elektrotehničkom fakultetu univerziteta u Luvenu.

2. Opis master rada

Master rad kandidata napisan je na ukupno 63 strane. Glavnica rada smeštena je u 5 poglavlja uz jedan dodatak, uvodni sadržaj (tabela sadržaja, slika i tabela u radu), i spisak korišćene literature. Spisak literature sastoji se od 18 referenci.

Prvo poglavlje sadrži uvod i motivaciju za ovaj rad.

Drugo poglavlje sadrži opis pojmova na kojima počiva ovaj rad. Naime, opisana je PRIMATEs familija algoritama, kao i relevantne tehnike i platforme implementacije.

Treće poglavlje govori o hardverskim implementacijama permutacije na kojoj je bazirana PRIMATEs familija algoritama. Dobijeni rezultati su upoređeni i diskotovana je njihova moguća primena. Implementacije su optimizovane da koriste minimalne količine hardverskih resursa; za upotrenu u *lightweight* uređajima.

Četvrto poglavlje govori o arhitekturi koprocesora za enkripciju (dekripciju) korišćenjem nekog od algoritama iz PRIMATEs familije. Dizajnirani koprocesor baziran je na jednom od jezgara iz prethodnog poglavlja i omogućava izvršavanje različitih modova enkripcije.

Poslednje, peto, poglavlje sadrži zaključke autora i ideje za nastavak istraživanja na ovu temu.

3. Analiza rada sa ključnim rezultatima

Master rad dipl. inž. Danila Šijačića sadrži jednu paralelnu i tri serijske implementacije permutacije PRIMATEs familije algoritama.

Paralelna imlmenentacije ostvaruje odlične performanse, ali zauzima previše hardverskih resursa da bi bila prihvatljiva za upotrebu u *lightweight* uređajima.
Sa druge strane, sve tri serijske implementacije napravljene su tako da se minimizuje dodatna upotreba resursa vezanih za kontrolu toka izvršavanja. U zavisnosti od načina kako su implementirane transformacije podataka tokom permutacije dobijene su tri različite implementacije. Zbog velikog broja ciklusa potrebnog za izvršavanje jedna dobijena implementacija je podesna jedino za sisteme koji imaju veću učestanost signala takta od onih kojih su uobičajeni za *lightweight* uređaje. Preostale dve implementacije prevazilaze očekivanja modernih *lightweight* uređaja po pitanju performansi. Prema proceni autora u stanju su da obezbede do pet puta veći protok enkriptovanih podataka. Takođe, implementacije koriste daleko manje od *2000 GE,* što je procenjena granica resursa potrebna da se ispoštuje u *lightweight* udeđajima.
Pošto je istražio granice *lightweight* implementacija PRIMATE permutacije, Danilo je za svoj master rad dizajnirao i implementirao koprocesor baziran na najefikasnoj implementaciji jezgra. Koprocesor je osmišljen kao periferija za mikrokontroler is MSP430 familije mikrokontrolera. Celokupan sistem je spušten na odabranu FPGA platformu, uključujući *OpenMSP430* otvorenu implementaciju mikrokontrolera, i testiran radi dokazivanja funkcionalnosti. Interfejs koprocesora je napravljen da unosi minimalno kašnjenje i da zauzima minimalnu količinu dodatnih resursa. Dizajn podrazumeva kombinaciju hardvera i softvera, tako da se hardver jezgra može lako koristiti u za više modova enkripcije iz PRIMATEs familije. Performanse koprocesora procenjene su na oko 2.5 puta bolje od minimalnih potrebnih za *lightweight* uređaje.

Rezultati svih implementacija dati su za FPGA (Spartan-6 XC6SLX45-3CSG324) platformu, kao i ASIC rezultati u više biblioteka standardnih ćelija (npr. *NanGate 45nm*).

4. Zaključak i predlog

Kandidat, Danilo Šijačić, je u svom master radu uspešno implementirao jezgro PRIMATEs familije algoritama za enkripciju. Pored postignute funkcionalnosti, rad kandidata je optimizovan da koristi minimalnu količinu hardverskih resursa, pri tome ostvarujući performanse koje se mogu koristiti u stvarnim sistemima.

Kandidat je pokazao dozu inovativnosti u optimizaciji arhitekture odabranog algoritma, kao i temeljno znanje hardverskih imlementacija namenjenih za uredjaje sa ograničenim resursima. Takođe, kandidat je pokazao poznavanje izabrane oblasti koje prevazilazi trenutno ostvarene implementacije i ima inicijativu ka daljem unapredjivanju u ovoj oblasti.

Na osnovu gore-navedenog Komisija predlaže Komisiji za studije II stepena Elektrotehničkog fakulteta u Beogradu da prihvati rad „Hardverska implementacija PRIMATEs familije algoritama'' dipl. inž. Danila Šijačića kao master rad i odobri javnu usmenu odbranu.

U Beogradu, 14.09.2015.

dr Lazar Saranovac,
vanredni profesor, član komisije

dr Nenad Jovičić,
docent, član komisije