KOMISIJI ZA STUDIJE II STEPENA ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Komisija za studije II stepena Elektrotehničkog fakulteta u Beogradu na svom sastanku održanom 9.12.2014. godine imenovala nas je u Komisiju za pregled i ocenu master rada dipl. ing. Dušana Kostića, 2013/3195, pod naslovom „Primena Pollard Rho algoritma pomoću OpenCL tehnologije na grafičkim procesorima".

Komisija je pregledala priloženi rad i dostavlja Nastavno-naučnom veću Elektrotehničkog fakulteta u Beogradu sledeći

IZVEŠTAJ

1. Biografski podaci

Dušan Kostić je rođen 21.8.1990. godine u Pirotu. Osnovnu školu je završio kao nosilac Vukove diplome, a nakon toga je završio Gimnaziju u Pirotu. Elektrotehnički fakultet Univerziteta u Beogradu upisao je 2009. godine. Diplomirao je 2010. godine na Odseku za računarsku tehniku i informatiku, sa prosečnom ocenom 8,82 i ocenom 10 na diplomskom radu.

Master studije na Elektrotehničkom fakultetu, na Odseku za računarsku tehniku i informatiku, upisao je 2013. godine. Ispite predviđene nastavnim planom i programom položio je sa prosečnom ocenom 9,50.

2. Predmet, cilj i metodologija istraživanja

Većina današnjih kriptosistema se zasniva ili na problemu faktorizacije brojeva ili na problemu diskretnog logaritma. Najbrži poznati metod za rešavanje problema diskretnog logaritma u grupama eliptičnih kriva nad konačnim poljima je Pollard Rho algoritam.

Predmet ovog master rada je ispitivanje opravdanosti paralelizacije Pollard Rho algoritma za rešavanje problema diskretnog logaritma na eliptičnim krivama. Posle detaljne analize stanja u oblasti, zaključeno je da korišćenje OpenCL tehnologije pruža mogućnosti za paralelizaciju ovog algoritma na grafičkim procesorima i obećava značajno ubrzanje u odnosu na centralne procesore.

Strategija se zasniva na paralelizaciji iterativne funkcije Pollard Rho algoritma koja služi za generisanje karakterističnih tačaka. Centralni procesor šalje grafičkom procesoru određen broj početnih tačaka, nakon čega svaka kreirana nit na grafičkom procesoru izvršava iterativnu funkciju dok ne generiše karakterističnu tačku. Kada se generiše određen broj karakterističnih tačaka izvršavanje na grafičkom procesoru se zaustavlja i tačke se šalju centralnom procesoru.

Nakon paralelizacije sprovedena je evaluacija performansi dobijenih implementacija, kao i diskutovanje uticaja različitih parametara na celokupne performanse programa. Merenje performansi algoritama je obavljeno na tri različite platforme sa savremenim višejezgarnim procesorima, kao i na tri nVidia grafička procesora i jednom integrisanom Intel grafičkom procesoru. Dobijeni rezultati su detaljno analizirani i diskutovani. Rezultati su uglavnom očekivani i prikazuju moguće iskorišćenje snage grafičkih procesora u kriptoanalitičkim algoritmima, kao i postignuto ubrzanje.

3. Sadržaj i rezultati

Rad je podeljen na 8 poglavlja. U prvom poglavlju, uvodu, data je motivacija za rad, prikaz glavnih ideja koje su korišćene u radu i kratak pregled rada po poglavljima.

U drugom poglavlju je dat pregled matematičkih konstrukata na kojima se zasniva kriptografija pomoću eliptičnih kriva uz objašnjenje osnovnih termina vezanih za eliptične krive, konačna polja, zakon grupe i diskretan logaritam.

Treće poglavlje detaljno predstavlja sekvencijalni i paralelni Pollard Rho algoritam. Data je i procena potencijalnog ubrzanja algoritma na multiprocesorskim sistemima. Takođe je objašnjena važna operacija sabiranja dve tačke na eliptičnim krivama i prilagođavanje ove operacije grafičkim procesorima.

U četvrtom poglavlju su predstavljene sve aritmetičke operacije u konačnim poljima koje su potrebne za implementaciju algoritma. Pored reprezentacije brojeva predstavljeni su algoritmi aritmetičkih operacija kao što su sabiranje, množenje, redukcija i inverzija. Svi algoritmi rade sa brojevima sa polinomijalnom osnovom u binarnim konačnim poljima.

U petom poglavlju je detaljno data struktura aplikacije i implementacija algoritma. Najpre je kratko opisana specifikacija OpenCL-a, nakon čega je predstavljena implementacija OpenCL „framework"-a sa osnovnim funkcijama za rad sa OpenCL-om. Potom su date korišćene strukture podataka i opisana struktura paralelne aplikacije. Na kraju je detaljno opisana implementacija OpenCL kernela, korišćeni tipovi podataka, implementacija aritmetičkih funkcija, implementacija sabiranja dve tačke i implementacija same iterativne funkcije algoritma.

Šesto poglavlje opisuje hardverske platforme korišćene za testiranje aplikacije, prikazuje podatke dobijene testiranjem i podrobno analizira rezultate. Detaljno su predstavljene arhitekture korišćenih grafičkih procesora i ukratko navedene specifikacije centralnih procesora. Rezultati testiranja su prikazani kroz više grafika i tabela. Svi rezultati pažljivo analizirani i diskutovani. Prvo su navedeni rezultati testiranja na centralnim procesorima, a nakon toga su dati rezultati za svaki grafički procesor posebno za različite ulazne parametre i test slučajeve. Kao zaključak šestog poglavlja dat je presek postignutih rezultata na svim uređajima i međusobno poređenje najboljih rezultata. Pokazano je da su paralelizacijom postignuta značajna ubrzanja.

U sedmom poglavlju je dat zaključak rada i naznačeni su mogući pravci daljeg istraživanja.

Osmo poglavlje sadrži spisak korišćene literature.

4. Zaključak i predlog

Prema mišljenju članova Komisije predloženi master rad sadrži sledeće značajne doprinose:

1. Preciznu eksplikaciju problema izračunavanja diskretnog logaritma na eliptičnim krivima i algoritma za njegovo rešavanje
2. Određivanje strategije paralelizacije i paralelna implementacija Pollard Rho algortima,
3. Izbor i konfiguracija platformi za evaluaciju
4. Opsežna uporedna evaluacija sekvencijalnog i paralelnog algoritma na više platformi i pažljiva analiza i diskusija rezultata.

Na osnovu izloženog, Komisija predlaže Komisiji za studije II stepena Elektrotehničkog fakulteta u Beogradu da rad Dušana Kostića pod naslovom „Primena Pollard Rho algoritma pomoću OpenCL tehnologije na grafičkim procesorima" prihvati kao master rad i odobri usmenu odbranu.

U Beogradu, 16.3.2015.

Članovi Komisije

dr Milo Tomašević, vanredni profesor

dr Boško Nikolić, vanredni profesor