Математички факултет
Универзитета у Београду

МОЛБА
ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да ми се одобри израда мастер рада под насловом:

Разбијање алгоритма DES грубом силом коришћењем акцелератора Maxeler

Значај теме и области:

DES (Data Encryption Standard) је један од шифарских система који је имао највише утицаја на развој модерне криптографије. Широко је коришћен поред осталог за невојну комуникацију владиних органа у САД, као и у комерцијалне сврхе. Замењен је новим стандардом AES, јер је због дужине кључа од свега 56 бита и због напретка технологије цена напада грубом силом (испробавање свих могућих кључева) постала мала. Прецизније, алгоритам DES се и даље користи, али у варијанти са удвострученим кључем.
Maxeler Technologies је једна од водећих компанија која пружа решења за програмирање на нивоу хардвера (FPGA). Такав начин програмирања омогућује паралелизацију, односно велико убрзавање израчунавања, уз битно смањен утрошак електричне енергије.

Специфични циљ рада:

Циљ рада је практична реализација напада са познатим паром (отворени текст, шифрат) на систем DES алгоритмом грубе силе, причему се sa паралелизацију користи персонални рачунар са картицом Maxeler, који постоји у Рачунарској лабораторији Математичког факултета. За развој програма треба користити окружење MaxIDE са преводиоцем MaxCompiler, који на основу кода написаног на високом језику генерише хардверску имплементацију.

Јован Радисављевић 1091/2014, Информатика
(име и презиме студ., бр. инд., ознака програма и модула)

Сагласан ментор др Миодраг Живковић

_____
(својеручни потпис студента)

_____
(својеручни потпис ментора)

_____
(датум подношења молбе)

Чланови комисије

1. др Предраг Јаничић, ред. проф.
2. др Саша Малков, ванр. проф.

Катедра за рачунарство и информатику је сагласна са предложеном темом.

_____
(*шеф катедре*)

_____
(*датум одобравања молбе*)