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

Одлуком Катедре и ННВ од 30.05.2014. именовани смо у комисију за одбрану мастер рада под насловом "Анализа излазног низа генератора RC4" кандидата **Јоване Радуловић,** студијски програм Математика, модул Рачунарство и информатика.

Кандидат је 3.7.2015. доставила текст свог рада. Тема рада један од најпознатијих криптографских генератора псеудослучајног низа RC4. Уобичајено је да се RC4 користи у оквиру проточних шифри тако што се његов излазни низ сабира по модулу два, бит по бит, са поруком - отвореним текстом. Отпорност проточних шифри на криптоаналитичке нападе уопште (уобичајено је да се подразумева напад са познавањем пара отворени текст, одговарајући шифрат) повезана је квалитетом одговарајућег генератора псеудослучајног низа. Под квалитетом се подразумева отпорност пре свега на алгебарске нападе (решавање одговарајућег система нелинеарних Булових једначина) и статистичку анализу, која се своди на ефективно разликовање излазног низа генератора од низа независних случајних бита са равномерном расподелом вероватноће. Предмет рада је анализа излазбог низа генератора RC4 са статистичког аспекта.

Рад се састоји од пет поглавља и закључка. После увода и основних појмова о криптографији у другом поглављу, у трећем поглављу се описује генератор RC4. У четвртом поглављу се на основу књиге [1] приказују резултати теоријске анализе статистичких особина излазног низа. Типични резултати су приближне вредности појединих биномних вероватноћа у вези са генератором RC4. Пето поглавље описује програм и резултате статистичких тестова којима су проверена тврђења наведена у четвртом поглављу. Тестови са довољно великом величином узорка не одступају статистички значајно од тих процена. С друге стране, испоставља се да са величином узорка која прелази нпр. 10^7 низова добијених случајним независним кључевима, приближне вредности параметара постају систематски статистички различите од оних добијених симулацијом. На крају се дају закључци и преглед могућих праваца даљег рада.

Мишљење.
Увидом у текст **Јоване Радуловић** " Анализа излазног низа генератора RC4" 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, 7.7.2015.

Др Миодраг Живковић, ред. проф., ментор

Др Предраг Јаничић, ред. проф.

Др Младен Николић, доцент

Др Данко Јоцић, ред. проф.