Универзитет у Београду
Електротехнички факултет

НАСТАВНО-НАУЧНОМ ВЕЋУ

Предмет: Подобност теме и кандидата дипл. инж. електротехнике Omran Al Rasheed за израду докторске дисертације

Одлуком Наставно-научног већа Електротехничког факултета Универзитета у Београду бр. 5049/11-1 од 29.4.2015. године, именовани смо за чланове Комисије за оцену подобности теме и кандидата Omran Al Rasheed, дипл. инж. електротехнике, за израду докторске дисертације и научне заснованости теме

„Алгоритми декодовања мале комплексности погодни за примену у асиметричним криптосистемима"

"Low complexity decoding algorithms suitable for application in asymmetric cryptosystems"

На основу материјала приложеног уз Захтев кандидата, Комисија подноси следећи

И З В Е Ш Т А Ј

1. Подаци о кандидату

1.1. Биографски подаци

Omran Al Rasheed рођен је 30.01.1984. године у Shekh Mesken, Сирија. Основну школу и гимназију завршио је у Shekh Mesken са одличним успехом. Електротехнички и електронски факултет Универзитета у Алепу уписао је школске 2003/04. године. Дипломирао је на Одсеку за електронику и телекомуникације 2008. године, са просечном оценом 74.46/100.00. Дипломски рад под насловом "Designing Patch Antenna for GPS System", одбранио је са оценом 93/100. Ментор дипломског рада био је dr. Rami Alkhatib. Тренутно је студент докторских студија на Електротехничком факултету Универзитета у Београду, на модулу Телекомуникације.

Има активно знање арапског, енглеског и српског језика и основно знање немачког језика.

1.2. Стечено научноистраживачко искуство

Докторске студије уписао је школске 2011. године на Електротехничком факултету Универзитета у Београду, на модулу Телекомуникације, где је положио све испите са највишом оценом и урадио све обавезе предвиђене планом и програмом докторских студија.

Списак положених испита:

1. Случајни процеси у телекомуникацијама (оцена: 10, 9 ЕСПБ)
2. Савремене технике контроле грешака у телекомуникацијама (оцена: 10, 9 ЕСПБ)
3. Класификација и естимација сигнала (оцена: 10, 9 ЕСПБ)
4. Линеарне и нелинеарне методе анализе сигнала (оцена: 10, 9 ЕСПБ)
5. Савремене радио-технологие (оцена: 10, 9 ЕСПБ)
6. Симболичка обрада сигнала (оцена: 10, 9 ЕСПБ)
7. Просторно-временска обрада сигнала (оцена: 10, 9 ЕСПБ)
8. Нумеричка анализа (оцена: 10, 9 ЕСПБ)
9. Специјалне функције (оцена: 10, 9 ЕСПБ)
10. Увод у научни рад (оцена: 10, 6 ЕСПБ)

У оквиру предмета на докторским студијама урадио је задатке који покривају различите области телекомуникација, а који подразумевају проучавање литературе, познавање теорије, израду програма којима су имплементирани разни алгоритми битни за функционисање телекомуникационих система.

Конкретно, активности по предметима су следеће:

1. Случајни процеси у телекомуникацијама: проучавање литературе и провера теоријског знања, израда програма у софтверском пакету *Matlab* за прорачун перформанси бежичног телекомуникационог система у коме су примењени просторно-временски кодови;

2. Савремене технике контроле грешака у телекомуникацијама: проучавање литературе, писање већег броја програма у програмском језику C у којима су имплементирани разни алгоритми за декодовање кодова са малом густином провера парности (*Low Density Parity Check*, LDPC). Посебна пажња посвећена је ефикасној имплементацији алгоритма декодовања на основу сумирања и производа (*Sum Product Algorithm*, SPA).

3. Класификација и естимација сигнала: проучавање литературе, провера теоријског знања, пројектовање параметарских и непараметарских класификатора и практичан рад за класификацију коришћењем неуралних мрежа (*Neural Networks*, NN).

4. Линеарне и нелинеарне методе анализе сигнала: похађање предавања о карактеристикама сложених просторно-временских сигнала и издвајању доминантних компонената сигнала, израда семинарских радова и презентација о анализи помоћу главних компонената (*Principal Component Analysis*, PCA), детрендованој анализи одступања (*Detrended Fluctuation Analysis*, DFA), фракталној и мултифракталној анализи сигнала и њиховим применама.

5. Савремене радио-технологије: проучавање литературе, семинарски рад који је за тему имао кодовање и декодовање у LTE систему (*Long Term Evolution*, LTE).

6. Симболичка обрада сигнала: проучавање литературе, провера теоријског знања, израда програма у софтверском пакету *Matlab* за пројектовање аналогних и дигиталних филтара коришћењем система рачунарске алгебре.

7. Просторно-временска обрада сигнала: предавања, консултације, израда програма у софтверском пакету *Matlab* за анализу примене антенских низова у телекомуникационим системима коришћењем техника вештачке интелигенције (*Partical Swarm Optimization*, PSO).

8. Нумеричка анализа: проучавање литературе, провера теоријског знања и вежбе.

9. Специјалне функције: проучавање литературе, провера теоријског знања и семинарски рад везан за примену специјалних функција у телекомуникационим системима.

10. Увод у научни рад: проучавање начина за припрему рада за објављивање у научном часопису и приказ истраживања на научним конференцијама. Припремање студента да оформи докторску тезу, припреми семинар о проблему који истражује, успешно комуницира са редакторима и рецензентима научних часописа.

Окосницу истраживачког рада у вези са докторском тезом чини развој новог алгоритма за декодовање LDPC кодова кога одликују мала комплексност и добре перформансе. У другом делу рада на тези, развијени алгоритам је примењен на унапређење сигурности криптосистема са јавним и тајним кључевима. Радови из ове области, чији је први аутор, прихваћени су и презентовани на међународним конференцијама, један рад је објављен у међународном часопису а два рада су објављена у домаћем часопису.

1.2.1. Објављени радови

Рад публикован у страном часопису (M22):

[1.1] O. Al Rasheed, P. Ivanis, and B. Vasic, "Fault-Tolerant Probabilistic Gradient-Descent Bit Flipping Decoder," *IEEE Communications Letters*, vol. 18, no. 9, September 2014, pp. 1487–1490. (ISSN: 1089-7798, IF: 1.463, DOI: 10.1109/LCOMM.2014.2344031, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6868233).

Радови публиковани у домаћим часописима (M53):

[1.2] O. Al Rasheed, D. Radović and P. Ivaniš, "Performance analysis of iterative decoding algorithms for PEG LDPC codes in Nakagami fading channels," *Telfor Journal*, vol. 5, no. 2, 2013, pp. 97-102. (ISSN: 1821-3251 - Print Issue, ISSN: 2334-9905 - Online).

[1.3] O. Al Rasheed, S. Brkic, P. Ivanis and B. Vasic, "Performance Analysis of Faulty Gallager-B Decoding of QC-LDPC Codes with Applications," *Telfor Journal*, vol. 6, no. 1, 2014, pp. 7-11. (ISSN: 1821-3251 - Print Issue, ISSN: 2334-9905 - Online).

Радови саопштени на међународним научним скуповима (M33):

[1.4] O. Al Rasheed, D. Radovic, P. Ivanis, "Performances of Progressive Edge-Growth LDPC codes in Nakagami fading channel," in *Proceedings of 20st Telecommunication Forum (TELFOR 2012)*, November 2012, Belgrade, Serbia, pp. 560-563.

[1.5] O. Al Rasheed, S. Brkic, P. Ivanis and B. Vasic, "Performance analysis of faulty Gallager B decoding of QC-LDPC Codes," in *Proceedings of 21st Telecommunication Forum (TELFOR 2013)*, November 2013, Belgrade, Serbia, pp. 323-326.

[1.6] O. Al Rasheed and P. Ivanis, "Analiza bit fliping dekodera LDPC kodova realizovanih pomoću nepouzdanih komponenti," *INFOTEH-JAHORINA*, vol. 13, March 2014, pp. 403-407, M33.

[1.7] O. Al Rasheed, D. Drajić, P. Ivanis and G. Đorđević, "Complexity of the McEliece Cryptosystem based on GDBF Decoder for QC-LDPC Codes," in *Proceedings International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST 2014)*, vol. 2, June 2014, Niš, Serbia, pp. 321-324.

[1.8] P. Ivanis, O. Al Rasheed and B. Vasic, "MUDRI: A fault-tolerant decoding algorithm," in *Proceedings IEEE International Conference on Communications (ICC)*, London, June 2015. (paper accepted).

1.2.2. Извештај са јавне усмене одбране предложене теме докторске дисертације

Јавна усмена одбрана предложене теме докторске дисертације одржана је 4.5.2015. године на Електротехничком факултету Универзитета у Београду, пред комисијом у саставу:

- др Зоран Чича, доцент Електротехничког факултета Универзитета у Београду
- др Горан Т. Ђорђевић, ванредни професор Електронског факултета Универзитета у Нишу
- др Марија Рашајски, ванредни професор Електротехничког факултета Универзитета у Београду

Усмена одбрана је почела у 13:00 часова, а завршена је у 14:00 часова.

На усменој одбрани су били присутни сви чланови Комисије.

Одбрану је отворио председник Комисије доц. др Зоран Чича 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 30 минута изложио у најсажетијем облику област и предмет истраживања, актуелност истраживања, постојећа решења са критичким осврtом, као и своје предлоге за унапређење једне класе алгоритама за декодовање кодова мале густине провера парности, са могућим применама у криптосистемима са јавним и тајним кључевима.

Кандидат је успешно одговорио на сва питања која су му чланови Комисије поставили.

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

Комисија је закључила да је кандидат Omran Al Rasheed на јавној усменој одбрани предложене теме докторске дисертације добио оцену „задовољио". Комисија предлаже да ментор докторске дисертације буде др Предраг Иваниш, ванредни професор Електротехничког факултета Универзитета у Београду.

1.3. Оцена подобности кандидата за рад на предложеној теми

На основу претходног приказа резултата досадашњег рада и оствареног искуства кандидата Omran Al Rasheed, Комисија је стекла увид у способност кандидата за научно-истраживачки рад, као и његове могућности, да током израде предложене докторске дисертације, оствари резултате који могу бити верификовани од стране како домаће тако и међународне научне заједнице.

2. Предмет и циљ истраживања

Предмет истраживања предложене теме ове докторске дисертације су криптосистеми са јавним и тајним кључевима (асиметрични криптосистеми) засновани на примени заштитних кодова. У теми ће посебно бити размотрена варијанта криптосистема заснована на *МцЕлиесе* алгоритму, код кога се на предајној страни за криптовање података користи јавни кључ при чему се поступак криптовања заснива на примени заштитног блок кода, линеарне трансформације и намерног уношења унапред одређеног броја грешака на случајне позиције кодне речи. На страни пријема примењује се декодер за кога је познато да са сигурношћу исправља тип грешака који је унет на предајној страни.

Циљ истраживања је модификација *McEliece* криптосистема тако да се постигне побољшана сигурност алгоритма уз поједностављену имплементацију. Планирано је да се ово постигне коришћењем алгоритама декодовања мале комплексности који би обезбедили велики проток корисничких података без погоршања сигурности криптосистема, а који ће бити развијени

као оригинални допринос дисертације. Познато је да се у случају примене кодова са малом густином провере парности може реализовати итеративни поступак декодовања чија комплексност расте линеарно са порастом дужине кодне речи, што ову класу кодова чини посебно атрактивном за примену у асиметричним криптосистемима. Ипак, постоји више итеративних алгоритама декодовања који се могу применити на исти LDPC код и они немају исте перформансе нити имају исти ниво комплексности.

Сигурност криптосистема директно је одређена немогућношћу препознавања фамилије кодова из пресретнуте секвенце (обезбеђује се линеарном трансформацијом) и перформансама примењеног декодера. Уколико декодер има већу могућност корекције грешака, моћи ће да буде унето више грешака при формирању криптограма а да оне при декриптовању буду уклоњене, тако да се послата информација потпуно реконструише на страни пријема. Са друге стране, велика комплексност декодера захтева обављање великог броја операција у јединици времена, што директно утиче на смањење корисничког протока.

Како мали кориснички проток представља основнуману асиметричних криптосистема у односу на симетричне (који користе тајни кључ, исти на предајној и на пријемној страни), јасно је да је велика комплексност декодера веома непожељна.

Стога циљ истраживања представља развој нове класе алгоритама за декодовање LDPC кодова који треба да имају значајно мању комплексност од алгоритама са меким декодовањем, као што је алгоритам са сумирањима и производима, који у телекомуникационим применама представља стандардно решење. Са друге стране, развијени алгоритми треба да имају боље перформансе од бит-флипинг (*Bit Flipping, BF*) алгоритма који у телекомуникационим применама обезбеђује протоке реда Tb/s али су његове способности у погледу корекције грешака врло скромне.

Предложена тема докторске дисертације припада актуелној и значајној области телекомуникација и теорије информација. Последњих година, ова проблематика добија нови замах услед све већих захтева за сигурним преносом велике количине података у реалном времену. Очекивани развој квантних рачунара у скорој будућности доводи у питање сигурност стандардних асиметричних криптосистема као што је RSA (*Rivest-Shamir-Adleman*). У таквој ситуацији, асиметрични криптосистеми засновани на примени заштитних кодова добијају на значају јер за њих још увек није смишљен ефикасан метод криптоанализе, како на класичним тако ни на квантним рачунарима.

Пројектовање асиметричних криптосистема базираних на заштитним кодовима је актуелна област коју покрива већи број часописа из теорије информација и примењене математике. Поред тога, стално се појављују нове књиге које покривају баш ову специфичну област криптографије. У једној од њих, објављеној ове године (G. Gilbert, Y. S. Weinstein, M. Hamrick, *Quantum Cryptography*, World Scientific, 2015) посебно је описана рањивост класичних асиметричних криптосистема у будућности, док је у другој (M. Baldi, *QC-LDPC Code-Based Cryptography*, Springer Briefs in Electrical and Computer Engineering, Springer 2014) детаљно размотрена могућност примене квазицикличних (*Quasy Cyclic, QC*) LDPC кодова у асиметричним криптосистемима.

Релевантни библиографски извори и остварени резултати на које се надовезују предвиђена истраживања у предложеној дисертацији укључују следеће:

[2.1] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," *Deep Space Network Progress Report Progress Report*, 44:114–116, January 1978.

[2.2] C. Monico, J. Rosenthal, and A. Shokrollahi. "Using low density parity check codes in the McEliece cryptosystem," in *Proc. IEEE International Symposium on Information Theory (ISIT 2000)*, page 215, Sorrento, Italy, June 2000.

[2.3] M. Baldi and F. Chiaraluce, "Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes," in *Proc. IEEE International Symposium on Information Theory (ISIT 2007)*, Nice, France, June 2007, pp. 2591–2595.

[2.4] R. M. Tanner, D. Sridhara, A. Sridharan, T. E. Fuja, and D. J. Costello, "LDPC block and convolutional codes based on circulant matrices," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 2966–2984, December 2004.
[2.5] T. J. Richardson, "Error floors of LDPC codes," in *Proc. 41st Annual Allerton Conference on Communications, Control and Computing*, Monticello, USA, September 2003, pp. 1426–1435.
[2.6] M. Ivkovic, S. Chilappagari, and B. Vasic, "Trapping sets in low-density parity-check codes by using Tanner graph covers," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3763–3768, August 2008.
[2.7] R. Misoczki, JP. Tillich, N. Sendrier and P. Barreto, "MDPC-McEliece: New McEliece variants from moderate density parity-check codes," in *Proc. IEEE International Symposium on Information Theory (ISIT 2013)*, Istanbul, Turkey, July 2013, pp. 2069–2073.
[2.8] M. Baldi, M. Bianchi, F. Chiaraluce, "Security and complexity of the McEliece cryptosystem based on quasi-cyclic low-density parity-check codes," *IET Information Security*, vol. 7, no. 3, pp. 212-220, September 2013.

У раду [2.1] описана је основна идеја асиметричног криптосистема базираног на алгебарској теорији заштитних кодова. У овом раду се сматра да се користе *Goppa* кодови чија је способност исправљања грешака доминантно одређена њиховим минималним Хеминговим растојањем. Тешкоће при имплементацији овог алгоритма (пре свега услед велике дужине кључа) описане су у раду [2.2], где је предложена примена LDPC кодова како би се превазишли уочени проблеми.

У раду [2.3] закључено је да су QC LDPC кодови посебно погодни за примену у криптосистемима са јавним и тајним кључевима. Ова класа кодова провобитно је предложена и детаљно анализирана у раду [2.4], у коме је објашњено да су ови кодови изузетно погодни за практичну имплементацију због уштеде меморијских ресурса и знатног скраћења дужине јавног кључа. Ипак, у раду [2.5] је показано је да LDPC кодови (за разлику од класичних алгебарских кодова) често не успевају да исправе патерне грешака мале тежине, те може да се деси да при појави свега неколико грешака у кодној речи декодовање не буде успешно изведено. Услед овог ефекта јавља се заравњење криве зависности вероватноће да кодна реч не буде исправно декодована (*Frame Error Rate*, FER) од вероватноће грешке у каналу, тзв. *error floor*. Ова појава је посебно уочљива код структуираних кодова, као што су QC LDPC кодови, и потиче од подграфова специфичне структуре (тзв. трапинг сетови) који доводе до тога да декодер осцилује између неколико погрешних структура графа онемогућавајући га да настави конвергенцију ка кодној речи [2.6]. Услед овог ефекта, не може се гарантовати да ће декодер увек моћи да исправи грешке које се намерно уносе на страни декодера у циљу повећања сигурности комуникације. Ово као директну последицу има смањену сигурност криптосистема јер је број грешака који се сме унети смањен због постојања трапинг сетова.

Овај проблем се може ублажити тиме што се користе кодови са већом густином матрице провере парности [2.7]. Под одређеним условима, на овај начин се могу побољшати перформансе декодера али се подиже комплексност. У раду [2.8] размотрена је примена различитих алгоритама декодовања у асиметричним криптосистемима. Неки од њих омогућавају велике протоке података али обезбеђују релативно скромну сигурност (BF), док други обезбеђују веома добре перформансе али уз велику комплексност и повећану дисипацију енергије у декодеру (SPA).

3. Полазне хипотезе

У овој докторској дисертацији кренуће се од основне претпоставке да се оптимизацијом итеративног декодера LDPC кодова може повећати сигурност асиметричног криптосистема уз истовремено повећање корисничког протока. Побољшање перформанси декодера биће обезбеђено модификацијом постојећих алгоритама са тврдим одлучивањем.

У овом истраживању полази се од следећих претпоставки (хипотеза):

1) *McElliece* криптосистем има мању комплексност реализације и обезбеђује два до три пута веће корисичке протоке од РСА криптосистема, који представља најчешће примењивани асиметрични криптосистем. Замена алгебарских *Gonna* кодова (који су оригинално предложени за примену у *McElliece* криптосистему [2.1]) LDPC кодовима може у великој мери смањити комплексност криптосистема. Ово је директна последица чињенице да се и LDPC кодови са великом дужином кодне речи могу декодовати уз умерену комплексност, применом итеративних поступака декодовања. Ова чињеница је већ уочена у литератури [2.2], [2.3] и представља основу даљег рада.
2) Сигурност *McElliece* криптосистема је већа ако се примени LDPC декодер који има већу способност исправљања грешака. Ова тврдња је директна последица природе LDPC кодова. Док је у случају алгебарских кодова максималан број грешака одређен пре свега начином конструкције кода, у случају LDPC кодова он веома зависи од примењеног алгоритма декодовања [2.8]. Чак и у случају врло ефикасних декодера, не може се гарантовати да ће сви патерни грешака мале тежине моћи са сигурношћу да буду декодовани чак и када код има добре особине (велико минимално Хемингово растојање) [2.4], [2.5]. Зато је циљ да се пројектују декодери који ће добро да раде у *error floor* режиму, односно декодери који имају могућност да елиминишу штетан утицај трапинг сетова.
3) Комплексност декодера зависи од сложености његове реализације и броја операција које треба обавити у јединици времена, а кориснички проток је утолико мањи што су комплексност декодера и кашњење при декодовању већи. Јасно је да декодери који оперишу реалним бројевима имају већу комплексност од декодера који раде са бинарним бројевима. Примера ради, за успешан рад SPA декодера неопходно је да се са великом прецизношћу представе релевантне вероватноће а пожељно је да аритметика буде реализована по принципу пливајућег зареза (*floating point*). Са друге стране, у случају декодера са тврдим одлукама све операције се могу реализовати помоћу бинарних операција (ексклузивно или, већинско одлучивање) што је знатно једноставније за имплементацију. Такође, пожељно је да се избегне пропагирање порука кроз граф (*message passing*) јер оно додатно подиже комплексност имплементације. Како бит-флипинг алгоритам има све жељене особине, он представља добар избор за основни алгоритам од кога се модификацијом може доћи до новог алгоритма са знатно унапређеним перформансама али који ће при томе имати знатно мању комплексност од постојећих решења.
4) У криптосистему ће се користити разне модификације развијеног алгоритма декодовања (понављање са случајном реиницијализацијом, паралелни рад више декодера), зависно од тога да ли је главни захтев високи степен сигурности, мала комплексност или мало максимално кашњење при декодовању. Поред тога, треба идентификовати параметре који утичу на просечно и максимално кашњење услед процеса декодовања. Дакле, циљ је да решење буде такво да се омогући реконфигурабилност у односу на постављене захтеве.
5) Да би се остварила енергетска ефикасност пожељно је да решење буде такво да перформансесистема не буду битно деградиране углед појаве грешака у самом процесу декодовања (нпр. услед смањења нивоа напајања на ниво нижи од оптималног).

4. Научне методе истраживања

У овом истраживању издвојени су следећи општи методи анализе асиметричних криптосистема:

1) Општа теорија анализе криптостистема са јавним и тајним кључевима, заснована на алгебарској теорији кодовања и елементима дискретне математике.
2) Испитивање сигурности криоптосистема на основу перформанси LDPC итеративних декодера чији се рад може описати применом теорије бипартитних графова.
3) Испитивање перформанси декодера рачунарском симулацијом, применом Монте Карло симулационих метода.
4) Испитивање перформанси криптосистема у коме је извршена интеграција декодера са оригинално развијеним алгоритмом и подешавање параметара у циљу постизања унапред постављених захтева.
5) Анализа развијеног криптосистема у циљу испитивања сигурности система на активности малициозних корисника.

У вези са остваривањем предвиђеног истраживања, очекује се развој унапређене варијанте *McElliece* криптосистема заснованог на QC LDPC кодовима, у коме се користи оригинално развијен декодер мале комплексности. При развоју криптосистема треба да се укључе сви релевантни резултати из наведених библиографских извора и унапреде постојећа решења. Посебно треба да се омогући реконфигурабилност у смислу испуњавања захтева у погледу сигурности, протока података и захтева за минималним кашњењем при декодовању.

5. Очекивани научни допринос

Очекивани допринос докторске дисертације је развој унапређене варијанте *McElliece* криптосистема, код које се обезбеђује повећана сигурност и мања комплексност реализације у односу на тренутно постојећа решења.

- Основни допринос представљаће развој новог алгоритма за декодовање LDPC кодова, који ће имати знатно боље перформансе од BF алгоритма и нижу комплексност реализације у односу на SPA алгоритам.
- Као директна последица особина развијеног алгоритма, очекује се да се доступни кориснички проток при примени посматраног криптостистема са јавним и тајним кључевима увећа бар десет пута у односу на тренутно постојећа решења.
- Алгоритам декодовања ће бити дизајниран са циљем да буде отпоран на хардверске грешке у самом декодеру, које могу настати као последица рада са нивоима напајања који су нижи од номиналних.
- Како алгоритам декодовања у значајној мери одређује дисипацију енергије читавог криптосистема, очекује се да примена алгоритма ниске комплексности који је отпоран на хардверске грешке омогући имплементацију енергетски ефикасних декодера.
- Алгоритам декодовања ће бити дизајниран тако да омогући знатно побољшање перформанси у *error floor* режиму рада, очекује се да предложено решење доведе до повећане сигурности криптосистема чак и у случају примене кодова мање дужине.

Предложена модификација *McElliece* криптосистема, као исход овог истраживања, може имати практичну примену за реализацију система преноса у коме би се обезбедила знатно бржа комуникација, уз додатно повећану сигурност преноса података у односу на постојећа решења.

6. План истраживања и структура рада

План истраживања ове докторске дисертације може се поделити у неколико корака:

1) Проучавање основних библиографских извора о криптосистемима са јавним и тајним кључевима,са посебним освртом на особине криптосистема заснованим на примени заштитних кодова.
2) Преглед најновијих истраживања из области примене QC LDPC кодова у асиметричним криптосистемима базираним на *McElliece* алгоритму.
3) Развој новог алгоритма декодовања LDPC кодова који треба да има ниску комплексност али боље перформансе од постојећих алгоритама са тврдим одлучивањем.
4) Оптимизација развијеног алгоритма декодовања тако да се обезбеди отпорност на хардверске грешке и побољшану енергетску ефикасност у односу на постојећа решења.
5) Интеграција развијеног декодера у криптосистем и оптимизација његових параметара тако да се обезбеде постављени захтеви по питању сигурности, протока података и максималног кашњења.
6) Анализа сигурности криптосистема испитивањем рањивости на постојеће методе криптоанализе.
7) Упоредна анализа са решењима која су описана у отвореној доступној литератури.
8) Препознавање и установљавање могућих даљих праваца истраживања.

Структура предложене тезе пратиће наведени план истраживања. Поред уводног прегледа основних теорија асиметричних криптосистема заснованих на заштитним кодовима, централни део рада садржаће приказ итеративних алгоритама декодовања LDPC кодова а посебно опис новог алгоритма који ће бити развијен тако да обезбеди побољшане перформансе у односу на постојеће декодере са тврдим одлучивањем и смањену комплексност у односу на декодере који се стандардно примењују у телекомуникационим системима. Остатак тезе биће посвећен интеграцији развијеног итеративног декодера у криптосистем тако да се испуне постављени захтеви за сигурношћу и повећаним протоком корисничких података,. У обзир ће бити узети и захтеви за енергетском ефикасношћу и смањеној осетљивости криптосистема на хардверске грешке, као и ограничено максимално кашњење при декодовању. Коначно, биће извршена и компаративна анализа добијених резултата и резултата из доступне литературе.

7. Закључак и предлог

На основу претходно изложеног, Комисија сматра да кандидат **Omran Al Rasheed**, дипломирани инжењер електротехнике, испуњава све законске, формалне и суштинске услове као и све критеријуме који се уобичајено примењују приликом оцене подобности кандидата и теме на Електротехничком факултету Универзитета у Београду. Комисија констатује да тема припада научној области **Телекомуникација** за коју је **Електротехнички факултет Универзитета у Београду** матичан, и при томе за ментора докторске дисертације предлаже **ванредног професора др Предрага Иваниша** запосленог на Електротехничком факултету Универзитета у Београду. У контексту овог предлога, уз извештај је приложен списак радова који квалификују ванредног професора др Предрага Иваниша за ментора.

Комисија има задовољство и част да предложи Наставно-научном већу Електротехничког факултета Универзитета у Београду да одобри израду докторске дисертације кандидату Omran Al Rasheed под насловом **„Алгоритми декодовања мале комплексности погодни за примену у асиметричним криптосистемима".**

Како је кандидат страни држављанин, дисертација ће бити написана и брањена на енглеском језику, под насловом **"Low complexity decoding algorithms suitable for application in asymmetric cryptosystems".**

У Београду, 6.5.2015. године

ЧЛАНОВИ КОМИСИЈЕ

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

др Зоран Чича, доцент
Универзитет у Београду – Електротехнички факултет

др Горан Т. Ђорђевић, ванредни професор
Универзитет у Нишу – Електронски факултет

др Марија Рашајски, ванредни професор
Универзитет у Београду – Електротехнички факултет