Математички факултет
Универзитета у Београду

МОЛБА
ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да ми се одобри израда мастер рада под насловом:

Напад на генераторе са неуниформним тактовањем

Значај теме и области:
Криптографски генератори псеудослучајног низа (ГПСН) су коначни аутомати, чије почетно стање је одређено тајним податком - кључем. Криптографски ГПСН се користе за шифровање тако што се чланови његовог излазног низа (обично бинарне цифре) сабирају по модулу два са одговарајућим битима поруке. Напад на криптографски ГПСН подразумева одређивање његовог почетног стања на основу неког дела излазног низа.
Често се као важна компонента криптографских генератора псеудослучајног низа (ГПСН) користе померачки регистри са линеарном повратном спрегом (ПРЛПС), јер њихов излазни низ има добре статистичке особине. Због алгебарске једноставности ПРЛПС
(његово почетно стање се на основу дела излазног низа одређује решавањем система линеарних једначина), често се излазни низ ПРЛПС трансформише "насумичним" (рецимо под контролом излазног низа другог ПРЛПС) избацивањем неких чланова, односно његовим *неуниформним тактовањем*.
Једноставан напад на најједноставнији ГПСН са неуниформним тактовањем описан је у раду [1]. Усавршени напад који користи концепте теорије графова за упрошћавање стабла претраге једноставног напада описан је у раду [2].
Специфични циљ рада:
Циљ рада је описати и реализовати алгоритме за одређивање почетног стања ГПСН описане у радовима [1,2].
Остале битне информације:
Литература:
[1] M. Živković, An Algorithm for the Initial State Reconstruction of the Clock-Controlled Shift Register, IEEE Transactions on Information Theory 37(5) (1991), 1488–1490
[2] P. Caballero-Gil, A. Fúster-Sabater, A simple attack on some clock-controlled generators. Computers & Mathematics with Applications, 58(1), (2009), 179–188

Јована Рибић, 1045/2020 МР Сагласан ментор Миодраг Живковић

(име и презиме студ., бр. инд., ознака програма и модула)

_____
(својеручни потпис студента)

_____
(датум подношења молбе)

_____
(својеручни потпис ментора)

Чланови комисије

1. др Саша Малков, ванр. проф.
2. др Стефан Мишковић, доцент

Катедра за рачунарство и информатику је сагласна са предложеном темом.

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