Универзитет у Београду
Електротехнички факултет

НАСТАВНО-НАУЧНОМ ВЕЋУ

**Предмет:** Реферат о урађеној докторској дисертацији кандидата Борише Јовановића.

Одлуком Наставно-научног већа бр. 5040/2016-3 од 24.05.2018. године, именовани смо за чланове Комисије за преглед и оцену докторске дисертације кандидата Борише Јовановића, дипломираног инжењера рачунарске технике и информатике, под насловом

ЕФИКАСАН МЕХАНИЗАМ КРИПТОГРАФСКЕ СИНХРОНИЗАЦИЈЕ У АЛГОРИТМИМА СЕЛЕКТИВНОГ ШИФРОВАЊА МУЛТИМЕДИЈАЛНИХ СИСТЕМА НОВЕ ГЕНЕРАЦИЈЕ

После прегледа достављене дисертације, као 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 Бориша Јовановић, дипломирани инжењер рачунарске технике и информатике, докторске академске студије је уписао у новембру 2008. на студијском програму Електроника и рачунарство, модул Софтверско инжењерство. Новембра месеца 2016. године поновно је уписан на докторске академске студије на студијском програму Електроника и рачунарство, модул Софтверско инжењерство, уз признавање свих претходно положених испита.

Дана 26.10.2017. године пријавио је тему докторске дисертације под насловом „Ефикасан механизам криптографске синхронизације у алгоритмима селективног шифровања мултимедијалних система нове генерације“. Комисија за студије трећег степена разматрала је предлог теме за израду докторске дисертације и предлог Комисије о оцени подобности теме и кандидата упутила Наставно–научном већу на усвајање 31.10.2017. године. Одлуком Наставно-научног већа бр. 5040/16-1 од 16.11.2017. године, именована је Комисија за оцену подобности теме и кандидата за израду докторске дисертације и научне заснованости теме у саставу:

1. др Зоран Јовановић, редовни професор, Универзитет у Београду – Електротехнички факултет,
2. др Зоран Шеварац, доцент, Универзитет у Београду – Факултет организационих наука,
3. др Предраг Иваниш, ванреднини професор, Универзитет у Београду – Електротехнички факултет.

За ментора је именован доц. др Славко Гајин, Универзитет у Београду - Електротехнички факултет.

Усмена одбрана теме одржана је на Електротехничком факултету, 30.11.2017. године. На усменој одбрани су били присутни сви чланови Комисије. Одбрана је почела тако што је кандидат изложио предмет, циљ и методологију свог истраживања, као и мотивацију за његово спровођење. Потом су чланови комисије кандидату поставили неколико питања из области истраживања. На сва ова питања, кандидат је позитивно одговорио, што је Комисија потврдила оценом "задовољио". На основу одбране, као и поднетог Образложења теме, Извештај о подобности теме и кандидата Борише Јовановића за израду докторске дисертације под називом „Ефикасан механизам криптографске синхронизације у алгоритмима селективног шифровања мултимедијалних система нове генерације“ је поднела комисија у саставу:

1. др Зоран Јовановић, редовни професор, Универзитет у Београду – Електротехнички факултет,
2. др Зоран Шеварац, доцент, Универзитет у Београду – Факултет организационих наука,
3. др Предраг Иваниш, ванредни професор, Универзитет у Београду – Електротехнички факултет.

Наставно-научно веће Еектротехничког факултета у Београду је усвојило горе наведени извештај, одлуком бр. 5040/16-2 од 16.01.2018. године.

Веће научних области техничких наука Универзитета у Београду је 29.01.2018. године донело одлуку бр. 61206-276/2-18 чиме је дало сагласност на предлог теме докторске дисертације.

Кандидат је предао докторску дисертацију на преглед и оцену 05.04.2018. године. Комисија за студије трећег степена потврдила је испуњеност потребних услова за подношење предлога Наставно-научном већу Електротехничког факултета за формирање Комисије за преглед и оцену докторске дисертације 08.05.2018. године.

Коначно, Наставно-научно веће Електротехничког факултета је одлуком бр. 5040/16-3 од 24.05.2018. године именовало Комисију за преглед и оцену докторске дисертације Борише Јовановића, у саставу:

1. др Зоран Јовановић, редовни професор, Универзитет у Београду – Електротехнички факултет,
2. др Павле Вулетић, доцент, Универзитет у Београду – Електротехнички факултет,
3. др Владан Девецић, редовни професор, Универзитет у Београду – Факултет организационих наука.

## 1.2. Научна област дисертације

Научна област докторске дисертације под насловом „Ефикасан механизам криптографске синхронизације у алгоритмима селективног шифровања мултимедијалних система нове генерације“ кандидата Борише Јовановића је Електротехника и рачунарство, а ужа научна област Софтверско инжењерство. За наведену област матичан је Електротехнички факултет Универзитета у Београду.

Дисертација је урађена под менторством др Славка Гајина, доцента Електротехничког факултета Универзитета у Београду. Ментор има научне радове из уже научне области која је предмет дисертације кандидата. Поред тога, ментор предаје више предмета на Катедри за рачунарску технику и информатику на Електротехничком факултету, који су у вези са предметом дисертације. Релевантни радови ментора су наведени приликом пријаве теме докторске дисертације кандидата.

## 1.3. Биографски подаци о кандидату

Бориша Ж. Јовановић је рођен у Сурдулици 17.02.1982. године. Основну школу завршио је у Црној Трави, а гимназију, природно математички смер, у Власотинцу са оценом 5,00. Дипломирао је на Војној академији – Одсек Логистике, смер Служба Информатике по програму Рачунарска техника и информатика, као други у рангу, са просечном оценом 9,68. Одбранио је дипломски рад у области Вештачке интелигенције и експертских система, са освртом на њихову примену у наставно образовном процесу.

Од 2006. године запослен је у Центру за примењену математику и електронику, Управе за телекомуникације и информатику, Генералштаба Војске Србије. Као виши криптолог и начелник одсека за криптозаштиту у рачунарским мрежама, ради на руковођењу и реализацији већег броја научно-истраживачких пројекта у области вишеслојне архитектуре заштите рачунарских мрежа и криптозаштите у мобилним комуникацијама. Наведени пројекти и постигнути резултати су од великог значаја за безбедност рачунарских мрежа Министарства одбране и Војске Србије. Такође, ради као сарадник у настави и асистент на предметима „Заштита рачунарских система“ и „Оперативни системи“ на Војној академији у Београду. У звање асистента изабран је одлуком Наставно-научног већа Војне Академије, бр. 10-1087, на седници одржаној 05.12.2016. године.

У новембру 2008. је уписан на докторске студије на студијском програму Електроника и рачунарство, модул Софтверско инжењерство. Новембра месеца 2016. године је поновно уписан на докторске студије на студијском програму Електроника и рачунарство, модул Софтверско инжењерство, уз признавање свих претходно положених испита. На докторским студијама је стипендиста Министарства одбране Републике Србије.

Током докторских студија бавио се истраживањем у области безбедности рачунарских система, вишеслојне архитектуре криптозаштите рачунарских мрежа и примењене криптографије. Посебан акценат у истраживачком раду дат је у области примењене криптографије и на истраживању механизама шифровања и селективног шифровања у мултимедијалним информацијама – посебно у области видео компресије.

Аутор је једног рада у међународном часопису са *impact* фактором, једног рада на међународној конференцији и већег броја радова на домаћим конференцијама и у домаћим часописима.

## 2. ОПИС ДИСЕРТАЦИЈЕ

### 2.1. Садржај дисертације

Докторска дисертација је написана у седам поглавља, на 127 страна текста. Садржи 35 слика, 8 табела, као и списак од 75 коришћених референци.

Дисертација је структуирана у 7 (седам) поглавља чији су називи дати у наставку:

1. Увод
2. HEVC/H.265 – нови стандард компресије видео података
3. Теоријске основе селективног шифровања података
4. Криптографска основа понуђеног решења
5. Имплементација предложеног механизма криптографске синхронизације
6. Примена у војним комуникационим системима
7. Закључак

### 2.2. Кратак приказ појединих поглавља

Уводно поглавље докторске дисертације даје објашњење начина примене традиционалних криптографских алгоритама, којима се шифрује целокупни садржај видео података, као и објашњење начина примене савремених алгоритама селективног шифровања којима се шифрује само мали део видео података, уз очување задовољавајућег нивоа криптографске сигурности и значајну уштеду ресурса (процесорско време, рок трајања батерије на преносивим уређајима). Уводно поглавље идентификује и актуелни проблем алгоритама селективног шифровања. Ниједан од јавно доступних алгоритама селективног шифровања не дефинише адекватан и ефикасан механизам криптографске синхронизације приликом операције случајног приступа произвољном делу селективно шифрованог видео тока. Додатно, у уводном поглављу дат је и преглед научних доприноса предложене докторске дисертације са кратким освртом на резултате који су добијени током израде исте.

У другом поглављу дисертације дат је кратак преглед најновијег HEVC/H.265 (*HEVC – High Efficiency Video Coding*) стандарда компресије видео података са детаљним освртом на карактеристике и специфичности имплементације механизма случајног приступа у оквиру HEVC видео тока. Најновији стандард је описан кроз анализу основних карактеристика слоја кодовања видеа (*VCL – Video Coding Layer*) и слоја апстракције мреже. Слој кодовања видеа убухвата целокупну обраду слика на најнижем нивоу укључујући наменски дефинисану поделу слике на блокове (*quadtree* структуре), интер и интра предикцију, кодовање трансформације, кодовање ентропије и примењене филтере у петљи енкодера и декодера. Слој апстракције мреже обухвата енкапсулацију кодираних видео података, заједно са пратећим информацијама, у NAL (*NAL – Network Abstraction Layer*) јединице које представљају логичке формате пакета којима се видео подаци преносе различитим технологијама на транспортном слоју. Распоред и начин ешалонирања NAL јединица имају пресудан утицај на избор локације за смештање криптографских синхронизационих података у селективно шифровани HEVC видео ток.

У трећем поглављу је дата детаљна теоријска основа алгоритама селективног шифровања почевши од Шенонове теорије, и везе између компресије и шифровања података. Поред теоријске основе алгоритама селективног шифровања, ово поглавље дефинише и објашњава предности примене алгоритама селективног шифровања видео података као и њихову поделу. Такође, у овом поглављу су дефинисани елементи оцене перформанси алгоритама селективног шифровања који се на крају поглавља користе за анализу и оцену перформанси јавно доступних алгоритама селективног шифровања за најновији стандард компресије видео

података. На крају поглавља, дат је осврт на опште карактеристике доступних алгоритама селективног шифровања и уочена потреба за постојањем ефикасног механизма криптографске синхронизације приликом операције случајног приступа селективно шифрованом видео току који је независтан од примењеног алгоритма селективног шифровања.

Четврто поглавље се бави проблемом криптографске основе понуђеног механизма криптографске синхронизације, кроз кратак опис AES криптографског алгоритма који представља најчешће употребљавани стандардни симетрични блоковски криптографски алгоритам у алгоритмима селективног шифровања HEVC видео тока. Посебан аспект овог поглавља посвећен је модовима рада блоковских криптогафских алгоритама са освртом на то како наведени модови утичу на криптографску синхронизацију. Како је утицај различитих модова рада, на механизам криптографске синхронизације, потпуно различит потребно је да декодер приликом операције случајног приступа располаже синхронизационим подацима како би несметано дешифровао и декодира селективно шифровани видео ток.

У петом поглављу је детаљно описана синтакса и семантика понуђеног механизма криптографске синхронизације у алгоритмима селективног шифровања HEVC видео тока. Понуђено решење је реализовано кроз дефиницију синтаксе и семантике нове не-VCL NAL јединице која је названа CSPS NAL јединица (*CSPS – Cryptography Synchronization Parameter Set*) и која представља скуп параметара криптографске синхронизације. Овако дефинисана не-VCL NAL јединица може да представља и представља проширење HEVC стандарда. Такође, у овом поглављу је дефинисана, одређена и описана јасна и недвосмислена позиција на којој се новодефинисана NAL јединица смешта у HEVC видео ток. Наведена позиција је у потпуној сагласности са ограничењима везаним за распоред и положај NAL јединица, која су дефинисана HEVC/H.265 стандардом. У даљем делу петог поглавља дата је формална и теоријска спецификација ефикасности понуђеног решења која се огледа у процентуално исказаном броју додатих бајтова у селективно шифрованом HEVC видео току у односу на нешифровани HEVC видео ток. Теоријски је показано да је код видеа са већом резолуцијом ефикасност понуђеног решења већа. На самом крају петог поглавља дат је опис имплементације понуђеног решења. Опис имплементације је дат кроз опис модификације референте имплементације HEVC енкодера и опис модификације јавно доступне HEVC библиотеке отвореног кода, на страни декодера. Имплементација наведених модификација тестирана је на подскупу тест секвенци коришћеним у процесу стандардизације, док су резултати имплементације на систематичан начин обрађени и приказани у завршним разматрањима овог поглавља. Из резултата имплементације може се закључити да су претходно дефинисане теоријске претпоставке ефикасности понуђеног решења у потпуности потврђене.

Шесто поглавље представља теоријске основе могуће примене понуђеног решења у војним комуникационим системима. Понуђени механизам криптографске синхронизације је могуће користити у свим сегментима војних комуникација где год се користе и размењују селективно шифровани HEVC видео подаци. Према томе, наведени механизам се може користити у различитим наменским системима за извиђање и надзор из ваздуха као што су беспилотне летелице, у системима за надзор и физичко-техничку заштиту специфичних инфраструктурних објеката, у системима видеоконференцијске комуникације, у сателитским војним комуникационим системима и у војним комуникационим мрежама базираним на IEEE 802 стандарду (WiMAX и WiFI мреже).

Закључно, седмо поглавље садржи закључна разматрања као и правце за даљи рад који би као основу имали резултате приказане у овој докторској дисертацији.

## 3. ОЦЕНА ДИСЕРТАЦИЈЕ

### 3.1. Савременост и оригиналност

HEVC/H.265 је најновији стандард компресије видео података. Он представља најефикаснији систем компресије видеа данас који обезбеђује око 30-50% редукције битског протока (битске брзине) у односу на еквивалинтни перцептуални квалитет који се постиже претходним стандардом видео компресије – H.264/AVC. Како за претходни, тако и за најновији стандард компресије видео података, развијен је велики број јавно доступних алгоритама селективног шифровања. Ниједан од предложених алгоритама не разматра операцију случајног приступа селективно шифрованом видео току. Недостатак наведених јавно публикованих алгоритама селективног шифровања огледа се у томе што они не дефинишу механизме криптографске синхронизације процеса шифровања и дешифровања компресованог видео тока у моду рада са случајним приступом видео току. Случајни приступ селективно шифрованом видео току података је веома значајан за операције промене канала или промене извора тока видео података, операцију случајног скока на одређену локацију у складиштеним видео подацима као и у сервисима динамичког видео стриминга.

У оквиру дисертације је дефинисан оригиналан и ефикасан механизам криптографске синхронизације у оквиру селективно шифрованог HEVC видео тока. Дефинисање наведеног механизма представља потребан и довољан услов за имплементацију HEVC крипто енкодера и декодера са могућношћу случајног приступа селективно шифрованом видео току. Механизам криптографске синхронизације дефинисан је кроз дефиницију синтаксе и семантике NAL јединице која представља проширење стандарда. Кандидат је у дисертацији теоријски и практично показао и потврдио ефикасност понуђеног механизма кроз анализу његовог утицаја на повећање битског протока.

Имајући претходно наведено у виду, истраживања Борише Јовановића представљају оригиналан, значајан и вредан допринос, применљив у различитим мултимедијалним системима при операцијама промене канала или промене извора видео тока, као и при операцијама случајног скока на одређену позицију у селективно шифрованом видео току.

### 3.2. Осврт на референтну и коришћену литературу

У раду је коришћено 75 референци из релевантних часописа из области мултимедијалних система и алата, компресије видео података, обраде сигнала и криптографије. Имајући у виду да је тема дисертације уско везана са проблемом криптографске синхронизације у алгоритмима селективног шифровања најновијег стандарда компресије видео података, коришћене референце представљају публикације ширег временског оквира са циљем да се што објективније и тачније представи утицај изабраног криптографског мода рада на механизам криптографске синхронизације у савременим алгоритмима селективног шифровања. Референце укључене у дисертацију обухватају и рад који је објављен у часопису са SCI листе (са импакт фактором) и који садржи оригиналан дизајн ефикасног механизма криптографске синхронизације у алгоритмима селективног шифровања и резултате до којих је кандидат дошао у току научноистраживачког рада, а који је претходио овој докторској дисертацији у оквиру које је директно пружен научни допринос.

### 3.3. Опис и адекватност примењених научних метода

Кандидат је извршио критичку анализу доступних алгоритама селективног шифровања намењених најновијем стандарду компресије видео података, а као резултат те анализе настали су дизајн и резултати описани у овој дисертацији.

У контексту примене алгоритама селективног шифровања идентификовани су недостаци доступних алгоритама, па је кандидат извршио анализу постојећих и дао предлог сопственог, оригиналног и ефикасног механизма криптографске синхронизације у алгоритмима селективног шифровања HEVC видео тока. Као алат за истраживање и описивање резултата истраживања коришћена је референтна имплементација HEVC енкодера. Наведена референтна имплементација је надограђена, модификована и проширена тако да одговара предложеном дизајну. Кандидат је дао формалну спецификацију ефикасности понуђеног решења. Тачност формалне спецификације потврђена је имплементацијом и тестирањем имплементираног на подскупу тест секвенци које су коришћене приликом процеса стандардизације. Синтакса и семантика понуђеног решења у потпуности су у складу са техникама за дефинисање синтаксних елемената дефинсаних HEVC стандардом. За имплементацију је такође коришћена референтна имплементација HEVC енкодера.

### 3.4. Применљивост остварених резултата

Криптографска синхронизација приликом случајног приступа селективно шифрованом HEVC видео току веома је значајна за имплементацију операција промене канала или промене извора селективно шифрованог видео тока. Такође, значајна је и код операција случајног скока на одређену локацију у ускладиштеним видео подацима као и у сервисима динамичког видео стриминга. Код предлога новог механизма криптографске синхронизације морају се сагледати његова предност која се огледа у независности од примењеног алгоритма селективног шифровања. Такође, предложени механизам криптографске синхронизације је независтан од начина рада примењеног симетричног блоковског криптографског алгоритма.

Са друге стране, дефиниција наведеног дизајна представља потребан и довољан услов за имплементацију HEVC крипто енкодера и декодера са могућношћу случајног приступа селективно шифрованом видео току. Применљивост и ефикасност понуђеног механизма показана је кроз анализу његовог утицаја на повећање битског протока, али и теоријским сагледавањем могућности да се исти имплементира у различитим областима примене у војним комуникационим системима.

Имајући претходно у виду, може се сматрати да је постављени циљ истраживања испуњен, с обзиром да је у овој дисертацији предложени дизајн решења и анализирани су резултати како би се у потпуности покрила проблематика криптографске синхронизације у алгоритмима селективног шифровања у мултимедијалним системима нове генерације.

### 3.5. Оцена достигнутих способности кандидата за самостални научни рад

Кандидат Бориша Јовановић је у току припрема истраживања и израде своје докторске дисертације стекао мултидисциплинарно искуство и знање из области мултимедијалних система, компресије видео података и криптографије како са теоретског тако и са практичног аспекта. Његов научноистраживачки рад је посебно обухватао алгоритме селективног шифровања најновијег стандарда компресије видео података. Како би био у стању да пружи

научни допринос у свом раду, кандидат је направио критички осврт на тренутно стање механизама криптографске синхронизације у постојећим алгоритмима селективног шифровања, у чему му је помогло практично искуство у имплементацији различитих механизама криптографске заштите у војним комуникационим системима.

Дизајн понуђеног механизма криптографске синхронизације и његов утицај на повећање бутске брзине финалног видео тока захтевало је од кандидата да предложи формалну спецификацију ефикасности понуђеног решења. Систематски обрађени и приказани резултати у потпуности потврђују формално специфицирану ефикасности понуђеног механизма.

Током горе наведеног научно-истраживачког рада, кандидат је показао изузетну аналитичку способност и самосталност да анализира тренутно стање у наведеној области, да формулише и идентификује проблем и да за исти да предлог решења. Осим тога, кандидат је у својим научним доприносима дао критичке осврте на непостојеће механизме криптографске синхронизације у алгоритмима селективног шифровања на основу којих је формулисао ефикасан механизам криптографске синхронизације и дао резултате конкретне имплементације којим је потврдио ефикасност предложених решења.

## 4. ОСТВАРЕНИ НАУЧНИ ДОПРИНОС

### 4.1. Приказ остварених научних доприноса

Током свог научноистраживачког рада, кандидат је најпре пошао од критичке и компаративне анализе постојећих алгоритама селективног шифровања новог стандарда видео компресије. На основу резултата те анализе, кандидат је идентификовао кључни проблем у примени алгоритама селективног шифровања који се огледа у непостојању могућности криптографске синхронизације предајне и пријемне стране приликом операције случајног приступа селективно шифрованом HEVC видео току.

Као механизам криптографске синхронизације који се може једноставно имплементирати без озбиљних имплементационих проблема и са минималним модификацијама на страни енкодера и декодера, кандидат је предложио дизајн ефикасног механизам криптографске синхронизације кроз дефинисање синтаксе и семантике новог типа NAL поља која у себи садржи све релевантне информације потребне за имплементацију криптографске синхронизације приликом операције случајног приступа произвољној позицији селективно шифрованог видео тока. На основу тога, детаљни опис доприноса дисертације се даје у наставку:

- Кандидат је дао оригинални дизајн механизма криптографске синхронизације у алгоритмима селективног шифровања HEVC видео тока. Код предложеног механизма криптографске синхронизације је специфично то што је механизам понуђен и осмишљен као структурирана и прецизно дефинисана целина која припада видео току и представља новодефинисани елемент валидног HEVC видео тока.
- Понуђени механизам криптографске синхронизације је изразито ефикасан са аспекта његовог утицаја на повећање битског протока. У раду је спроведена компаративна анализа ефикасности понуђеног решења на тест секвенцама коришћеним у процесу стандардизације које припадају различитим класама секвенци.
- С обзиром да се као релевантан и репрезентативан елемент ефикасности понуђеног решења посматра његов утицај на повећање битског протока, како би се показала

величина утицаја на повећање битског протка, кандидат је дао формалну спецификацију ефикасности понуђеног решења.

- Спроведена је компаративна анализа постојећих алгоритама селективног шифровања, уз претходно дефинисање основних параметара за оцену њиховог квалитета. Овако систематски дефинисан скуп параметара за оцену квалитета алгоритама селективног шифровања доприноси њиховом бољем разумевању.
- Спроведено је практично тестирање кроз имплементацију два различита алгоритма селективног шифровања, чиме је потврђена универзалност понуђеног механизам криптографске синхронизације и његова независност од примењеног алгоритма селективног шифровања.
- Спроведена је компаративна анализа ефикасности понуђеног решења на различитим класама примењених тест секвенци којом је идентификована и потврђена полазна хипотеза да је ефикасност већа уколико се примењује над секвенцом са већом резолуцијом слике.
- Спроведена је анализа могуће употребе понуђеног решења и дат је теоријски осврт на могућу примену у војним комуникационим системима. Свуда где се HEVC видео може срести и применити, а где је потребно имплементирати механизам очувања тајности података, може се и применити дефинисани механизам криптографске синхронизације који омогућава случајни приступ селективно шифрованом HEVC видео току.

## 4.2. Критичка анализа резултата истраживања

Научни доприноси који проистичу из дисертације представљају значајан допринос у области криптографске синхронизације и у области примењене криптографије и алгоритама селективног шифровања HEVC видео тока. Остварени резултати научноистраживачког рада кандидата указују на валидност понуђеног механизма криптографске синхронизације јер се уз минимално повећање битског протока омогућава случајни приступ произвољној тачки у селективно шифрованом HEVC видео току.

Предложени дизајн механизам криптографске синхронизације, формална спецификација ефикасности и резултати практичних тестирања верификовани су кроз објављивање резултата ове дисертације у часопису од међународног значаја.

4.3. Верификација научних доприноса

Током свеобухватног и детаљног истраживања који је претходио изради дисертације, кандидат је објавио неколико радова, док је оригинални научни допринос дисертације верификован објављивањем рада у часопису са импакт фактором. Најзначајнији радови који се односе на научно истраживачки рад кандидата су следећи:

*Раду у истакнутом међународном часопису категорије (М22):*

1. **B. Jovanovic** i S. Gajin: „An efficient mechanism of cryptographic synchronization within selectively encrypted H.265/HEVC video stream", Multimedial tools and application, Volume 77, Number 2, 15 january 2018, 1537-1553 pages.(ISSN 1380-7501, doi: 10.1007/s11042-017-4389-3) – **IF 1.530 (2017)**

*Рад на међународном скупу (М33):*

1. **B. Jovanović**: "Criteria for evaluating the performance of IKEv2 implementation", The 4th International Scientific Conference on Defensive Tehnologies OTEH 2011, Belgrade, 6-7. 10. 2011, Miliraty Tehnical Institute, Belgrade. (ISBN 978-86-81123-50-8).

*Рад у часопису од националног значаја (М52):*

1. **B. Jovanović**, "Algoritmi selektivnog šifrovanja – pregled sa ocenom performansi", Vojnotehnički glasnik 4/2010, Ministarstvo odbrane Republike Srbije, Beograd, 2010. (ISSN 0042-8469)

*Saopštenje sa skupa nacionalnog značaja štampano u celini (M63):*

1. **B. Jovanović**: "JPSEC – Standardno okruženje za zaštitu slika u JPEG2000 formatu", 16-ti simpozijum o računarskim naukama i informacionim tehnologijama YU-INFO 2010, Kopaonik, Srbija, 3-6. 03. 2010. (ISBN 987-86-85525-05-6)
2. **B. Jovanović**, B. Planić: "Kriterijumi za ocenu performansi algoritama selektivnog šifrovanja", XXXVII Simpozijum o operacionim istraživanjima SYM-OP-IS 2011, Zlatibor, Srbija, 04.-07. 10. 2011. (ISBN 978-86-403-1168-7)

## 5. ЗАКЉУЧАК И ПРЕДЛОГ

На основу претходно наведеног, Комисија је закључила да докторска дисертација Борише Јовановића, под насловом: „Ефикасан механизам криптографске синхронизације у алгоритмима селективног шифровања мултимедијалних система нове генерације“ испуњава све формалне и суштинске услове предвиђене Законом о високом образовању, као и прописима Универзитета у Београду и Електротехничког факултета.

Предлози и резултати садржани у овој докторској дисертацији су верификовани објављивањем рада у часопису са импакт фактором. Ефикасност понуђеног механизма криптографске синхронизације у алгоритмима селективног шифровања верификована је на већам броју референтних тест секвенци. Додатно, наведеним предложеним дизајном механизма криптографске синхронизације из ове дисертације, кандидат је испунио све постављене почетне циљеве свог научноистраживачког рада.

Комисија предлаже Наставно-научном већу Електротехничког факултета да се докторска дисертација под насловом „Ефикасан механизам криптографске синхронизације у алгоритмима селективног шифровања мултимедијалних система нове генерације“ кандидата Борише Јовановића, прихвати, а затим упути на коначно усвајање Већу научних области техничких наука Универзитета у Београду и давање одобрења кандидату да приступи усменој одбрани.

Београд, 31.05.2018.

**ЧЛАНОВИ КОМИСИЈЕ**

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

др Павле Вулетић, доцент
Универзитет у Београду – Електротехнички факултет

др Владан Девецић, редовни професор
Универзитет у Београду – Факултет организационих наука