КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА
ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 23.06.2026 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Марко Гавриловић под насловом „Криптографски акцелератор на FPGA платформи заснован на ECDH, SHA-3 и AES-GCM алгоритмима". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Марко Гавриловић је рођен 04.03.2001. године у Ужицу. Завршио је основну школу „Милинко Кушић" у Ивањици као вуковац и ђак генерације. Уписао је Гимназију у Ивањици коју је завршио са врло добрим успехом. Током школовања освојио је више награда на државним такмичењима из физике и математике. Електротехнички факултет уписао је 2020. године. Дипломирао је на одсеку за Електронику и дигиталне системе 2024. године са просечном оценом 8,78. Завршни рад одбранио је у септембру 2024. године са оценом 10. Мастер студије на Електротехничком факултету у Београду, на модулу Електроника и дигитални системи уписао је у октобру 2024. године. Положио је све испите са просечном оценом 10.

2. Извештај о студијском истраживачком раду

Кандидат Марко Гавриловић је као припрему за израду мастер рада урадио истраживање релевантне литературе која се односи на хардверско убрзање криптографских алгоритама и пројектовање хибридних криптосистема. Полазну тачку тог истраживања чинили су стандарди: FIPS 202 (SHA-3 фамилија), NIST SP 800-38D (GCM режим рада), SP 800-186, SP 800-56A (криптографија елиптичких кривих и размена кључа), SP 800-56C (извођење кључа, KMAC) и FIPS 186 (дигитални потписи, ECDSA). Анализиране су постојеће хардверске реализације Keccak пермутације, AES језгара и множача у пољима GF(2m), укључујући digit-serial архитектуре, Karatsuba множење и Itoh-Tsujii-ев поступак инверзије, као и начини повезивања оваквих језгара у целину са уједначеним интерфејсом. На основу тог истраживања одабрани су алгоритми и параметри који систему у целини дају сигурносни ниво од 256 битова, дефинисан је заједнички AXI4-Stream интерфејс за сва три језгра и постављена јединствена методологија мерења на циљној платформи Xilinx Kria KR260.

3. Опис мастер рада

Мастер рад обухвата 110 страна, од чега четири прилога заузимају 7 страна, са укупно 60 слика, 40 табела и 40 референци. Рад садржи увод, пет поглавља и закључак (укупно 7 поглавља), четири прилога, списак коришћене литературе, као и листе табела и слика.

Прво поглавље представља увод у коме су описани предмет и циљ рада: реализација криптографског акцелератора који на једној FPGA платформи обједињује размену кључа, извођење кључева и заштиту саобраћаја.
У другом поглављу су објашњене криптографске основе. У њих спадају сигурносни захтеви, симетрична и асиметрична криптографија, хибридни ток од успостављања заједничке тајне до заштићеног пакета, класе алгоритама и усклађен избор параметара.

Треће поглавље покрива теоријски аспект сва три имплементирана алгоритма, од аритметике у пољу GF(2m) и ECDH размене кључа Монтгомеријевим мердевинама над кривом B-571, преко SHA-3 фамилије са сунђер конструкцијом и KMAC (cSHAKE) оквиром за извођење кључева, па све до AES-GCM са бројачким режимом рада и GHASH аутентификацијом, уз разрађене нумеричке примере и нагласке битне за хардверску реализацију.

У четвртом поглављу описана је хардверска реализација три акцелераторска IP језгра са заједничким AXI4-Stream интерфејсом. Чине их ECDH језгро, SHA-3 језгро и AES-GCM акцелератор са проточном и вишејезгарном архитектуром. Описано је и повезивање језгара у ланац хибридног криптосистема.

У петом поглављу приказани су резултати. Исправност је проверена према независним референтним моделима и тест векторима из стандарда. Мерења заузећа ресурса, учестаности, протока и кашњења спроведена су јединственом методологијом, пост-имплементационо, над одабраним конфигурацијама сва три језгра. SHA-3 језгро је валидирано и на хардверској платформи.

Шесто поглавље излаже потенцијална унапређења за будући рад.

Седмо поглавље је закључак у коме су резимирани резултати и доприноси рада.

У прилозима се налазе математичке основе, AES табеле, параметри криве B-571 и Keccak константе.

4. Анализа са кључним резултатима

Мастер рад дипл. инж. Марка Гавриловића се бави пројектовањем и мерењем криптографског акцелератора који на FPGA платформи обједињује хибридни криптографски ток размене кључа, извођења кључева и заштите саобраћаја. Сва три језгра написана су у VHDL-у и параметризована генерицима. Основни доприноси рада су:

1. Реализована су три параметризована акцелераторска IP језгра са заједничким AXI4-Stream интерфејсом: ECDH над кривом B-571, SHA-3 са cSHAKE/KMAC подршком и AES-GCM.

2. Цео ланац хибридног криптосистема, од размене кључа преко KMAC извођења до заштићеног пакета, проверен је симулацијом између две стране, над запакованим језгрима.

3. Спроведена су мерења перформанси свих конфигурација. Најбржа ECDH конфигурација опслужи око 3875 размена кључа у секунди, SHA-3 језгро достиже проток од 18,49 Gb/s, а AES-GCM акцелератор постиже око 51 Gb/s на нивоу AES језгра односно око 30 Gb/s када је језгро интегрисано у целу путању података (енгл. datapath).

4. Исправност је потврђена по нивоима према независним софтверским моделима и векторима из стандарда, а SHA-3 језгро и на хардверској платформи под PetaLinux системом, са убрзањем од 9,74 пута у односу на OpenSSL реализацију.

5. Показано је да сва три језгра заједно стају у око 84 процента циљног чипа уз сигурносни ниво од 256 битова, чиме је потврђена изводљивост целог система на једној наменској FPGA платформи.

5. Закључак и предлог

Кандидат Марко Гавриловић је у свом мастер раду „Криптографски акцелератор на FPGA платформи заснован на ECDH, SHA-3 и AES-GCM алгоритмима” успешно пројектовао, реализовао и измерио перформансе хардверског акцелератора хибридног криптографског система. У раду су усклађено одабрани алгоритми и параметри, реализована три параметризована IP језгра, спроведена верификација по нивоима и мерења перформанси на циљној платформи.
Марко Гавриловић је исказао самосталност и систематичност у своме поступку, као и иновативне елементе у обједињавању три криптографска алгоритма у јединствен систем на једној FPGA платформи.
На основу изложеног, Комисија за преглед и оцену мастер рада предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Марка Гавриловића прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 10.09.2026. године

Чланови комисије:

др Владимир Петровић Доцент
сагласан, 10.09.2026.

др Драгомир Ел Мезени Доцент
сагласан, 10.09.2026.