Математички факултет
Универзитета у Београду

**МОЛБА**
**ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА**

Молим да ми се одобри израда мастер рада под насловом:

„Корелационо имуне Булове функције“

**Значај теме и области:**
Проточне шифре као основну компоненту имају генератор псеудослучајног низа (ГПСН) кључа; шифровање се врши сабирањем знака отвореног текста са наредним елементом низа кључа. Један од познатих типова ГПСН (тзв. Комбинациони генератор) користи Булову функцију са $n$ улаза да би од $n$ улазних бинарних низова формирао излазни бинарни низ. Ако се улазни бити сматрају случајним и независним, са једнаком вероватноћом нуле и јединице, онда је излазни бит случајна променљива. У неким случајевима могуће је одредити неки од улазних низова када се зна излазни низ ГПСН ако је вероватноћа једнакости излазног бита и тог улазног бита различита од ½. Булова функција је корелационо имуна реда $k$ ако је излазни бит некорелисан са било којом линеарном комбинацијом од највише $k$ улазних бита, Корелационо имуне функције су битне за широку класу криптографских система: одсутност корелационе иуности може учинити систем рањивим на тзв. корелациони напад са познатим отвореним текстом. Сем корелационе имуности за криптографске примене важне особине су поред осталог уравнотеженост (једнак број јединица и нула у табели), односно степен одговарајућег полинома по модулу два.

**Специфични циљ рада:**

Циљ рада је описати и реализовати алгоритме за добијање корелационо имуних, корелационо имуних и уравнотежених, односно Булових функција које су корелационо имуне и имају дрге пожељне особине, као што је нелинеарност (степен одговарајућег полинома).

**Литература**

[1] T. Cusick, P. Stanica, “Cryptographic Boolean Functions and Applications”, 2009, поглавље 4.

Зоран Глигорић, 1129/2015, Информатика
(име и презиме студ., бр. инд., ознака програма и модула)

Сагласан ментор Миодраг Живковић

(својеручни потпис студента)

(својеручни потпис ментора)

17.07.2017
(датум подношења молбе)

Чланови комисије

1. др Филип Марић, ванр. проф.
2. др Весна Маринковић, доцент

Катедра за рачунарство и информатику је сагласна са предложеном темом.

(*шеф катедре*)

(*датум одобравања молбе*)