Математички факултет
Универзитета у Београду

МОЛБА
ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да се одобри израда мастер рада под називом:

Корелациони напад на проточне шифре

чији су значај и специфични циљ следећи:

Проточне шифре су значајна класа алгоритама за шифровање који користе генератор псеудослучајног низа (ГПСН). Сваки бит шифрата добија се сабирањем по модулу два са одговарајућим битом низа кључа, излазом ГПСН. Напад на овакве алгоритме је обично напад са познатим отвореним текстом, што значи да на основу познавања дела излазног низа ГПСН треба одредити његово почетно стање, односно кључ.

Уобичајени елемент ГПСН су линеарни померачки регистри. На неке ГПСН са линеарним померачким регистрима могућ је *корелациони напад*, статистички напад кога карактерише независно одређивање почетног стања померачких регистара – компоненти ГПСН.

У раду треба описати неколико карактеристичних конструкција ГПСН са линеарним померачким регистрима и корелационе нападе на такве ГПСН. Поред тога, треба програмски реализовати корелациони напад на изабрани ГПСН.

Литература:
A. Joux, Algorithmic Cryptanalysis, CRC Press, New York, 2009.

Душан Ристовски, 1154/2013, P
(*име и презиме студента, бр. индекса, модул*)

_____
(*својеручни потпис студента*)

31.10.2014.
(*датум подношења молбе*)

Сагласан ментор Миодраг Живковић

_____
(*својеручни потпис ментора*)

Чланови комисије
1. Предраг Јаничић
2. Младен Николић

Катедра за рачунарство и информатику даје сагласност предложеној теми

_____ _____

(*шеф катедре*) (*датум одобравања молбе*)