УНИВЕРЗИТЕТ У БЕОГРАДУ - ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ
Булевар краља Александра 73, 11000 Београд, Србија
Тел. 011/324-8464, Факс: 011/324-8681

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 01.06.2021. године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Зорана Милићевића под насловом „Апликација за обраду финансијских података коришћењем хомоморфне енкрипције“. Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Зоран Милићевић је рођен 08.01.1996. године у Крушевцу. Завршио је основну школу "Аца Алексић" у Александровцу као носилац дипломе „Вук Караџић“. Средњу школу „Свети Трифун са домом ученика“ (гимназија, општи смер) завршио је као ђак генерације и носилац дипломе „Вук Караџић“. Током школовања учествовао је на државним такмичењима из математике и физике. Електротехнички факултет у Београду уписао је 2015. године. Дипломирао је на одсеку за Рачунарску технику и информатику 2019. године са просечном оценом 8,73. Дипломски рад одбранио је у септембру 2019. године са оценом 10. Мастер академске студије на Електротехничком факултету у Београду уписао је у октобру 2019. године, на Модулу за софтверско инжињерство. Положио је све испите са просечном оценом 9,40.

2. Опис мастер рада

Мастер рад обухвата 62 стране, са укупно 21 сликом, 4 табеле и 25 референци. Рад садржи резиме, 7 поглавља и закључак (укупно 9 поглавља), списак коришћене литературе и додатак.

Прво поглавље представља увод у коме су описани предмет, мотивација и циљ рада. Објашњен је проблем сигурности обраде корисничких података који постоји код коришћења услуга рачунарства у облаку. У другом поглављу приказана је историја развоја хомоморфне енкрипције, која је једна од технологија којима може да се реши овај проблем. У трећем и четвртом поглављу описане су математичке решетке, као и алгоритми и проблеми у математичким решеткама који могу да се примене у криптографији. У петом поглављу уведене су дефиниције потпуно и парцијално хомоморфне енкрипције. Дефинисане су методе бутстраповања (енг. *bootstraping*) и промене модула (енг. *modulus switching*) које шеме потпуно хомоморфне енкрпције користе за редуковање нивоа шума.

У шестом поглављу детаљно су анализиране три тренутно најпопуларније шеме хомоморфне енкрипције: BGV, BFV, CKKS. Објашњена је математичка основа ових шема, и приказано како свака врши генерисање јавног и приватног кључа, енкрипцију и декрипцију података, као и како свака од поменутих шема спроводи израчунавања над хомоморфно енкриптованим подацима. У седмом поглављу су изнете основне информације о IBM-овој библиотеци отвореног кода за хомоморфну енкрипцију HElib која је коришћена у овом раду. Наведено је које су шеме хомоморфне енкрипције и оптимизације шема имплементиране у библиотеци и укратко је објашњена архитектура библиотеке.

У осмом поглављу детаљно је објашњена архитектура, начин рада и коришћења клијент-сервер апликације за обраду финансијских података коришћењем хомоморфне енкрипције – Secure Wallet. Дискутовани су недостаци апликације као и могући начини да се ти недостаци отклоне. Такође, извршена је и анализа временских и меморијских перформанси Secure Wallet апликације, анализа утицаја нивоа сигурности на перформансе, као и дата оквирна процена колико су операције над хомоморфно енкриптованим подацима спорије од операција над неенкриптованим подацима.

3. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Зорана Милићевића се бави анализом неких од постојећих шема потпуно хомоморфне енкрипције. Извршена је детаљна анализа теоријских основа потпуно хомоморфне енкрипције и шема потпуно хомоморфне енкрипције. Продискутоване су мане и ограничења анализираних шема потпуно хомоморфне енкрипције. Анализирано је како мане и ограничења шема потпуно хомоморфне енкрипције утичу на могућности њиховог коришћења у развоју тржишног софтвера на примеру клијент-сервер апликације за обраду финансијских података, развијене у склопу мастер рада, која користи Helib имплементацију BGV шеме хомоморфне енкрипције да енкриптује податке.

Основни доприноси рада су: 1.) имплементација апликације за обраду финансијских података која користи хомоморфну енкрипцију 2.) анализа и приказ тренутног статуса имплементација хомоморфне енкрипције за реализацију практичних пројеката из перспективе функционалности (рад са целим и реалним бројевима) и перформанси система.

4. Закључак и предлог

Кандидат Зоран Милићевић је у свом мастер раду извршио анализу најчешће коришћених актуелних шема потпуно хомоморфне енкрипције. Анализу је поткрепио имплементацијом, резултатима рада клијент-сервер апликације за обраду финансијских података, која користи BGV шему хомоморфне енкрипције и анализом перформанси система.

Кандидат је исказао самосталност и систематичност у свом поступку.

На основу горе наведеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Зорана Милићевића под насловом „Апликација за обраду финансијских података коришћењем хомоморфне енкрипције“ прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 30.8.2021. године

Чланови комисије:

Др Павле Вулетић, ванр. професор

_____

Др Жарко Станисављевић, ванр. професор