Катедри за рачунарство и информатику
Предмет: Извештај о прегледу мастер рада.-

Одлуком Катедре и ННВ од 22.06.2016. именовани смо у комисију за одбрану мастер рада под насловом "Разбијање алгоритма DES грубом силом коришћењем акцелератора Maxeler" кандидата **Јована Радосављевића,** студијски програм Информатика.

Кандидат је 20.9.2016. доставио текст свог рада. Тема рада је DES (Data Encryption Standard), један од шифарских система који је имао највише утицаја на развој модерне криптографије. Широко је коришћен за комуникацију владиних органа у САД и у комерцијалне сврхе. Због дужине кључа од свега 56 бита и због напретка технологије, цена напада грубом силом (одређивања кључа ако се знају шифрат и одговарајући отворени текст простим испробавањем свих могућих 2^{56} кључева) постала је релативно мала. Због тога се DES користи само у утрострученој варијанти са двоструким или троструким кључем. Поред тога, DES је званично замењен новим стандардом AES (Advanced Encryption Standard). Тема рада је паралелизација напада на DES применом Maxeler акцелератора.
Рад се састоји од пет поглавља и закључка. После увода, у поглављу 2 описује се алгоритам DES. У поглављу 3 приказана је укратко историја напада грубом силом на DES, као и алгоритам сусрет на пола пута који може да битно убрза напад на двоструки DES са два различита кључа. У поглављу 4 излажу се основни појмови о програмирању вођеном током података, затим о Maxeler акцелератору и развојном окружењу за рад са акцелератором. У поглављу 5 описана је програмска реализација напада на рачунару са Maxeler акцелератором. Акцелератор у сваком позиву испробава 2^{30} кључева. Добијена је процена да би на рачунару са Maxeler акцелератором комплетан поступак разбијања трајао око 23 дана. У време када је настао DES, процењивало се да би за напад који траје месец дана био потребан специјализовани рачунар, чија би цена била неколико десетина милиона долара. На крају се дају закључци и преглед могућих праваца даљег рада.

Мишљење.

Увидом у текст **Јована Радосављевића** "Разбијање алгоритма DES грубом силом коришћењем акцелератора Maxeler" 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, 25.9.2016.

Др Миодраг Живковић, ред. проф., ментор

Др Предраг Јаничић, ред. проф.

Др Саша Малков, ванр. проф.