

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 29.08.2023. године именovalo нас је у Комисију за преглед и оцену мастер рада дипл. инж. Николије Радојичић под насловом „Поређење класичних и постквантних алгоритама за дигитални потпис”. Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Николија Радојичић је рођена 19.12.1994. године у Ужицу. Завршила је основну школу „Милинко Кушић” у Ивањици као ђак генерације. Уписала је Гимназију у Ивањици коју је завршила као носилац Вукове дипломе. Електротехнички факултет уписала је 2013. године. Дипломирала је на модулу за Рачунарску технику и информатику 2017. године са просечном оценом 8,91. Дипломски рад на тему „Визуелизација начина рада CAST-128 алгоритама” одбранила је у септембру 2017. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на модулу за Рачунарску технику и информатику, уписала је у октобру 2020. године. Положила је све испите са просечном оценом 8,40.

2. Извештај о студијском истраживачком раду

Кандидаткиња Николија Радојичић је као припрему за израду мастер рада урадила истраживање релевантне литературе која се односи на област којој припада тема мастер рада. За три традиционална и три постквантна алгоритама за дигитални потпис, најпре је проучила начин рада сваког алгоритама понаособ, њихове математичке основе, тежине проблема на којима се заснива њихова сигурност, као и специфичне скупове параметара које користе. Потом се бавила истраживањем доступности библиотека и изворног кода који омогућавају употребу алгоритама у различитим програмским језицима и поређењем једноставности коришћења доступних решења. Утврђено је да за постквантне алгоритме као релативно нову област, још увек не постоји довољан број библиотека које се могу користити, а чак и постојеће су још увек у експерименталној фази. Са друге стране, за класичне алгоритме пронађено је мноштво опција и може се направити избор према жељеном програмском језику и перформансама које имплементације нуде.

3. Опис мастер рада

Мастер рад обухвата 54 стране, са укупно 13 слика, 10 табела и 28 референци. Рад садржи увод, 3 поглавља и закључак (укупно 5 поглавља), списак коришћене литературе, списак скраћеница, списак слика и списак табела.

Прво поглавље представља увод у коме је дат увид у проблематику области рада, као и мотивација за израду рада. Направљен је и кратак преглед осталих поглавља.

У другом поглављу најпре су уопштено описани алгоритми за дигитални потпис, са освртом на сигурност алгоритама и класификацију по овом критеријуму, а потом је дат нешто детаљнији опис сваког појединачног алгоритама.

У трећем поглављу су анализиране доступне библиотеке и изворни код који омогућавају коришћење алгоритама. Као илустрација коришћења алгоритама приказана је имплементација програма који омогућава дигитално потписивање, као и упутство за коришћење овог програма. Поред своје основне намене, програм омогућава и мерење перформанси алгоритама.

Резултати мерења брзине основних операција алгоритама, заузећа оперативне меморије, дужине кључева и потписа представљени су у четвртом поглављу. На основу ових резултата и теоријског нивоа сигурности дата је упоредна анализа алгоритама.

Пето поглавље представља закључак у коме су сумирани резултати рада и дате смернице за одабир и коришћење одређеног алгорита у зависности од конкретних потреба.

4. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Николије Радојичић се бави анализом и поређењем класичних и недавно стандардизованих постквантних алгоритама за дигитални потпис. Од класичних алгоритама су разматрани DSA, RSA, и ECDSA, а од постквантних CRYSTALS-Dilithium, FALCON и SPHINCS+. За потребе поређења коришћен је јавно доступни изворни код анализираних алгоритама, као и код OpenSSL библиотеке са имплементацијом алгоритама.

Основни доприноси рада су: 1) анализа сложених математичких модела постквантних криптографских алгоритама и поређење са класичним алгоритмима; 2) преглед постојећих библиотека и јавно доступних имплементација анализираних алгоритама, који омогућавају њихову употребу; 3) имплементација сопственог програма за демонстрацију дигиталног потписивања уз помоћ свих анализираних алгоритама; 4) упоредна анализа алгоритама и препоруке за одабир алгорита за коришћење.

5. Закључак и предлог

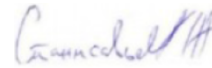
Кандидаткиња Николија Радојичић је у свом мастер раду успешно спровела анализу класичних и постквантних алгоритама за дигитални потпис. За одабране алгоритме разматрани су: њихова сигурност, временске и меморијске перформансе и могући начини имплементације. На основу ових критеријума кандидаткиња је успешно упоредила одабране алгоритме, систематично изложила њихове предности и недостатке и дала корисне смернице за коришћење алгоритама, као и за смер наставка истраживања.

Кандидаткиња је исказала самосталност и систематичност у своме раду.

На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Николије Радојичић под насловом „Поређење класичних и постквантних алгоритама за дигитални потпис” прихвати као мастер рад и кандидаткињи одобри јавну усмену одбрану.

Београд, 01.09.2023. године

Чланови комисије:



др Жарко Станисављевић,
ванредни професор



др Павле Вулећић,
ванредни професор