УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ ОРГАНИЗАЦИОНИХ НАУКА

Наставно-научном већу
Факултета организационих наука

Предмет: Реферат о урађеној докторској дисертацији кандидата Бориса Дамјановића

Одлуком Наставно-научног већа ФОН-а бр. 3/106-3 од 30.03.2016. именовани смо у Комисију за преглед, оцену и одбрану завршене докторске дисертације кандидата **Бориса Дамјановића**, под насловом **„Адаптибилна примена *AES* алгоритма код савремених оперативних система“** и на основу тога подносимо следећи

Р Е Ф Е Р А Т

1. УВОД

1.1. Хронологија одобравања и израде дисертације

Кандидат Борис (Стевана) Дамјановић, рођен 02.06.1965. године у Бања Луци, ЈМБГ 0206965160008, стално настањен у улици Жарка Згоњанина 44, Приједор, Република Српска/БиХ, поднео је дана 15.09.2010. године пријаву на Конкурс за упис докторских студија Факултета организационих наука Универзитета у Београду са потребним документима и доказом о уплати накнаде за упис. На ранг листи од 27.09.2010. године, кандидат је имао укупно 70.44 бода.

Кандидат Борис Дамјановић уписао је дана 05.10.2010. године докторске студије, изборно подручје Информациони системи, на Факултету организационих наука Универзитета у Београду. Кандидат Борис Дамјановић, индекс број 5005/2010, током докторских студија на Факултету организационих наука Универзитета у Београду положио је свих девет предмета са просечном оценом 10. Након што је остварио потребних 90 ЕСПБ бодова кандидат је дана 23.10.2013 године поднео Служби за последипломске студије Пријаву за израду приступног рада на докторским студијама са приложеном биографијом, образложењем теме приступног рада и листом радова. Кандидат је у Пријави навео предлог теме приступног рада и предложио ред. проф. др Дејан Симића за ментора који ће га водити током израде приступног рада и докторске дисертације.

На седници научно наставног већа Факултета организационих наука Универзитета у Београду од 13.11.2013. године именовани су чланови Комисије за преглед и одбрану приступног рада и оцену научне заснованости пријављене докторске дисертације кандидата на докторским студијама Бориса Дамјановића под насловом „АДАПТИБИЛНА ПРИМЈЕНА *AES* АЛГОРИТМА КОД САВРЕМЕНИХ ОПЕРАТИВНИХ СИСТЕМА“ у саставу:

1. др Дејан Симић, редовни професор Факултета организационих наука, Универзитета у Београду
2. др Душан Старчевић, редовни професор Факултета организационих наука, Универзитета у Београду
3. др Бошко Николић, ванредни професор Електротехничког факултета, Универзитета у Београду
На истој седници кандидату је одобрена израда приступног рада на докторским студијама, а за ментора је именован редовни професор др Дејан Симић.

Кандидат Борис Дамјановић је бранио Приступни рад под називом „АДАПТИБИЛНА ПРИМЈЕНА *AES* АЛГОРИТМА КОД САВРЕМЕНИХ ОПЕРАТИВНИХ СИСТЕМА“ дана 25.11.2013. године. На седници научно наставног већа Факултета организационих наука Универзитета у Београду од 03.12.2013. године усвојен је Извештај Комисије за оцену научне заснованости пријављене докторске дисертације кандидата на докторским студијама Бориса Дамјановића под насловом »АДАПТИБИЛНА ПРИМЕНА *AES* АЛГОРИТМА КОД САВРЕМЕНИХ ОПЕРАТИВНИХ СИСТЕМА«. За ментора је предложен др Дејан Симић, ред. проф. ФОН-а. Извештај је достављен Већу научних области техничких наука Универзитета у Београду.

Дана 09.02.2016. године ментор др Дејан Симић, ред. проф. ФОН-а предао је Извештај ментора о завршетку рада кандидата на изради докторске дисертације, којом је известио Наставно-научно Веће Факултета организационих наука да је кандидат Дамјановић (Стевана) Борис завршио са израдом докторске дисертације под насловом „Адаптибилна примјена *AES* алгоритма код савремених оперативних система“.

1.2. Научна област дисертације

Докторска дисертација под називом „АДАПТИБИЛНА ПРИМЕНА *AES* АЛГОРИТМА КОД САВРЕМЕНИХ ОПЕРАТИВНИХ СИСТЕМА“ припада области техничких наука. Изборно подручје дисертације су информациони системи. Ужа научна област којом се бави дисертација су информационе технологије.

Ментор, др Дејан Симић, објавио је више радова из наведених научних области у међународним часописима на СЦИ листи са импакт факторима. Одговарајући научни радови ментора су наведени приликом пријаве теме докторске дисертације кандидата.

1.3. Подаци о кандидату

Борис Дамјановић је рођен 02.06.1965. године у Бања Луци. Завршио је средњу Електро-техничку школу у Приједору 1983. godine. Високу школу за економију и информатику у Приједору завршава 2008. године са просечном оценом 9.61. Након тога уписује дипломске академске студије - Мастер на Факултету организационих наука у Београду, студијски програм Информациони системи и технологије, студијско подручје Информациони системи. Мастер рад под насловом „Имплементација и проширење *AES* алгоритма“ под менторством проф. др Симић Дејана одбранио је са оценом 10 и завршио студије са просечном оцјеном 10.00. Борис Дамјановић уписао је дана 05.10.2010. године докторске студије, изборно подручје Информациони системи, на Факултету организационих наука Универзитета у Београду. Дана 25.11.2013. године, Борис Дамјановић је на Факултету организационих наука Универзитета у Београду одбранио Приступни рад под називом „АДАПТИБИЛНА ПРИМЈЕНА *AES*

АЛГОРИТМА КОД САВРЕМЕНИХ ОПЕРАТИВНИХ СИСТЕМА“. Од тренутка уписа докторских студија у октобру 2010. године до момента писања извештаја (март, април 2016. године), Борис Дамјановић је задржао статус студента на Факултету организационих наука Универзитета у Београду.

Програмирањем и развојем информационих система се бави од 1988. године. Од 1991. запослен је у ИТЦ Козарски Вјесник - Радио Приједор, најпре као реализатор програма, а касније и као шеф технике. Од 1998. године ради у предузећу *Esprit Radio* у Приједору, најпре као шеф технике а затим као менаџер. Од 2008. године запослен је у предузећу *Commercial D.O.O.* као програмер и сувласник. Аутор је великог броја разнородних апликација и ЕРП решења (*Media Light, Media Pro, RadioAMP, Sinapsa, KFKK, FCMidi, FCMidiVP, FCMini, KasaPDV...*) и интернет презентација (*Geno Balkan, Esprit Radio, Arifagić Investment, AGK, ...*). Паралелно са радом у привреди, почевши од школске 2008/2009 године Борис Дамјановић је као сарадник у настави на Високој школи за економију и информатику Приједор учествовао у припреми, извођењу вежби и предавања, као и испита на предметима: Заштита рачунарских система и Архитектура и функција рачунара. Почевши од школске 2010/2011 године, кандидат је као предавач на Високој школи за економију и информатику учествовао у припреми, извођењу вежби, предавања, као и испита на предметима: Базе података 1, Базе података 2, Заштита рачунарских система и Архитектура и функција рачунара. Од школске 2014/2015 године Борис Дамјановић је као сарадник у настави Универзитета за пословни инжењеринг и менаџмент у Бања Луци учествовао у припреми, извођењу вежби и предавања, као и испита на предметима: Криптографија, Увод у *WWW*, Софтверски студио 2, Софтверски студио 3, Програмирање интернет апликација и Оперативни системи.

2. ОПИС ДИСЕРТАЦИЈЕ

2.1. Садржај дисертације

Докторска дисертација кандидата Дамјановић Бориса под насловом „АДАПТИБИЛНА ПРИМЈЕНА *AES* АЛГОРИТМА КОД САВРЕМЕНИХ ОПЕРАТИВНИХ СИСТЕМА“ писана је латиницом, фонт Ариал величине 12 тачака, формат странице А4. Докторска дисертација има укупно 209. страна текста, 84 слике, 25 табела, 56 листинга и 79 једначина. На крају дисертације дат је списак коришћене референтне литературе, који садржи 172 библиографске јединице. Докторска дисертације је структуирана у 13 поглавља:

1. Увод
   - 1.1 Структура рада
   - 1.2 Дефинисање проблема и предмета истраживања
   - 1.3 Циљеви истраживања
   - 1.4 Полазне хипотезе
   - 1.5 Методе истраживања
2. Алгоритам *AES*
   - 2.1 Спецификација и формална репрезентација
3. Начини енкрипције унутар оперативних система
   - 3.1 Начини енкрипције оријентисани ка медијуму за чување података (*storage encryption*)

3.2 Мрежно орјентисани начини енкрипције

3.3 Подршка криптографским акцелераторима у оквирима оперативних система

3.4 Студије адаптивности софтверских ресурса хардверским могућностима ради побољшања перформанси

3.5 Компаративна анализа криптографских решења у оквиру оперативних система

4. Методе и технологије примењене у развоју решења

4.1 Технологије за креирање криптографских модула

4.2 Виртуелни фајл систем *Apache Commons*

4.3 Рударење података и машинско учење

4.4 Систем за управљање базама података *Firebird*

4.5 *Java Database Connectivity (JDBC)*

4.6 Механизми интерпроцесне комуникације

4.7 Технологија сокета

4.8 Технологија именованих и неименованих цеви (*Named Pipes – Unnamed, Anonymous Pipes*)

4.9 *XML* стандард

4.10 Криптографски начини рада који су утицали на паралелизацију извршења

4.11 *XEX*, *XE* конструкције и *XTC-AES* начин рада

4.12 Тестне платформе

5. Модел и основне карактеристике адаптибилне примене *AES* алгоритма у савременим оперативним системима

5.1 Модел адаптибилног криптографског фајл система

5.2 Дефинисање ограничења и претпоставки истраживања

5.3 Криптографски модули

5.4 Концепт модула за координацију

5.5 Неке последице избора технологије и модела независних од платформе

6. Архитектура решења за адаптибилну примену *AES* алгоритма на нивоу оперативног система

6.1 Структура модула за координацију

6.2 Модели комуникације криптографских ресурса и адаптибилног криптографског фајл система

6.3 *Apache Commons VFS* као контејнер за адаптибилни виртуелни криптографски фајл систем

6.4 Криптографски модули коришћени као криптографски ресурси

6.5 Подсистем за одређивање прага искористивости у односу на дужине датотека

7. Једнонитни (*single-threaded*) модули

8. Паралелни *CUDA* модул за шифровање и дешифровање *AES* алгоритмом као криптографски ресурс оперативног система

9. Једнонитни (*single-threaded*) експерименти са могућим начинима модификације *AES* алгоритма

9.1 Стандардом дефинисани алгоритам и правила генерисања кључева

9.2 Модификација алгоритма испод границе од 128 бита

9.3 Модификација алгоритма изнад границе од 256 бита

9.4 Резултати мерења брзине извршења модификованих верзија алгоритма као тренинг подаци за креирање модела података

10. Разматрања могућности паралелизације криптографског алгоритма *AES*
11. Евалуација система и приказаних решења
    11.1 Провера хипотеза
12. Закључак
13. Референтна литература

2.2. Кратак приказ појединачних поглавља

Предмет истраживања докторске дисертације обухвата анализу искоришћености расположивих хардверских и софтверских криптографских ресурса од стране модерних оперативних система у имплементацији алгоритма *AES*. У уводном делу рада дата су разматрања везана за постојање зависности између алгоритма *AES* и хетерогених хардверских и софтверских ресурса који могу да се нађу у произвољном рачунарском систему. Централни проблем који се разматра у овом раду је могућност адаптибилне примене алгоритма *AES* у оквиру оперативног система у зависности од доступних ресурса. Примарни циљ овог истраживања је развој модела за адаптибилну примену алгоритма *AES* на нивоу оперативног система. Секундарни циљеви односе се на повећање квалитета заштите модификацијом алгоритма, као и на истраживање постојећих и нових решења за паралелизацију извршења алгоритма *AES* који су формално репрезентовани и имплементирани ради потврде концепта и на крају истраживање могућности за укључење посебних хардверских компонената (*CUDA GPU*) као криптографских ресурса оперативног система. У уводном делу су наведене и полазне хипотезе које су провераване у оквиру докторске дисертације.

У другом поглављу дата су уводна објашњења и теоретске претпоставке везане за формалну репрезентацију алгоритма *AES*. У овом поглављу се описују нотације и конвенције које су карактеристичне за *AES*, затим математичке претпоставке, трансформације овог алгоритма и основне идеје везане за оптимизацију његовог извршења.

Након тога, у трећем поглављу се представља истраживање коришћених начина енкрипције у оквиру оперативних система, где се приказују различите идеје, места и начини на које је она реализована у различитим оперативним системима. На основу истраживања које је представљено у делу овог поглавља настала је публикација у националном часопису у категорији М52. У наставку поглавља представљен је одређен број радова који је истраживао подршку криптографским акцелераторима у оперативним системима, као и адаптивност софтверских ресурса хардверским могућностима рачунара. На крају трећег поглавља дата је компаративна анализа криптографских решења у оперативним системима у којој је дат упоредни приказ дела решења која се данас користе у модерним оперативним системима.

У четвртом поглављу дат је преглед метода и технологија примењених у развоју решења. Од потребних технологија за развој најпре је приказана Јава са *JCA/JCE* скупом *API*-ја, а затим *Oracle/SUN JCE* и *Bouncy Castle* криптографске библиотеке. Након тога представљен је *Intel*-ов *Advanced Encryption Standard New Instructions* (*AES-NI*) скуп инструкција. Следећа технологија која је представљена у оквиру овога поглавља је *CUDA* архитектура и паралелно програмирање. Након тога је представљен

виртуелни фајл систем *Apache Commons* који је намењен да служи као контејнер за виртуелни криптографски фајл систем. У наставку је представљен концепт машинског учења са методама регресионе анализе, M5' и *Hill-climbing*. Након тога, представљени су механизми за интерпроцесну комуникацију, а на крају су представљени криптографски начини рада (*modes of operation*) који су утицали на решења приказана у раду.

У петом поглављу приказује се развој модела за адаптибилну примену *AES* алгоритма у савременим оперативним системима. Модел је позициониран унутар виртуелног фајл система унутар којег је смештен модул за координацију. У оквиру овог модула логички су смештени системи за тренинг, категоризацију и за селекцију најефикаснијег ресурса, везе са одабраним системом за управљање базама података, са улазно излазним подсистемом, конфигурација система и одређен број криптографских ресурса (модула) који су у стању да врше шифровање и дешифровање помоћу алгоритма *AES*. У наставку се врши позиционирање претходно наведених техника и технологија, које иако логички спадају у модул за машинско учење, физички могу и морају бити сасвим другачије реализовани. У овом поглављу се анализирају и заједничке карактеристике имплементираних криптографских модула и утврђују границе развоја система.

Шесто поглавље садржи опис архитектуре решења за адаптибилну примену *AES* алгоритма на нивоу оперативног система. У овом делу су логичке компоненте које су представљене у моделу сада приказане као засебни физички модули који не морају, а у случајевима криптографских модула и не би требало, да буду у саставу модула за координацију. Овде су представљени *Apache Commons VFS*, системи за тренинг и категоризацију, систем за селекцију најефикаснијег ресурса са подсистемима за класификацију и номинацију, везе са библиотеком програма за машинско учење, са одабраним системом за управљање базама података (СУБП), улазно-излазни модул, коришћени СУБП, модели комуникације, као и подсистем за одређивање прага искористивости.

У седмом поглављу анализирају се основне карактеристике имплементираних једнонитних криптографских модула. Најпре се разматрају оригиналне једнонитне имплементације у програмском језику Јава које се ослањају на идеје аутора алгоритма (*EAESG*). Након тога представљена је имплементација омотача око криптографске библиотеке *Oracle/SUN JCE*. Потом је представљено једнонитно решење имплементирано помоћу *MS Visual C++* компајлера. На крају представљања једнонитних модула је приказано решење које се ослања на *AES-NI* скуп инструкција. Део овог поглавља који истражује имплементацију омотача око *third party* библиотека довео је до резултата који су представљени у међународном часопису у категорији M21.

У поглављу 8 дат је опис криптографског модула који паралелизује извршење *AES* алгоритма уз помоћ *CUDA* архитектуре, комбинацијом *CUDA C* компајлера и *MS Visual C/C++* компајлера, где се *CUDA GPU* појављује као ресурс оперативног система. Међу приказаним модулима овај се, уз модул који се ослања на специјализовано хардверско *AES-NI* шифровање, издваја својим великим потенцијалом за брзу обраду података.

У поглављу 9, представљени су начини модификације алгоритма *AES* који су пронађени у доступној литератури, као и властите кандидатове модификације овог алгоритма. Део истраживања која су представљена у овом поглављу потекао је из

Мастер рада кандидата, а други делови истраживања су представљени у публикацијама у категорији М51 и М52.

У десетом поглављу су представљене идеје за паралелизацију извршења *AES* алгоритма коришћењем модификованог *OFB* начина рада. У овом поглављу су дати и резултати овога истраживања. Делови истраживања су објављени у публикацијама у категоријама М51, М52 и М23.

У једанаестом поглављу даје се евалуација приказаних решења, са компаративним приказом степена слагања креираних модела и података, са међусобним поређењем предиктивних модела појединих криптографских ресурса од стране виртуелног криптографског фајл система. На крају овог поглавља се даје провера хипотеза у циљу потврде сврхе истраживања, која се огледа у утицају који на перформансе има адаптација оперативних система расположивим хардверским и софтверским криптографским ресурсима.

У закључним разматрањима дати су најзначајнији доприноси дисертације, истакнут је значај истраживања проблема искоришћења расположивих криптографских ресурса и дате су смернице за даљи рад.

3. ОЦЕНА ДИСЕРТАЦИЈЕ

3.1. Савременост и оригиналност

Предмет дисертације припада актуелним областима истраживања информационих система и информационих технологија. Унапређење перформанси оперативних система у делу адаптибилне примене криптографских функција представља важну тему у научним и стручним радовима.

Кандидат је урадио систематизацију и детаљну анализу досадашњих приступа енкрипцији унутар оперативних система на основу доступне литературе. Након критичког осврта на постојећа решења кандидат је дао предлог модела и представио модуле адаптибилног оперативног система за коришћење криптографских функција. Поред тога, дат је опис израде свих предложених појединачних модула.

Формални опис модела и метода развоја система за динамички адаптибилну примену *AES* алгоритма, као и креирање модела комуникације оперативног система са окружењем представља зачајан и оригиналан научни допринос.

3.2. Осврт на референтну и коришћену литературу

Кандидат је у раду навео укупно 172 референце. Коришћена обимна литература обухвата период од 1967-2016. године. На основу увида у наведене библиографске референце може се закључити да је кандидат свеобухватно изабрао релевантну литературу узимајући у обзир водеће међународне часописе и значајне конференције за област истраживања. Обухваћене су најзначајније IEEE, ACM, IBM, Intel, NIST, MIT, Springer, Microsoft, Oracle и Linux референце релевантне за област истраживања. Листа референци садржи и 6 радова где је кандидат први аутор.

3.3. Опис и адекватност примењених научних метода

У изради докторске дисертације примењене су методе:

- прикупљања, сређивања и анализе постојећих научних резултата,
- моделовања,
- аналитичко-дедуктивна метода,
- метода компарације,
- методе регресионе и корелационе анализе,
- метода научне дескрипције и
- експериментална провера предложеног модела и модула адаптибилне примене *AES* алгоритма у савременим оперативним системима.

Методе прикупљања, сређивања и анализе постојећих научних резултата су коришћене у поглављима 2, 3, 4 и 8.

Метода моделовања је коришћена у поглављима 5 и 6. Метода моделовања је теоријско-емпиријска метода у чијој основи су методе типологизације, апстракције и конкретизације.Моделовање је у дисертацији представљено помоћу типологизације (као представљање типичног фајл система), затим помоћу апстракције различитих криптографских компонената и конкретизације алгоритма за одлучивање о избору најбоље компоненте.

Аналитичко-дедуктивна метода је коришћена у поглављу 11 у циљу провере хипотеза.

Метода компарације је коришћена такође у поглављу 11.

Методе регресионе и корелационе анализе су интензивно коришћене у поглављима 7, 8, 9, 10 и 11. Наведене методе су коришћене за израчунавање коефицијента корелације, средње апсолутне грешке, средње квадратне грешке, релативне апсолутне грешке и релативне квадратне грешке.

Метода научне дескрипције се интензивно користи у поглављима 2, 3, 8, 9 и 10.

Поред тога, у поглављима 7, 8, 9, 10 и 11 су коришћене методе машинског учења *M5 Prime*, *M5Rules*, *Multilayer perceptron* (врста неуронске мреже) и *LWL* (*locally weighted learning*, тј. локално пондерисано учење). Ове методе су представљене у потпоглављима:
4.3 Рударење података и машинско учење и
4.3.3 M5 и M5' методе.

Такође, у докторској дисертацији су коришћене и технике за математичку оптимизацију *Hill-climbing* и *Random restart Hill-climbing*. Ове технике су представљене и коришћене у потпоглављима:
4.3.4 Техника пењања (*Hill-climbing*) и
6.1.2.2 Подсистем за номинацију (модул номинатор).

На основу анализе докторске дисертације, може се закључити да примењене научне методе и технике у потпуности одговарају теми дисертације и спроведеном истраживању.

3.4. Применљивост остварених научних резултата

Резултати докторске дисертације могу имати ширу примену у софтверским системима којима су на располагању криптографске функције имплементиране помоћу различитих софтверских и хардверских криптографских ресурса. Главну примену резултати докторске дисертације могу наћи како у новим верзијама комерцијалних оперативних система, тако и у новим верзијама оперативних система отвореног кода у циљу унапређења перформанси у делу примене криптографских функција.

Паралелно *OFB* шифровање са одложеном синхронизацијом нити у коме се користе *XEX* и *XE* конструкције, као један од резултата истраживања, може се применити у сателитским комуникацијама.

3.5. Оцена достигнутих способности кандидата за самостални научни рад

Кандидат је на основу резултата истраживања у области докторске дисертације објавио више научних радова од којих су 2 рада објављена у међународним часописима са СЦИ листе са импакт факторима. На оба рада кандидат је први аутор.

На основу прегледане докторске дисертације, као и на основу објављених научних радова Комисија је оценила да је кандидат Борис Дамјановић достигао потребан ниво способности за самостални научни рад.

4. ОСТВАРЕНИ НАУЧНИ ДОПРИНОС

4.1. Приказ остварених научних доприноса

Остварени научни доприноси у оквиру докторске дисертације су:

1. Систематизација и детаљна анализа досадашњих приступа енкрипцији унутар оперативних система.
2. Анализа адаптибилности оперативних система за ефикасну употребу *AES* алгоритма.
3. Анализа могућности школских проширења *AES* алгоритма.
4. Предлог и представљање модела адаптибилног криптографског оперативног система.
5. Формални опис модела и метода развоја фајл система за динамички адаптибилну примену *AES* алгоритма.
6. Приказ методологије, припреме и извођења експеримената и приказа резултата експеримената.
7. Креирање модела комуникације оперативног система са окружењем.
8. Предлог новог криптографског начина рада под називом паралелно *OFB* шифровање са одложеном синхронизацијом нити у коме се користе *XEX* и *XE* конструкције.
9. Предлог увођења метода машинског учења (M5′ метода) у доношењу одлуке оперативног система о избору најефикаснијег ресурса (средства за извршавање алгоритма) система.
10. Анализа имплементације свих предложених појединачних модула (*AES NI, CUDA*, модула за машинско учење, модула омотача око *third party* библиотека).
11. Истраживање нових експерименталних идеја за паралелизацију *AES* алгоритма, извођење експеримената и приказ емпиријских резултата.

Стручни допринос истраживања се огледа у:

- имплементацији школских проширења *AES* алгоритма коришћењем различитих дужина кључа;
- имплементацији нових експерименталних идеја за паралелизацију *AES* алгоритма;
- имплементацији различитих модула који су у стању да користе бројне хардверске и софтверске криптографске ресурсе који стоје на располагању модерним оперативним системима.

Друштвени допринос истраживања се огледа у следећем:

- резултати истраживања ће помоћи при идентификацији ресурса који од стране оперативног система могу да буду искоришћени за убрзање шифровања и дешифровања помоћу *AES* алгоритма;
- резултати истраживања ће допринети при анализи и дескрипцији процеса имплементације криптографске адаптибилности оперативних система у делу примене *AES* алгоритма;
- резултати истраживања могу да буду искоришћени за даља унапређења *AES* алгоритма;
- резултати истраживања ће допринети при даљем развоју метода криптографске адаптибилности и ефикаснијем коришћењу криптографије у оквирима оперативних система.

4.2. Критичка анализа резултата истраживања

Кандидат је анализирао досадашње приступе енкрипцији и декрипцији унутар оперативних система. Савремени оперативни системи немају уграђену адаптибилност расположивим хардверским и софтверским ресурсима приликом извршавања криптографских функција. Кандидат је истражио начине помоћу којих извршавање *AES* алгоритма може да се прилагоди променљивим хардверским и софтверским криптографским могућностима на системском нивоу, тј. на нивоу оперативног система. За разлику од досадашњих публикованих анализа кандидат је најпре дао модел криптографски адаптибилног оперативног система, затим приказао детаљну архитектуру решења за адаптибилну примену *AES* алгоритма на нивоу оперативног система.

Кључни модули као што су модул за координацију, модул за тренинг и категоризацију, модул за селекцију, који садржи подсистем за класификацију и подсистем за номинацију су детаљно описани.

Верификација предложеног модела и модула криптографски адаптибилног оперативног система је потврђена имплементационом анализом и остварeним експерименталним резултатима.

4.3. Верификација научних доприноса

У области која је уско везана са темом докторске дисертације кандидат је објавио више радова од којих су издвојени следећи:

Категорија М21:

1. Damjanović B., Simić D. (2013), *Performance evaluation of AES algorithm under LINUX operating system, Proceedings of the Romanian Academy - series A: Mathematics, Physics, Technical Sciences, Information Science,* Volume 14, number 2/2013, pp.177-183, ИФ за 2014 годину: 1.658.

Категорија М23:

1. Damjanović, B., Simić, D. (2015), *Tweakable parallel OFB mode of operation with delayed thread synchronization, Wiley, Security and Communication Networks, Security Comm. Networks (2015), Published online in Wiley Online Library (wileyonlinelibrary.com).* ДОИ: 10.1002/sec.1404, ИФ за 2015 годину: 0.72.

Категорија М51:

1. Damjanović B., Simić D. (2011), *Comparative implementation analysis of AES algorithm, JITA, Banja Luka,* ИССН 2232-9625, pp.119-127.

Категорија М52:

1. Дамјановић Б., Симић Д. (2013), Преглед примјењених приступа за софтверску енкрипцију података у различитим оперативним системима, Инфо М, Београд , вол. 12, бр. 47, стр. 32-37.

2. Дамјановић Б., Симић Д. (2013), Експерименти са могућим модификацијама *AES* алгоритма, Инфо М, Београд, вол. 12, бр. 46, стр. 34-39.

Категорија М63:

1. Дамјановић Б., Старчевић Д. (2015), *Mean Shift* алгоритам за праћење објеката у *OpenCV* библиотеци, *InfoTech* 2015, Аранђеловац, ИСБН 978-86-82831-21-1.

2. Дамјановић Б., Симић Д. (2014), Моделирање перформанси различитих имплементација алгоритма *AES* помоћу M5’ методе, *InfoTech* 2014, Аранђеловац.

Такође, кандидат је објавио и следеће радове:

Категорија М53:

1. Микић Ђ., Микић Н., Дамјановић Б. (2012), Оцјењивање релевантности критерија управљачког протокола на бази приоритета и матричне анализе, Транзиција, Вол.14, Но. 30, Тузла

Категорија М63:

1. Damjanović B., Banjac O., Tejić B., Kos A. (2014), *The Theoretical Framework for Face Detection with OpenCV Library, Proceedings of XVI International Scientific Conference on Industrial Systems (IS'14), University of Novi Sad - Faculty of Technical Sciences,* Novi Sad, Serbia, ISBN 978-86-7892-652-5

2. Дамјановић Б., Марјановић З. (2013), Неки аспекти унутрашње структуре СУБП *Firebird* базе података, *InfoTech* 2013, Аранђеловац.

3. Дамјановић Б., Раниловић М. (2010), Стандарди, теоретске претпоставке и напредни алати као пут ка побољшању ефикасности израде информационих система, Ефикасност у привреди 2010, Зрењанин;

5. ЗАКЉУЧАК И ПРЕДЛОГ

Према мишљењу Комисије а на основу обављеног прегледа, може се закључити да је докторска дисертација „Адаптибилна примена *AES* алгоритма код савремених оперативних система“ урађена самостално и у свему је у складу са одобреном пријавом. По предмету истраживања, структурираности и оствареним резултатима представља оригинални допринос, како у теоријском делу, тако и у могућности директне примене у пракси. Постављени циљеви истраживања су у потпуности обрађени и истраживачке хипотезе научно тестиране. Имајући у виду све наведене чињенице, комисија Наставно-научног већа предлаже да се рад Бориса Дамјановића под називом „Адаптибилна примена *AES* алгоритма код савремених оперативних система“ прихвати као докторска дисертација, изложи на увид јавности, упути на коначно усвајање и да се кандидату одобри усмена одбрана.

ЧЛАНОВИ КОМИСИЈЕ:

_____

Проф. др Дејан Симић, редовни професор,
Универзитет у Београду, Факултет организационих наука

_____

Проф. др Душан Старчевић, редовни професор,
Универзитет у Београду, Факултет организационих наука

_____

Проф. др Бошко Николић, редовни професор
Универзитет у Београду, Електротехнички факултет

У Београду, 13. април 2016. године