9/3

Математички факултет
Универзитета у Београду

УНИВЕРЗИТЕТ У БЕОГРАДУ
МАТЕМАТИЧКИ ФАКУЛТЕТ
Бр. 6/26
26 03 2014
Београд, Студентски трг 16
ТЕЛ. 20 27 801, ФАКС: 26 30 151

МОЛБА
ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да се одобри израда мастер рада под називом:

Криптоанализа шифре E_0

чији су значај и специфични циљ следећи:

Алгоритам за шифровање E_0, који се користи за блутут, треба програмски реализовати према спецификацији у раду [1], односно књизи [2]. Поред тога у мастер раду треба реализовати елементе напада на E_0 описаног у истом раду; не очекује се ефективна реализација комплетног напада, због његове сложености као целине (око 2^{76} корака). У посебном поглављу на основу књиге [2] треба изложити безбедносну архитектуру система блутут.

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

Милош Мартиновић,
1040/2013,Рачунарство и информатика (2мр сс)

Milos Martinovic
(*својеручни потпис студента*)

19.03.2014.
(*датум подношења молбе*)

Ментор МЖивковић
Миодраг Живковић

Чланови комисије

1. Предраг Јаничић
2. Саша Малков

Катедра за рачунарство и информатику даје подршку предложеној теми

(*шеф катедре*)

(*датум одобравања молбе*)