Математички факултет
Универзитета у Београду

МОЛБА
ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да ми се одобри израда мастер рада под насловом:

Криптоанализа шифре E_0

Значај теме и области:

Блутут (Bluetooth) је стандард за бежичну комуникацију уређаја као што су мобилни телефони, бежичне слушалице и штампачи. За шифровање података који се преносе применом овог стандарда користи се проточна шифра (stream cipher) E_0. Генератор псеудослучајног низа алгоритма E_0 састоји се од четири померачка регистра са линеарном повратном спрегом и коначног аутомата са четворобитним стањем. Ускоро по објављивању шифре E_0 појавили су се радови који описују поступке разбијања ове шифре.

Специфични циљ рада:

Циљ рада је описати безбедносну архитектуру стандарда блутут и алгоритам E_0 на основу књиге [2]. Алгоритам и напад на овај алгоритам описан у раду [1] потребно програмски реализовати и тестирати на верзији алгоритма E_0 у којој су поомерачки регистри замењени краћим.

Литература:

[1] C. De Canniere, T. Johanson, B. Preneel, Cryptanalysis of the Bluetooth Stream Cipher, COSIC internal report, 2001.
http://www.cosic.esat.kuleuven.be/publications/article-22.pdf
[2] C. Gehrman, J. Persson, B. Smeets, Bluetooth Security, Artech House, Boston, 2004.

Милош Мартиновић, 1120/2017 МР
(име и презиме студ., бр. инд., ознака програма и модула)

Сагласан ментор др Предраг Јаничић

_____
(својеручни потпис студента)

_____
(својеручни потпис ментора)

_____
(датум подношења молбе)

Чланови комисије

1. др Саша Малков
2. др Миодраг Живковић

Катедра за рачунарство и информатику је сагласна са предложеном темом.

_____
(*шеф катедре*)

_____
(*датум одобравања молбе*)