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

Одлуком Катедре и ННВ од 28.11.2014. именовани смо у комисију за одбрану мастер рада под насловом "Корелациони напад на проточне шифре" кандидата **Душана Ристовског,** студијски програм Математика, модул Рачунарство.

Кандидат је 20.9.2017. доставио текст свог рада. Тема рада су проточне шифре - значајна класа алгоритама за шифровање заснованих на коришћењу генератора псеудослучајног низа (ГПСН), коначног аутомата чије је почетно стање одређено тајним кључем. Сваки бит шифрата добија се сабирањем по модулу два бита отвореног текста са одговарајућим битом низа кључа, излазом ГПСН. Уобичајено је да се овакви алгоритми разматрају са аспекта отпорности на напад са познатим отвореним текстом. Другим речима, анализира се да ли се на основу познавања дела излазног низа ГПСН може одредити његово почетно стање, односно кључ. Уобичајени елемент ГПСН су померачки регистри са линеарном повратном спрегом (ПРЛПС). На неке ГПСН чије компоненте су ПРЛПС могућ је *корелациони напад*, статистички напад кога карактерише независно одређивање почетног стања померачких регистара – компоненти ГПСН.

Рад се састоји од пет поглавља и закључка. После увода, у поглављу 2 наводе се неопходни појмови из криптографије, посебно о ПРЛПС. После тога следи опис структуре комбинационог и филтерског генератора, као класа ГПСН, и Гефеовог генератора. У поглављу 3 описује се корелациони напад. У поглављу 4 приказују се усавршене верзије корелационог напада, тзв. брзи корелациони напад. У поглављу 5 описује се програмска реализација корелационог напада и приказују се резултати напада на конкретне генераторе. На крају се дају закључци и преглед могућих праваца даљег рада.

Мишљење.
Увидом у текст **Душана Ристовског** "Корелациони напад на проточне шифре" 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, 21.9.2017.

Др Миодраг Живковић, ред. проф., ментор

Др Предраг Јаничић, ред. проф.

Др Младен Николић, доцент