Математички факултет
Универзитета у Београду

МОЛБА
ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да ми се одобри израда мастер рада под насловом:

Алгоритми засновани на рођенданском парадоксу и примене

Значај теме и области:

Познато је да ако се у соби налази више од 23 особе, онда је вероватноћа да неке две од њих имају рођендан истог дана већа од 1/2. То је такозвани рођендански парадокс. Уопште, ако се $\alpha\sqrt{n}$ елемената вади са враћањем из скупа величине n, онда је вероватноћа да нека два од њих буду иста приближно $1 - e^{-\alpha^2/2}$. Другим речима, у току случајног лутања по скупу од n елемената, после отприлике $1.2\sqrt{n}$ очекује се наилазак на већ раније прегледани елеменат. Посебно је интересантан случај када се ради над коначним низовима код којих сваки елемент низа зависи само од претходног, што је имитација случајног лутања. Ови низови су увек периодични. Постоје ефикасни алгоритми за одређивање периода таквих низова, што је тема овог рада заједно са конкретним применама.

Специфични циљ рада:

У раду треба изложити и реализовати алгоритме за одређивање периода низова (X_n), $n = 1,2, \ldots$ елемената из коначног скупа, таквих да је $X_{n+1} = F(X_n)$, $n \geq 1$ и варијанте тих алгоритама са конкретном применом на факторизацију, решавање проблема дискретног логаритма, проналажење колизија код криптографских хеш функција и слично.

Остале битне информације:

Литература: Antoine Joux, *Algorithmic Cryptanalysis*, Taylor & Francis Group, 2009

Мина Бадовинац, 1105/2016, 2МР
(име и презиме студ., бр. инд., ознака програма и модула)

(својеручни потпис студента)

(датум подношења молбе)

Сагласан ментор проф. др Миодраг Живковић

(својеручни потпис ментора)

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*)