Катедри за рачунарство и информатику
Предмет: Сагласност за одбрану мастер рада.-

Одлуком Катедре и ННВ од 20.09.2013. именовани смо у комисију за одбрану мастер рада под насловом "Реализација алгоритма AES на платформи nVidia CUDA" кандидата **Милоша Ђурића,** студијски програм Информатика.

Кандидат је 14.9.2016. доставио текст свог рада. Тема рада је паралелна реализација шифровања алгоритмом AES (Advanced Encryption Standard) када се примењују начини шифровања ECB (Electronic Codebook), односно CBC (Cipher Block Chainig). Паралелизација је у случају режима ECB једноставна и ефикасна. Међутим, у случају режима CBC могућа је само паралелизација дешифровања, јер је поступак шифровања у том режиму инхерентно секвенцијалан. У случају шифровања у том режиму могућа је само паралелизација појединих корака у оквиру самог шифровања алгоритмом AES.

Рад се састоји од шест поглавља и закључка. У уводу је изложена историја настанка алгоритма AES. У другом поглављу је описан је стандардни алгоритма за шифровање AES. Начини рада са блоковским шифрама ECB и CBC изложени су у трећем поглављу. У четвртом поглављу изложен је преглед познатих имплементација алгоритма AES. У петом поглављу описује се о платформи nVidia CUDA. У шестом поглављу описана је програмска реализација паралелизованог шифровања, односно дешифровања у појединим режимима рада и приказани су добијени резултати. На крају се дају закључци и преглед могућих праваца даљег рада.

Мишљење.

Увидом у текст **Милоша Ђурића** " Реализација алгоритма AES на платформи nVidia CUDA" мишљења смо да приложени рад задовољава у потпуности захтеве који се постављају у изради мастер рада и предлажемо Катедри да одобри јавну одбрану рада.

У Београду, 21.9.2016.

Др Миодраг Живковић, ред. проф., ментор

Др Предраг Јаничић, ред. проф.

Др Саша Малков, ванр. проф.