

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 17.12.2024 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Алекса Вујнић под насловом „Визуелна репрезентација постквантног криптографског алгорита Kyber“. Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Алекса Вујнић је рођен 23.08.2000. године у Новом Саду. Завршио је основну школу „Светозар Марковић Тоза“ у Новом Саду као вуковац. Уписао је гимназију „Јован Јовановић Змај“ у Новом Саду коју је завршио са одличним успехом. Електротехнички факултет уписао је 2019. године. Дипломирао је на одсеку за Софтверско инжењерство 2023. године са просечном оценом 9,78. Дипломски рад одбранио је у септембру 2023. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду уписао је у октобру 2023. године, на модулу Софтверско инжењерство. Положио је све испите са просечном оценом 10. Запослен је у компанији Cisco као инжењер софтвера.

2. Извештај о студијском истраживачком раду

Кандидат Алекса Вујнић је као припрему за израду мастер рада урадио истраживање релевантне литературе која се односи на област којој припада тема мастер рада. Конкретно, анализирани су стандардизовани криптографски алгоритми који су дизајнирани да буду отпорни на нападе квантним рачунарима и на основу анализе одабран је један алгоритам за који је пожељно да постоји апликација за визуелну репрезентацију. Затим су анализирана постојећа решења у области алата за визуелизацију криптографских алгоритама. Истраживањем области утврђено је да не постоје решења која би била адекватна за визуелизацију одабраног постквантног криптографског алгорита. Резултати анализе искоришћени су и приликом дизајна апликације за визуелну репрезентацију, као и за одабир технологија за имплементацију.

3. Опис мастер рада

Мастер рад обухвата 44 стране, са укупно 22 слике, 4 табеле, 5 исечака из изворног кода и 25 референци. Рад садржи увод, 4 поглавља и закључак (укупно 6 поглавља), спискове коришћене литературе, скраћеница, слика, табела и исечака из изворног кода.

Прво поглавље представља увод у коме су описани предмет и циљ рада. Описан је концепт асиметричне криптографије и ризика који постоје у вези са нападима квантних рачунара на такве алгоритме.

У другом поглављу је дат кратак преглед стандардизованих постквантних криптографских алгоритама. Описан је начин рада, намена и теоријско утемељење сваког од три анализирана алгорита из ове групе. Направљен је упоредни преглед анализираних алгоритама, као и образложење за одабир алгорита за визуелизацију. На крају је детаљно објашњен алгоритам који је одабран за визуелизацију (Kyber).

У трећем поглављу су описани одабрани постојећи алати за визуелизацију криптографских алгоритама. Један од ових алата је генеричког типа, док су два алата специфична и омогућавају визуелизацију конкретних алгоритама. Дат је детаљан опис подржаних функционалности алата, као и њихов упоредни преглед, истичући њихове предности и ограничења.

Четврто поглавље описује дизајн и имплементацију софтверског решења у оквиру овог рада. Дат је преглед коришћених технологија, начина организације имплементираних решења, као и кључних имплементационих одлука у развоју апликације за визуелну репрезентацију криптографског алгорита Kyber.

У оквиру петог поглавља је дат детаљан опис начина рада имплементираних апликација.

Дато је упутство за покретање апликације у режиму за развој и главне функционалности апликације. Описано је како корисник интерагује са интерфејсом реализоване апликације и које кључне информације добија из алата.

Шесто поглавље је закључак у оквиру кога је описан значај реализованог решења и могућа даља унапређења. Резимирани су резултати рада, изазови приликом развоја и могућности употребе имплементираног решења.

4. Анализа са кључним резултатима

Мастер рад дипл. инж. Алексе Вујнића се бави проблематиком визуелизације комплексних постквантних криптографских алгоритама. Оваква софтверска решења, а самим тим и алат развијен у оквиру овог рада, налазе примену у образовању, науци и индустрији као алати за ефикасније усвајање знања и вршење истраживања у области криптографије. Софтверско решење је развијено као веб апликација у радном оквиру Angular, што омогућава да апликација буде доступна за коришћење на скоро свим уређајима са приступом интернету. Основни доприноси рада су: 1) упоредна анализа одабраних стандардизованих постквантних криптографских алгоритама; 2) детаљан опис постквантног криптографског алгоритама Kyber; 3) упоредна анализа одабраних постојећих решења за визуелизацију криптографских алгоритама; 4) имплементација апликације за визуелизацију постквантног криптографског алгоритама Kyber.

5. Закључак и предлог

Кандидат Алекса Вујнић је у свом мастер раду успешно решио проблем имплементације софтверског решења за визуелну репрезентацију постквантног криптографског алгоритама Kyber, које даје детаљан увид у све аспекте рада овог алгорита кроз интуитиван кориснички интерфејс у два нивоа.

Кандидат је исказао самосталност и систематичност у своме поступку, као и иновативне елементе у решавању проблематике овог рада.

На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Алексе Вујнића под насловом „Визуелна репрезентација постквантног криптографског алгоритама Kyber” прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 01.06.2025. године

Чланови комисије:

др Жарко Станисављевић Ванредни
професор
сагласан, 31.05.2025.

др Павле Вулетић Ванредни професор
сагласан, 31.05.2025.