Математички факултет
Универзитета у Београду

МОЛБА
ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да ми се одобри израда мастер рада под насловом:

„Ротациони напад на шифре ARX"

Значај теме и области:
Шифре ARX карактеристичне су по томе што користе операције сабирања, ротације и екслузивне дисјункције (XOR) примењене на рачунарске речи. Ротациона криптоанализа је пробаблилистички криптоаналитички напад који се може применити на блоковске шифре оријентисане на рад са рачунарским речима, при чему се између осталог користе ротације за фиксиране бројеве битова. У раду [1] прецизирана је анализа ефикасности овог напада и приказани су резултати напада на две ARX шифре, BLAKE2 и SKEIN.

Специфични циљ рада:
Циљ рада је програмска реализација ротационог напада на једну од шифри BLAKE2 или SKEIN — комплетну или са смањеним бројем рунди.

Остале битне информације:
Литература:
[1] Khovratovich D., Nikolić I., Pieprzyk J., Sokołowski P., Steinfeld R. (2015) Rotational Cryptanalysis of ARX Revisited. In: Leander G. (eds) Fast Software Encryption. FSE 2015. Lecture Notes in Computer Science, vol 9054. Springer, Berlin, Heidelberg

Теодора Мацановић, 1085/2020, МР Сагласан ментор **Миодраг Живковић**
(име и презиме студента, бр. индекса, модул)

(својеручни потпис студента) *(својеручни потпис ментора)*

7. јун 2021. године
(датум подношења молбе)

Чланови комисије
1. др Филип Марић, ванр. проф.
2. др Саша Малков, ванр. проф.

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

(шеф катедре) *(датум одобравања молбе)*