

Zagreb, 8. ožujka 2019.

DIPLOMSKI ZADATAK br. 2022

Pristupnik: **Kristijan Vulinović (0036483282)**
Studij: Računarstvo
Profil: Računarska znanost

Zadatak: **Pronalaženje Booleovih funkcija maksimalne nelinearnosti evolucijskim računanjem**

Opis zadatka:

Booleove funkcije sastavni su element kriptografskih algoritama. Kako bi se povećala otpornost na napade linearnom kriptanalizom, od posebnog je značaja svojstvo nelinearnosti Booleove funkcije. Booleove funkcije zadanog broja varijabli i maksimalne nelinearnosti nazivaju se Bent-funkcije, dok su sa stajališta primjene u kriptografskim algoritmima od posebnog interesa Booleove funkcije koje dodatno imaju i svojstvo balansiranosti.

U okviru ovog diplomskog rada potrebno je proučiti heurističke pristupe pronalaženja Booleovih funkcija maksimalne nelinearnosti te balansiranih Booleovih funkcija maksimalne nelinearnosti.


Potrebno je izraditi prototipne implementacije odabranih pristupa te prikazati i ocijeniti dobivene rezultate.

Radu priložiti izvorni kod razvijenih postupaka uz potrebna objašnjenja i dokumentaciju. Predložiti pravce budućeg razvoja. Citirati korištenu literaturu i navesti dobivenu pomoć.

Zadatak uručen pristupniku: 15. ožujka 2019.

Rok za predaju rada: 28. lipnja 2019.

Mentor:



Doc. dr. sc. Marko Čupić

Djelovođa:



Izv. prof. dr. sc. Tomislav Hrkać

Predsjednik odbora za
diplomski rad profila:



Doc. dr. sc. Marko Čupić