Универзитет у Београду
Електротехнички факултет

НАСТАВНО-НАУЧНОМ ВЕЋУ

Предмет: Реферат о урађеној докторској дисертацији кандидата Жарка Станисављевића, мастер инжењера електротехнике и рачунарства

Одлуком Наставно-научног већа Електротехничког факултета у Београду бр. 5050/08-3 од 02.10.2014. године, именовани смо за чланове Комисије за преглед и оцену докторске дисертације кандидата Жарка Станисављевића под насловом

Визуелна репрезентација криптографских алгоритама

После прегледа достављене Дисертације и других пратећих материјала и разговора са Кандидатом, Комисија је сачинила следећи

Р Е Ф Е Р А Т

1. УВОД

1.1. Хронологија одобравања и израде дисертације

Кандидат Жарко Станисављевић, мастер инжењер електротехнике и рачунарства, уписао је докторске студије на Електротехничком факултету у Београду у школској 2008/2009. години. По истеку законског рока за завршетак докторских академских студија, на захтев студента, одобрено је продужење рока за завршетак ових студија за још два семестра, сагласно члану 92. став 4 Статута Универзитета у Београду.

Кандидат је пријавио тему за израду докторске дисертације на Електротехничком факултету у Београду 26.02.2014. године. Комисија за студије трећег степена Електротехничког факултета у Београду разматрала је предлог теме за израду докторске дисертације 05.03.2014. године. Наставно-научно веће именовало је Комисију за оцену услова и прихватање теме докторске дисертације на седници одржаној 25.03.2014. године, у саставу др Зоран Јовановић, редовни професор (ментор, Универзитет у Београду – Електротехнички факултет), др Бошко Николић, ванредни професор (Универзитет у Београду – Електротехнички факултет), др Горан Квашчев, доцент (Универзитет у Београду – Електротехнички факултет), др Душан Старчевић, редовни професор (Универзитет у Београду – Факултет организационих наука). Извештај Комисије за оцену услова и прихватање теме докторске дисертације Наставно-научно веће је прихватило на седници

одржаној 20.05.2014. године, а Веће научних области техничких наука Универзитета у Београду дало је сагласност на тему 09.06.2014. године (број одлуке 61206-2607/2014).

Кандидат је предао докторску дисертацију 27.08.2014. године. На седници одржаној 17.09.2014. године Комисија за студије трећег степена дала је сагласност за образовање Комисије за преглед и оцену докторске дисертације. На седници Наставно-научног већа одржаној 25.09.2014. године именована је Комисија за преглед и оцену докторске дисертације Жарка Станисављевића, мастер инжењера електротехнике и рачунарства, под насловом „Визуелна репрезентација криптографских алгоритама". Чланови комисије су: др Зоран Јовановић, редовни професор (ментор, Универзитет у Београду – Електротехнички факултет), др Павле Вулетић, доцент (Универзитет у Београду – Електротехнички факултет), др Душан Старчевић, редовни професор (Универзитет у Београду – Факултет организационих наука), др Бошко Николић, ванредни професор (Универзитет у Београду – Електротехнички факултет), др Славко Гајин, доцент (Универзитет у Београду – Електротехнички факултет).

1.2. Научна област дисертације

Научна област дисертације је Електротехника и рачунарство, а ужа научна област је Рачунарска техника и информатика. За ову ужу научну област матичан је Електротехнички факултет у Београду.

Дисертација је рађена под менторством редовног професора др Зорана Јовановића. Ментор испуњава законске услове за ментора, бави се научним радом у ужој области Рачунарска техника и информатика, професионално се бави рачунарским мрежама, а учествовао је у настави предмета Сигурност и заштита рачунарских система на којем се изучавају теме обрађене у дисертацији.

1.3. Биографски подаци о кандидату

Жарко Станисављевић, мастер инжењер електротехнике и рачунарства, рођен је 21.09.1984. године у Београду, Република Србија, од оца Славка и мајке Марине. Основну школу „Стеван Синђелић" и средњу школу „Никола Тесла" завршио је у Београду као један од најбољих ученика. Током школовања показивао је интересовање за природне науке и био учесник многих такмичења.

Електротехнички факултет Универзитета у Београду, одсек Рачунарска техника и информатика, уписао је 2003. године. Све факултетске обавезе је одрадио у предвиђеном року и дипломирао у августу 2007. године са просечном оценом 8,89. Дипломски рад под називом „Графички симулатор виртуелне меморије страничне организације са јединицом за директно пресликавање" одбранио је са оценом 10 код проф. др Јована Ђорђевића. Дипломске академске студије - мастер је уписао 2007. године на Електротехничком факултету Универзитета у Београду, одсек Рачунарска техника и информатика, и завршио их је 2008. године са просечном оценом 9,67. Мастер рад под називом „Симулатор модела pipeline процесора за наставу архитектуре и организације рачунара" одбранио је са оценом 10 код проф. др Јована Ђорђевића. Докторске академске студије је уписао у јануару 2009. године на Електротехничком факултету Универзитета у Београду, одсек Рачунарска техника и информатика. На докторским студијама је положио све испите са просечном оценом 9,9.

Од септембра 2007. године до марта 2008. године био је запослен у фирми Ариус у Београду на позицији софтверског инжењера за развој интернет апликација. Од марта 2008. године ангажован је хонорарно као сарадник у настави на Електротехничком факултету Универзитета у Београду и на пројектима Електротехничког факултета под руководством проф. др Зорана Јовановића, а од јануара 2010. године је запослен на Електротехничком факултету Универзитета у Београду као асистент у настави.

Од 2008. године до данас кандидат је активно учествовао у извођењу наставе на Електротехничком факултету Универзитета у Београду као асистент на следећим предметима: предмети на којима кандидат више није ангажован: Практикум из основа рачунарске технике, Практикум из коришћења рачунара, Пројектовање софтвера, Програмирање корисничких интерфејса и Архитектура и организација рачунара 2; предмети на којима је кандидат тренутно ангажован: Заштита података, Основи рачунарске технике 1, Архитектура и организација рачунара, Организација рачунара и Архитектура и организација рачунара 1. На предметима Заштита података и Практикум из основа рачунарске технике кандидат је учествовао у формирању лабораторијских вежби.

Коаутор је два рада у међународним часописима са *impact* фактором са SCI листе од којих је један у директној вези са дисертацијом, једног рада у домаћем часопису, два рада на међународним конференцијама и три рада на домаћим конференцијама.

2. ОПИС ДИСЕРТАЦИЈЕ

2.1. Садржај дисертације

Докторска дисертација садржи насловну страну и кратак резиме рада на српском и енглеском језику, садржај, девет поглавља, преглед коришћене литературе, кратку биографију аутора, изјаву о ауторству, изјаву о истоветности штампане и електронске верзије докторске дисертације и изјаву о коришћењу. Поглавља су насловљена: 1. Увод, 2. Преглед релевантне литературе, 3. Опис подржаних криптографских алгоритама у COALA систему, 4. Визуелна репрезентација у COALA систему, 5. Опис COALA система, 6. Имплементација COALA система, 7. Примена COALA система, 8. Евалуација COALA система, 9. Закључак. Дисертација садржи 173 стране, 79 илустрација и 21 табелу.

2.2. Кратак приказ појединачних поглавља

Прво поглавље представља увод у дисертацију. У овом поглављу је најпре објашњена мотивација за израду ове докторске дисертације, затим је постављен конкретан проблем који је решаван у докторској дисертацији и дат је један предлог решења постављеног проблема. У другом поглављу је направљен преглед релевантне литературе. Најпре се даје генерални преглед области система за помоћ у учењу. Потом је направљен преглед области визуелне репрезентације алгоритама, а након тога и области визуелне репрезентације криптографских алгоритама. На крају овог поглавља на основу анализе извучено је неколико важних закључака. Прво је дефинисано како треба да буде дизајниран систем за визуелну репрезентацију криптографских алгоритама. Затим је дефинисано како такав систем треба користити да би био ефикасан у настави. Након тога предложен је начин провере ефикасности система. И на крају је извршена анализа постојећих система како би се утврдило да ли већ постоји систем који испуњава све дефинисане захтеве. На основу донетих закључака проширен је почетни предлог решења постављеног проблема. У трећем поглављу је приказан опис криптографских алгоритама који су подржани у реализованом систему за визуелну репрезентацију криптографских алгоритама (COALA). Систем подржава пет врста криптографских алгоритама: супституционе алгоритме (Цезар алгоритам, моноалфабетски алгоритам, *Playfair* алгоритам и *Vigenere* алгоритам), транспозиционе алгоритме (*Rail Fence* алгоритам и *Row Transposition* алгоритам), продукционе алгоритме (*Rotor Machine* алгоритам), симетричне блок алгоритме (DES алгоритам и AES алгоритам) и алгоритме са јавним кључем (*Diffie-Hellman* алгоритам и RSA алгоритам). У четвртом поглављу су објашњени детаљи везани за визуелну репрезентацију алгоритама коришћену у COALA систему. На основу закључака изведених у поглављу 2 произашао је дизајн коришћен у

COALA систему. Најпре је приказано на који начин је извршена визуелна репрезентација класичних криптографских алгоритама. Специфично за ове алгоритме је да су дизајнирани да раде са текстуалним порукама, па је и визуелна репрезентација направљена на тај начин. Затим је објашњено на који начин је реализована визуелна репрезентација симетричних блок алгоритама. Иако су два подржана алгоритма из ове групе доста различита, осмишљен је начин да њихова визуелна репрезентација садржи униформне апстракције. На крају је приказано и на који начин је реализована визуелна репрезентација криптографских алгоритама са јавним кључем. Код ових алгоритама је било битно да се лако могу променити улазни параметри и да се одмах може испратити извршавање алгоритма. У петом поглављу је приказан детаљан функционални опис COALA система који је реализован. За сваки алгоритам дат је један или више примера коришћења кроз које су приказане све могућности реализованог система. У шестом поглављу су објашњени детаљи везани за софтверску имплементацију COALA система. Прво је дат преглед технологија коришћених за софтверску имплементацију, након тога је објашњена структура софтверског решења, потом су дати детаљи неопходних проширења стандардног API-ја (*Application Programming Interface*) која су направљена и на крају је објашњен начин извршавања алгоритама подржаних у COALA систему. Код објашњења структуре софтверског решења дат је преглед пакета и затим је за сваки пакет дат списак најзначајнијих класа уз објашњење шта која класа представља. У оквиру приказа детаља проширења стандардног API-ја за нове класе набројане су и описане битније методе, док су најзанимљивије и приказане у целости. Начин извршавања сложенијих алгоритама објашњен је између осталог и коришћењем UML дијаграма секвенци. У седмом поглављу је описан начин коришћења реализованог COALA система у оквиру предмета Заштита података на Електротехничком факултету у Београду. Описано је на који начин је систем уведен на предмет у оквиру лабораторијских вежби и дат је опис сваке од три лабораторијске вежбе које су осмишљене, а разматран је и начин испитивања на лабораторијским вежбама. У осмом поглављу је описана евалуација COALA система са аспекта ефикасности приликом примене на предмету Заштита података на Електротехничком факултету у Београду. Систем се користи у настави у претходне три школске године (уведен је у наставу 2011/2012. школске године). Анализа резултата коришћења система подељена је на три дела: анализу ефеката увођења система у наставу прве школске године, анализу напретка у коришћењу између прве и друге школске године и анализу утиска студената о коришћењу система кроз упитник који су попуњавали. У деветом поглављу даје се закључак, као критички осврт на испуњење циљева постављених на почетку рада, као и резиме свега урађеног. У закључку су сумирани остварени доприноси у оквиру докторске дисертације, а предложени су и даљи правци истраживања. На крају је дат преглед коришћене литературе.

3. ОЦЕНА ДИСЕРТАЦИЈЕ

3.1. Савременост и оригиналност

Предмет истраживања у докторској дисертацији је визуелна репрезентација криптографских алгоритама. Истраживање је на пресеку две области: визуелне репрезентације алгоритама (енгл. *algorithm visualization*) и алата који се користе као помоћ у учењу (енгл. *e-learning tools*). Област визуелне репрезентације алгоритама није нова, али је и даље актуелна. Област визуелне репрезентације криптографских алгоритама као подобласт области визуелне репрезентације алгоритама је у почетној фази развоја. Област алата који се користе као помоћ у учењу има дугу традицију и константно је актуелна. Анализом постојећих решења из поменутих области дошло се до оригиналне методе за визуелну

репрезентацију криптографских алгоритама која је предложена у дисертацији. Развијен је и систем који користи предложену методу. Систем има могућност визуелне репрезентације пет врста криптографских алгоритама: супституционих, транспозиционих, продукционих, симетричних блоковских и алгоритама са јавним кључем. Развијени систем је потпуно оригиналан, што је у раду показано упоређивањем са постојећим системима. Највећи искорак у односу на постојеће системе направљен је код најсложенијих алгоритама који су подржани (DES и AES). У раду је предложен и начин употребе реализованог система као алата за помоћ у учењу, а на основу анализе ефикасности оваквих алата. Евалуација система је извршена провером ефикасности система приликом коришћења у настави.

3.2. Осврт на референтну и коришћену литературу

Кандидат је детаљно претражио и упознао се са одговарајућом литературом. У дисертацији су прецизно наведене 82 библиографске референце на литературу која је у вези са темом дисертације. Литература садржи и најновије радове релевантне за тему дисертације, као и одговарајуће радове чији је кандидат коаутор. Једно поглавље дисертације посвећено је анализи релевантних приступа у решавању проблема визуелне репрезентације криптографских алгоритама. Искази у том поглављу, као и у осталим деловима дисертације, добро су поткрепљени цитатима одговарајућих радова.

3.3. Опис и адекватност примењених научних метода

Истраживање у оквиру докторске дисертације обухватило је следеће фазе:

1. систематично проучавање литературе из области алата за помоћ у учењу,
2. систематично проучавање литературе из области визуелне репрезентације алгоритама са посебним осврtом на подобласт визуелне репрезентације криптографских алгоритама,
3. развој нове методе за визуелну репрезентацију криптографских алгоритама на основу резултата претходне анализе,
4. имплементација софтверског система који примењује развијену методу,
5. дефинисање адекватног начина примене имплементираног система у образовном процесу,
6. примену имплементираног система у образовном процесу,
7. евалуацију успешности развијене методе и имплементираног система.

Наведени поступци у основи припадају и теоријским и експерименталним истраживањима, и у потпуности одговарају проблему и постављеном циљу дисертације. Примењене експерименталне методе су адекватне и валидне.

3.4. Применљивост остварених резултата

У оквиру дисертације представљена је оригинална метода за визуелну репрезентацију криптографских алгоритама, приказан је начин имплементације ове методе у оквиру софтверског система и предложен је начин примене таквог система у образовном процесу.

Предложена метода је верификована имплементацијом у пет врста криптографских алгоритама: супституционих (Цезар, моноалфабетски, *Playfair*, *Vigenere*), транспозиционих (*Rail Fence*, *Row Transposition*), продукционих (*Rotor Machine*), симетричних блоковских (*DES*, *AES*) и алгоритама са јавним кључем (*RSA*, *Diffie-Hellman*). Метода се лако може применити и на друге криптографске алгоритме. Имплементирани софтверски систем је коришћен у образовном процесу и експерименталним путем је утврђено да предложена метода побољшава успешност студената и олакшава им стицање знања из области криптографских алгоритама.

3.5. Оцена достигнутих способности кандидата за самостални научни рад

Кандидат је у изради дисертације показао способност за самостални научни рад. Израдио је систематичну и критичку анализу постојећих решења, уз уочавање њихових недостатака. Развио је оригиналну методу визуелне репрезентације криптографских алгоритама. Показао је да је метода практично применљива њеном употребом у оквиру реализованог система за визуелну репрезентацију криптографских алгоритама (COALA). Резултате својих истраживања објавио је у часопису од међународног значаја са признатим фактором утицаја.

4. ОСТВАРЕНИ НАУЧНИ ДОПРИНОС

4.1. Приказ остварених научних доприноса

Допринос изложене докторске дисертације је у домену развоја система за визуелну репрезентацију криптографских алгоритама. Као саставни делови дисертације садржани су следећи научни доприноси:

- Генерални преглед области алата за помоћ у учењу (енгл. *e-learning tools*).
- Генерални преглед области визуелне репрезентације алгоритама (енгл. *algorithm visualization*) уз осврт на постојећу систематизацију и класификацију ове области и са посебним акцентом на применљивости и ефикасности у образовном процесу.
- Систематизација и класификација постојећих решења у области визуелне репрезентације криптографских алгоритама.
- Генерализација функционалности постојећих система за визуелну репрезентацију криптографских алгоритама.
- Формирање нове методе за визуелну репрезентацију криптографских алгоритама на основу класификације и анализе постојећих решења из ове области.
- Предлог и имплементација оригиналног софтверског система за визуелну репрезентацију криптографских алгоритама који примењује осмишљену методу.
- Предлог начина примене имплементираног софтверског система у образовном процесу на основу анализе применљивости и ефикасности оваквих система.
- Евалуација ефикасности имплементираног софтверског система приликом примене у образовном процесу.

4.2. Критичка анализа резултата истраживања

Увидом у дисертацију, полазне хипотезе и циљеве истраживања, Комисија констатује да је кандидат успешно одговорио на постављене изазове, и да резултати оправдавају почетна очекивања. Предложен је оригиналан приступ развоју система за визуелну репрезентацију криптографских алгоритама. Провера практичне употребљивости осмишљене методе у оквиру реализованог софтверског система за визуелну репрезентацију криптографских алгоритама потврђује да предложени приступ нема само теоријски значај. Особине приступа чине га јединственим у односу на конкурентске приступе и употребљивим у великом броју реалних примена. Резултати и објашњења истраживања из дисертације су од интереса за све који су заинтересовани за област визуелне репрезентације криптографских алгоритама. Дисертација може допринети развоју нових система за визуелну репрезентацију криптографских алгоритама, затим развоју алата за генерисање конфигурабилних система за визуелну репрезентацију симетричних блоковских криптографских алгоритама заснованих на *Feistel* структури алгоритма и развоју нових алата за помоћ у учењу који би омогућили визуелну репрезентацију сигурносних протокола или апликација. На крају, дисертација може да буде од користи будућим генерацијама студената докторских студија, инжењерима, практичарима и истраживачима које интересује ова област и који у њој желе да дају свој допринос.

4.3. Верификација научних доприноса

Кандидат је објавио следеће радове који су у непосредној вези са докторском дисертацијом:

Категорија М23:

1. **Stanisavljevic, Z.**, Stanisavljevic, J., Vuletic, P., Jovanovic, Z.: *COALA - System for Visual Representation of Cryptography Algorithms*, IEEE Transactions on Learning Technologies, Vol. 7, No. 2, pp. 178-190, April-June 2014. (**IF=1.22**) (ISSN: 1939-1382) (doi: 10.1109/TLT.2014.2315992).

Категорија М52:

1. **Stanisavljevic, Z.**, Stanisavljevic, J.: *Softverski sistem za vizuelnu reprezentaciju klasičnih kriptografskih algoritama*, INFO M, Vol. 48, 2013, pp. 21-28.

Категорија М63:

1. **Stanisavljevic, Z.**, Stanisavljevic, J.: *Softverski sistem za vizuelnu reprezentaciju Advanced Encryption Standard algoritma*, Zbornik radova sa konferencije TELFOR 2011, Beograd 2011, str. 1364-1367.

5. ЗАКЉУЧАК И ПРЕДЛОГ

Дисертација кандидата Жарка Станисављевића, мастер инжењера електротехнике и рачунарства, под насловом „Визуелна репрезентација криптографских алгоритама“ представља оригиналан, савремен и значајан научни допринос. Текст дисертације написан је јасно и разумљиво и добро је организован кроз поглавља и одељке. Циљеви дисертације јасно су формулисани и мотивисани, а резултати истраживања систематски изложени, тако да се научни доприноси могу недвосмислено утврдити. У спроведеним истраживањима предложена је нова метода визуелне репрезентације криптографских алгоритама. Практична примена предложене методе потврђена је њеном употребом у оквиру система за визуелну репрезентацију криптографских алгоритама. Објављивањем резултата својих истраживања у часопису од међународног значаја, кандидат је показао способност за самосталан научни рад, а доприноси истраживања добили су адекватну потврду ваљаности.

Комисија констатује да дисертација садржи оригиналне научне доприносе, испуњава све законске, формалне и суштинске услове, као и све критеријуме који се уобичајено примењују приликом вредновања докторских дисертација на Електротехничком факултету у Београду. Комисија са задовољством предлаже Наставно-научном већу Електротехничког факултета у Београду да се докторска дисертација под називом „Визуелна репрезентација криптографских алгоритама“ кандидата Жарка Станисављевића, мастер инжењера електротехнике и рачунарства, прихвати, а кандидату одобри усмена одбрана.

У Београду, 17.10.2014. године

ЧЛАНОВИ КОМИСИЈЕ

др Зоран Јовановић, редовни професор
Универзитет у Београду – Електротехнички факултет

др Павле Вулетић, доцент
Универзитет у Београду – Електротехнички факултет

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

др Бошко Николић, ванредни професор
Универзитет у Београду – Електротехнички факултет

др Славко Гајин, доцент
Универзитет у Београду – Електротехнички факултет