Математички факултет
Универзитета у Београду

МОЛБА
ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да ми се одобри израда мастер рада под насловом:

„Алгоритми за генерисање минималних Булових функција"

Значај теме и области:
Минималне (енг. bent) Булове функције су оне Булове фукције од парног броја $2n$ променљивих које су на једнаком Хеминговом растојању $2^{n-1} - 2^{n/2-1}$ од свих афиних Булових функција. Број минималних Булових функција од две, четири, шест и осам променљивих је редом 8, 896, 5425430528 $\simeq 2^{32.3}$, и

$$2^9 \times 193887869660028067003488010240 \simeq 2^{106.29}.$$

Није познат број ових функција од 10 променљивих. Због отпорности на корелациони напад, односно линеарну криптоанализу, имају значајне примене у криптографији. О њима је објављено више радова. Детаљни преглед познатих тврђења о минималним Буловим функцијама може се наћи у књизи [1]. Познато је да је степен полинома који представља минималну Булову функцију од $2n$ променљивих највише n.

Специфични циљ рада:
Циљ рада је реализовати алгоритам за генерисање минималних Булових функција из тачке 5.2 дисертације [2]. Реализованим алгоритмом треба генерисати примере минималних Булових функција од $2n$ променљивих свих степенова од 2 до n, за вредности бар $n = 8, 10, 12, 14, 16$.

Остале битне информације:
Литература:
[1] N. Tokareva, Bent Functions: Results and Applications to Cryptography, Academic Press, 2015.
[2] J. E. Fuller, Analysis of Affine Equivalent Boolean Functions for Cryptography, PhD thesis, Queensland University of Technology, 2003.

Горана Вучић, 1095/2017, Информатика
(име и презиме студента, бр. индекса, модул)

Сагласан ментор **Миодраг Живковић**

(својеручни потпис студента)

(својеручни потпис ментора)

7. јун 2021. године
(датум подношења молбе)

Чланови комисије
1. др Нина Радојичић Матић, доцент
2. др Стефан Мишковић, доцент

Катедра **за рачунарство и информатику** је сагласна са предложеном темом.

(шеф катедре)

(датум одобравања молбе)