

НАСТАВНО-НАУЧНОМ ВЕЋУ

Предмет: Подобност теме и кандидата дипл. инж. рачунарске технике и информатике
Борише Јовановић за израду докторске дисертације

Одлуком Наставно-научног већа Електротехничког факултета бр. 5040/16-1 од 16.11.2017. године, именовани смо за чланове Комисије за оцену подобности теме и кандидата дипл. инж. рачунарске технике и информатике Борише Јовановић за израду докторске дисертације и научне заснованости теме

„Ефикасан механизам криптографске синхронизације у алгоритмима селективног шифровања мултимедијалних система нове генерације“.

На основу материјала приложеног уз Захтев кандидата, Комисија подноси следећи

ИЗВЕШТАЈ

1. Подаци о кандидату

1.1. Биографски подаци

Дипл. инж. рачунарске технике и информатике Бориша Јовановић је рођен у Сурдулици 17.02.1982. године. Дипломирао је на Војној академији – Одсек Логистике, смер Служба Информатике по програму Рачунарска техника и информатика са средњом оценом 9,68 и оценом 10 на дипломском раду. 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 пројекта у области вишеслојне архитектуре заштите рачунарских мрежа. 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 предмету „Заштита рачунарских система“ и "Оперативни системи" на Војној академији у Београду.

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 механизма шифровања и селективног шифровања у мултимедијалним информацијама – посебно у области видео компресије.

На докторским студијама је стипендиста Министарства одбране Републике Србије.

Пројекти:

2006-2011: „Криптозаштита у рачунарским мрежама – заштита на мрежном нивоу“ – истраживачко-развојни пројекат у оквиру планских активности у Министарству одбране и Војсци Србије.

2010-2012: „Универзална корисничка софтверска платформа Географски Информациони Систем Војске Србије“ – учешће у својству члана истраживачког тима који учествује у пројектовању и надгледању реализације и имплементације механизма криптозаштите у наведеном информационом систему.

2011-2014: „Криптозаштита у рачунарским мрежама – заштита на транспортном нивоу“ – истраживачко-развојни пројекат у оквиру планских активности у Министарству одбране и Војсци Србије.

2015-у току: "Криптозаштита у мобилним комуникацијала" истраживачко-развојни пројекат у оквиру планских активности у Министарству одбране и Војсци Србије.

1.2. Стечено научноистраживачко искуство

Кандидат је докторске студије првобитно уписао школске 2008/2009. године, на Универзитету у Београду - Електротехнички факултет, на студијском програму Електротехника и рачунарство, модул Софтверско инжењерство, где је све испите положио са највишом оценом и урадио све обавезе предвиђене планом и програмом докторских студија. Након истека предвиђеног периода, кандидат је докторске студије поново уписао школске 2016/2017. године на Универзитету у Београду - Електротехнички факултет, на студијском програму Електротехника и рачунарство, модул Софтверско инжењерство, где су му признати сви претходно положени испити, и то:

1. ТСР/ИР Архитектура – оцена 10 (9 ЕСП бодова)
2. Сигурност и заштита рачунарских мрежа – оцена 10 (9 ЕСП бодова)
3. Софтверска техника – оцена 10 (9 ЕСП бодова)
4. Одабрана поглавља из оперативних система – оцена 10 (9 ЕСП бодова)
5. Принципи програмских језика – оцена 10 (9 ЕСП бодова)
6. Вештачка интелигенција и експертски системи – оцена 10 (9 ЕСП бодова)
7. Одабрана поглавља из објектних технологија – оцена 10 (9 ЕСП бодова)
8. Софтверски системи за рад у реалном времену – оцена 10 (9 ЕСП бодова)
9. Енглески језик – оцена 10 (6 ЕСП бодова).

У оквиру студијско истраживачког рада кандидат је урадио свеобухватан преглед и анализу постојећих алгоритама селективног шифровања са оценом перформанси. Рад је публикован у Војнотехничком гласнику 4/2010. Кандидат у оквиру свог радног места учествује и реализује већи број истраживачко-развојних пројеката који су до сада као резултат имали софтверско-хардверска решења за криптозаштиту у рачунарским мрежама која су усвојена у оперативну употребу и користе се у Телекомуникационо-информационом систему Министарства одбране и Војске Србије.

1.2.1. Објављени радови

M22-Рад у истакнутом међународном часопису

1. B. Jovanović, S. Gajin, An efficient mechanism of cryptographic synchronization within selectively encrypted H.265/HEVC video stream, Multimedia Tools and Applications (2017), pp. 1-17. (<https://doi.org/10.1007/s11042-017-4389-3>, ISSN: 1380-7501)

M33-Саопштење са међународног скупа штампано у целини

2. B. Jovanović: "Criteria for evaluating the performance of IKEv2 implementation", The 4th International Scientific Conference on Defensive Technologies OTEH 2011, Belgrade, 6-7. 10. 2011, Military Technical Institute, Belgrade.

M52-Часописи националног значаја

1. R. S. Gordić, B. Jovanović, Đ. Alfrević: "Izbor optimalnog puta za kretanje organizovanog kolonskog saobraćajnog toka na osnovu rezultata modeliranja", Vojnotehnički glasnik 2/2006, Ministarstvo odbrane Republike Srbije, Beograd, ISSN 0042-8469, Vol. 54, No. 2, 2006, str 202-213.
2. B. Jovanović, "Algoritmi selektivnog šifrovanja – pregled sa ocenom performansi", Vojnotehnički glasnik 4/2010, Ministarstvo odbrane Republike Srbije, Beograd, ISSN 0042-8469, Vol. 58, No. 4, 2010, str 134-154.

M63-Саопштење са скупа националног значаја штампано у целини

1. B. Jovanović, G. Šimić: "Ugradnja modela korisnika u sisteme za upravljanje sadržajem", 12-ti simpozijum o računarskim naukama i informacionim tehnologijama YU-INFO 2006, Kopaonik, Srbija i Crna Gora, 6-10. 03. 2006.
2. B. Jovanović, I. Tot, M. Merdžanović: "Razvoj informacionog sistema 'Vojne sportske reprezentacije' primenom UML tehnologija", XXXIII Simpozijum o operacionim istraživanjima SYM-OP-IS 2006, Banja Koviljača, Srbija, 03.-06. 10. 2006.
3. B. Jovanović: "Različite arhitekture virtuelnih privatnih mreža", 14-ti simpozijum o računarskim naukama i informacionim tehnologijama YU-INFO 2008, Kopaonik, Srbija, 9-12. 03. 2008.
4. 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.
5. B. Jovanović, B. Planić: "Kriterijumi za ocenu performansi algoritama selektivnog šifrovanja", XXXVII Simpozijum o operacionim istraživanjima SYM-OP-IS 2010, Zlatibor, Srbija, 04.-07. 10. 2011.
6. B. Jovanović: "Analiza ranjivosti implementacije IPsec protokola na LINUX operativnom sistemu", Zbornik radova 56. konferencija ETRAN, Zlatibor, 11.-14.06.2014

1.2.2. Извештај са јавне усмене одбране предложене теме докторске дисертације

Јавна усмена одбрана предложене теме докторске дисертације одржана је 30.11.2017. године на Електротехничком факултету Универзитета у Београду, пред комисијом у саставу:

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

Усмена одбрана је почела у 15:00 часова, а завршена је у 15:30 часова.

На усменој одбрани су били присутни сви чланови Комисије. Одбрану је отворио проф. др Зоран Јовановић, упознавши присутне са хронологијом пријаве теме, одлуком Наставно-научног већа, основним подацима о кандидату и основним подацима о пријављеној теми докторске дисертације. Кандидат је у трајању од 25 минута изложио у најсажетијем облику област и предмет истраживања, актуелност истраживања, постојећа решења са критичким освртом, као и своје полазне хипотезе, планирану методологију рада, очекиване, као и већ остварене резултате, укључујући и остварени научни допринос.

Професор Предраг Иваниш је поставио два питања. Прво питање је било зашто постоји захтев да се не нарушава валидност видео стрима, а друго питање је било како се ради синхронизација када се не зна почетак видео стрима или се нешто неочекивано деси на извору.

Доцент Шеварац је поставио два питања. Прво питање је било по чему је предложени систем енкрипције ефикаснији од других алгоритама и по којим параметрима се они пореде. Друго питање се односило на чињеницу да је референтни модел јаван, а да та јавност можда потенцијално нарушава безбедност система.

Професор Јовановић је поставио питање да ли се мења комплексност алгоритма са значајним повећањем резолуције видео стрима.

Кандидат Бориша Јовановић је успешно одговорио на сва постављена питања.

По завршеној одбрани, Комисија се повукла на већање и једногласно донела следећи закључак:

Комисија је закључила да је кандидат Бориша Јовановић на јавној усменој одбрани предложене теме докторске дисертације добио оцену „задовољно“. Комисија предлаже да ментор докторске дисертације буде др Славко Гајин, доцент Електротехничког факултета Универзитета у Београду.

1.3. Оцена подобности кандидата за рад на предложеној теми

Комисија је размотрила све претходно наведене резултате досадашњег рада и стечена искуства кандидата. На основу тога Комисија је стекла увид у способности кандидата за научно-истраживачки рад и његове могућности да током израде докторске дисертације оствари резултате који ће бити приказани и оцењени од стране међународне научне заједнице. Став Комисије је да дипл. инж. рачунарске технике и информатике Бориша Јовановић испуњава потребне услове да приступи изради докторске дисертације под наведеном темом.

2. Предмет и циљ истраживања

Брзи развој дигиталне мултимедије, доступност већих пропусних опсега у оквиру комуникационих мрежа и пораст процесорске снаге проузроковали су свакодневно коришћење дигиталних мултимедијалних података на различитим уређајима и у различитим сферама живота. На тај начин, велика количина како личних тако и пословних мултимедијалних података постаје јавно доступно и могу бити лако украдени, копирани или модификовани. HEVC (High Efficiency Video Coding) је најновији стандард компресије видео података који су заједно развиле институције ITU-T и ISO/IEC и који је публикован 2013. године [1]. Овај стандард представља најефикаснији систем компресије видеа данас који обезбеђује око 30-50% редукације битског протока (битске брзине) у односу на еквивалентни перцептуални квалитет који се постиже претходним стандардом видео компресије - H.264/AVC [2]. Међутим, овај стандард не обезбеђује безбедносне механизме којима се имплементирају криптографски сервиси: тајност, интегритет и аутентичност. Тачније, као и у претходним стандардима видео компресије, стандардизовани су синтакса и структура тока података, као и ограничења на самом току података и мапирања потребна за генерисање декодованих слика [3]. Постоји неколико јавно доступних алгоритама селективног шифровања за претходни H.264/AVC стандард компресије и неколико нових за нови

стандард – HEVC. Алгоритми селективног шифровања се користе да ограниче приступ оригиналним подацима у видео току података само овлашћеним корисницима који поседују исправан тајни кључ. Заштита тајности се постиже селективним шифровањем малог дела података у видео току података. Селективним шифровањем видео тока податка постиже се жељени и, теоријски доказиво, довољни ниво криптографске заштите наведених података а такође се постижу значајне уштеде у процесорском времену обраде података. Овакав начин очувања процесорске снаге је веома пожељан у комуникационим системима са ограниченим ресурсима (мрежне апликације које раде у реалном времену, размена слика и видео садржаја високог квалитета и резолуције, мобилни системи са уређајима који имају ограничену процесорску снагу и ограничен век батерије).

Након што је финална верзија HEVC/H.265 стандарда публикована, отпочео је процес истраживања, дизајнирања и развоја алгоритама селективног шифровања тока података који је резултат компресије видео података применом новог стандарда компресије. У [4] група истраживача је дизајнирала алгоритам чији је шифрат компатибилан по формату са оригиналним (нешифрованим) HEVC видео током података. Компатибилност по формату се постиже шифровањем одређеног подскупа бинстрингова у кодеру ентропије. Наведени стандард као кодер ентропије користи контекстно адаптивно бинарно аритметичко кодовање - CABAC (CABAC – Context-Adaptive Binary Arithmetic Coding). Алгоритам селективног шифровања дизајниран у [4] не уноси ниједан додатни бит у селективно шифровани ток видео података, а експериментални подаци приказани у наведеном раду показују и доказују да наведени алгоритам, уз употребу AES криптографског алгоритма у CBC моду рада, пружа задовољавајући ниво криптографске сигурности. У раду [5] такође је дизајниран алгоритам селективног шифровања HEVC видео тока података који је компатибилан по формату. У овом алгоритму је најпре идентификован подскуп синтаксних елемената који не утичу на сам процес декодовања, а онда је такав подскуп синтаксних података шифрован AES криптографским алгоритмом.

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 података у моду рада са случајним приступом видео току. Случајни приступ 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 [3].

Циљ истраживања је да се дефинише дизајн ефикасног механизма криптографске синхронизације у оквиру селективно шифрованог 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. Такође, циљ истраживања је да се ефикасност понуђеног механизма покаже кроз анализу његовог утицаја на повећање битског протока и сагледавањем могућности да се понуђен дизајн имплементира у различитим областима примене. Целокупно истраживање и анализа биће реализовано употребом референтне имплементације наведеног стандарда над тест секвенцама, резолуција од 416x240 до 2560x1600, које су коришћене током процеса стандардизације новог HEVC стандарда [6].

У литератури није обрађиван проблем селективног шифровања заједно са механизмима криптографске синхронизације и случајног приступа шифрованом видео току података. Случајни приступ шифрованом садржају је веома значајан за било који вид размене селективно шифрованог видео садржаја почевши од Интернет стриминга, конверзација у реалном времену (video chat), видеоконференције и различитих система комуникације и колаборације разменом видео садржаја до складиштења дигиталног видео садржаја или емитовања телевизијског сигнала велике резолуције (HD) преко сателита, кабловских и земаљских система преноса. Посебно значајна примена наведеног решења је у војним системима [7]:

- за видео праћење (надзор, даљинско надгледање и прикупљање обавештајних података) из ваздуха;
- за видео надзор и обезбеђење објеката посебне намене;
- сателитских војних комуникација;
- код бежичних комуникационих технологија (Wi-Fi и Wi-MAX) у војним применама.

РЕЛЕВАНТНИ БИБЛИОГРАФСКИ ИЗВОРИ:

- [1] High Efficiency Video Coding, Rec. ITU-T H. 265 and ISO/IEC, 23008-2, January 2013.
- [2] J.-R. Ohm, G. J. Sullivan, H. Schwarz, T. K. Tan, and T. Wiegand, "Comparison of the coding efficiency of video coding standards - Including High Efficiency Video Coding (HEVC)," IEEE Trans. Circuits Syst. Video Technol., vol. 22, no. 12, pp. 1668–1683, Dec. 2012.
- [3] G. J. Sullivan, J.-R. Ohm, W.-J. Han, and T. Wiegand, "Overview of the High Efficiency Video Coding (HEVC) Standard", IEEE Circuits and Systems for Video Technology, vol. 22, no. 12, pp. 1649 –1668, Dec. 2012.
- [4] Z. Shahid and W. Puech, "Visual Protection of HEVC Video by Selective Encryption of CABAC Binstrings," IEEE Transactions on Multimedia, vol. 16, pp 24-36, January 2014.
- [5] Van Wallendael, G., Boho, A., De Cock, J., Munteanu, A., and Van de Walle, R. (Aug. 2013). Encryption for High Efficiency Video Coding with Video Adaptation Capabilities. IEEE Transaction on Consumer Electronics 59(3) 634-642.
- [6] V. Baroncini, J.-R. Ohm, and G. Sullivan, "Report of Subjective Test Results of Responses to the Joint Call for Proposals (CfP) on Video Coding Technology for High Efficiency Video Coding (HEVC)," ITU-T/ISO/IEC Joint Collaborative Team on Video Coding (JCT-VC), Doc. JCTVC-A204, Geneva, CH, Tech. Rep., April 15-23 2010
- [7] Z. Miličević, "Multimedijalni H.264/AVC standard u vojnim komunikacionim sistemima", XXVI Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – PosTel 2008, Beograd 16. i 17. decembar 2008. godine

3. Полазне хипотезе

Основне хипотезе предложене докторске дисертације су следеће:

- Могуће је дизајнирати HEVC компатибилни енкодер који представља ефикасан механизам за имплементацију криптографске синхронизације у алгоритмима селективног шифровања HEVC видео тока података.
- Могуће је реализовати случајан приступ селективно шифрованом HEVC видео току података.
- Понуђени дизајн представља проширење HEVC стандарда видео компресије независан од примењеног алгоритма селективног шифровања.

- Могућа је примена за криптозаштиту видео података у војним комуникационим системима, коришћењем постојећих или нових алгоритама селективног шифровања.

4. Научне методе истраживања

Неколико научних метода ће бити примењено у циљу провере наведених полазних хипотеза и остварења задатих истраживачких циљева:

- Прикупљање и сређивање података о доступним алгоритмима селективног шифровања на основу доступне литературе, претраживањем Интернета, разменом информација и непосредним контактима са релевантним субјектима у свету.
- Компаративна анализа и преглед постојећих алгоритама селективног шифровања HEVC видео тока података.
- Компаративна анализа постојећих и предлог сопственог дизајна ефикасног HEVC крипто енкодера са механизмом криптографске синхронизације и могућношћу случајног приступа.
- Компаративна анализа могућности имплементације предложеног дизајна механизма криптографске синхронизације.
- Имплементација предложеног дизајна ефикасног HEVC крипто енкодера. Као алат за истраживање и описивање резултата истраживања биће коришћена референтна имплементација HEVC енкодера која ће бити надограђена и проширена тако да одговара предложеном дизајну.
- Формална спецификација резултата истраживања и верификација полазних хипотеза на тест секвенцама применом модификоване референтне имплементације.

5. Очекивани научни допринос

Значај овог истраживања је у томе што ће понуђени дизајн проширити наведени стандард и тиме значајно унапреди постојећи алгоритми селективног шифровања HEVC видео тока података. Допринос овог рада ће се огледати у оригиналности понуђеног механизма криптографске синхронизације који има примену у свакој области где се сам стандард компресије видео података користи, а у којој је потребно имплементирати криптографске сервисе очувања тајности и интегритета мултимедијалних података. У складу са тим, очекивани су следећи научни доприноси докторске дисертације:

- Оригинални дизајн механизма криптографске синхронизације у алгоритмима селективног шифровања HEVC видео тока података.
- Ефикасност механизма имплементације случајног приступа селективно шифрованом HEVC видео току података.
- Универзалност новог решења, јер оно треба да представља дизајн механизма криптографске синхронизације који је независан од примењеног алгоритма селективног шифровања.
- Допринос бољем разумевању алгоритама селективног шифровања у видео току.

- Понуђено решење ће се моћи примењивати у свим областима примене где се HEVC видео стандард примењује, а где је потребна имплементација криптографских сервиса за очување тајности и интегритета.
- Посебан допринос ће се дати у теоријској анализи могућности примене понуђеног решења у војним комуникационим системима.

6. План истраживања и структура рада

Предложено истраживање обухватаће следеће активности:

- Преглед и анализа релевантне литературе и праксе која се бави следећим областима: стандарди компресије видео података, примењена криптографија и селективно шифровање, селективно шифровање видео података, технике криптографске синхронизације.
- Дефинисање проблема, класификација алгоритама селективног шифровања и указивање на недостатке постојећих алгоритама селективног шифровања.
- Формална спецификација понуђеног дизајна ефикасног HEVC крипто енкодера са могућношћу случајног приступа.
- Имплементација понуђеног решења у референтну имплементацију HEVC енкодера са имплементацијом изабраног алгорита селективног шифровања.
- Анализа постигнутих резултата над тест секвенцама са освртом на ефикасност понуђеног решења.
- Теоријске основе могуће примене понуђеног решења у војним комуникационим системима.

7. Закључак и предлог

Након увида у наведене резултате досадашњег рада кандидата дипл. инж. рачунарске технике и информатике Борише Јовановић, Комисија је донела одлуку да је он способан за научно-истраживачки рад и за реализацију предвиђених истраживања. Одлука је донета имајући у виду његове досадашње стручне резултате остварене током основних и докторских студија, као и на основу његовог досадашњег истраживачког ангажовања на више пројеката. Такође, Комисија је мишљења да је предложена тема докторске дисертације „Ефикасан механизам криптографске синхронизације у алгоритмима селективног шифровања мултимедијалних система нове генерације“ адекватна у смислу наведених непосредних циљева рада, очекиваних резултата и научних доприноса, као и у контексту савремених научних истраживања у предложеној области. Комисија констатује да тема рада припада области Софтверско инжењерство за коју је Електротехнички факултет у Београду матичан и за ментора рада се предлаже др Славко Гајин, доцент Електротехничког факултета Универзитета у Београду. Из тог разлога уз овај Извештај је приложен и списак радова доцента др Славка Гајина који га квалификују за ментора.

Имајући у виду чињенице наведене у овом извештају, Комисија предлаже Наставно-научном већу Електротехничког факултета у Београду да прихвати тему докторске дисертације „Ефикасан механизам криптографске синхронизације у алгоритмима селективног шифровања мултимедијалних система нове генерације“ и да кандидату дипл. инж. рачунарске технике и информатике Бориши Јовановић омогући да приступи њеној изради.

У Београду, 8.12.2017. године

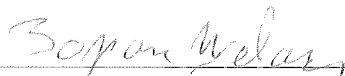
ЧЛАНОВИ КОМИСИЈЕ



др Славко Гајин, доцент,
Универзитет у Београду – Електротехнички факултет



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



др Зоран Шеварац, доцент
Универзитет у Београду – Факултет организационих наука



др Предраг Иваниш, ванредни професор,
Универзитет у Београду – Електротехнички факултет