Универзитет у Београду
Електротехнички факултет

НАСТАВНО-НАУЧНОМ ВЕЋУ

Предмет: Реферат о урађеној докторској дисертацији кандидата дипл. инж. електротехнике Omran Al Rasheed.

Одлуком Наставно-научног већа Електротехничког факултета у Београду донетој на 792. седници одржаној 27.10.2015. године (број одлуке 5049-11/3 од 3.11.2015. године), именовани смо за чланове Комисије за преглед, оцену и одбрану докторске дисертације кандидата Omran Al Rasheed под насловом

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

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

После прегледа достављене Дисертације и других пратећих материјала, као 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 је тему под насловом „Алгоритми декодовања мале комплексности погодни за примену у асиметричним криптосистемима" („Low complexity decoding algorithms suitable for application in asymmetric cryptosystems") пријавио 25.03.2015. године. Наставно-научно веће Електротехничког факултета Универзитета у Београду је на 785. седници одржаној 29.04.2015. године именовало Комисију за оцену услова и прихватање теме докторске дисертације у саставу: 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).

Извештај комисије за оцену услова и прихватање теме докторске дисертације је усвојен на 787. седници Наставно-научног већа Електротехничког факултета одржаној 23.06.2015. године. Веће научних области техничких наука дало је сагласност на предложену тему докторске дисертације на седници одржаној 06.07.2015. године (број одлуке 61206-3023/2-15).

Кандидат је урађену дисертацију поднео на преглед и оцену 07.10.2015. године, а Наставно-научно веће Електротехничког факултета је на 792. седници одржаној 27. 10.2015. године (број одлуке 5049-11/3 од 3.11.2015. године) именовало Комисију за преглед и оцену докторске дисертације у саставу: 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 Александра Смиљанић, редовни професор (Универзитет у Београду – Електротехнички факултет) и др Марија Рашајски, ванредни професор (Универзитет у Београду – Електротехнички факултет).

1.2. Научна област дисертације

Дисертација припада научној области Техничких наука - електротехнике, а у ужем смислу научној области Телекомуникације. За ове области матичан је Електротехнички факултет. Ментор дисертације је др Предраг Н. Иваниш, ванредни професор на Електротехничком факултету Универзитета у Београду због значајних научних доприноса у области теме докторске дисертације, посебно у области теорије информација.

1.3. Биографски подаци о кандидату

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 др Rami Alkhatib. Тренутно је студент докторских студија на Електротехничком факултету Универзитета у Београду, на модулу Телекомуникације.

Omran Al Rasheed је аутор или коаутор два рада у међународним часописима са импакт фактором, оба у категорији М22. Такође је аутор или коаутор 2 рада у часописима националног значаја, 2 рада у часописима националног значаја и 6 радова на конференцијама међународног значаја.

2. ОПИС ДИСЕРТАЦИЈЕ

2.1. Садржај дисертације

Дисертација је написана на 132 А4 стране куцаног текста и садржи 59 слика, 10 табела и 134 библиографске референце. Дисертација садржи насловну страну, кратак резиме на српском и енглеском језику, садржај, 7 глава и списак коришћене литературе. Наслови поглавља докторске дисертације су:

1. Увод,
2. McEliece криптосистем,
3. LDPC кодови и алгоритми за итеративно декодовање,
4. Унапређења бит-флипинг алгоритма и декодовање у присуству хардверских грешака,
5. Перформансе и комплексност модификованог McEliece криптосистема,
6. Закључак.

2.2. Кратак приказ појединачних поглавља

У уводној глави дисертације изложени су основни принципи криптосистема заснованих на заштитним кодовима. Описана је разлика између симетричних и асиметричних криптосистема, дат је детаљан преглед криптосистема са јавним и тајним кључевима. Посебно је размотрена сигурност разматраних алгоритама при коришћењу квантних рачунара. Величина приватног кључа је идентификована као значајан проблем у случају примене криптосистема базираних на примени заштитних кодова. На крају уводног поглавља дат је преглед структуре и допринос рада.

Друга глава представља детаљан преглед McEliece криптосистема базираних на заштитним кодовима. У њој је детаљно описан оригинални McEliece криптосистем са *Goppa* кодовима и наведене су његове предности у односу на конкурентске алгоритме. Затим је дат свеобухватан приказ модификација McEliece криптосистема које су до сада описане у литератури. Посебна пажња је посвећена претходно предложеним модификацијама заснованим на кодовима са проверама парности мале густине (*Low Density Parity Check, LDPC*), које су омогућиле ефикаснију имплементацију и значајно смањење комплексности. Затим су размотрена решења заснована на кодовима са проверама парности умерене густине (*Moderate Density Parity Check, MDPC*) који обезбеђују већи ниво сигурности. Показано је да квазициклични кодови имају велике предности у односу на друге фамилије кодова, јер омогућавају значајно смањење кључа у криптосистему. Стога су у овој глави детаљно размотрени и поступци за ефикасну имплементацију разматраних алгоритама.

Преглед теорије линеарних блок кодова, кодова са проверама парности мале густине и алгоритама за итеративно декодовање дат је у трећој глави. У овом делу рада дате су неопходне дефиниције и описан начин представе LDPC кодова помоћу графа. Укратко су описани поступци конструкције контролне матрице за најзначајније типове LDPC кодова. Затим је описана процедура за ефикасно формирање кодне речи LDPC и MDPC кодова, као и поступак за добијање генеришуће матрице на основу контролне матрице кода. Дат је детаљан преглед алгоритама за итеративно декодовање заснован на размени порука између чворова у бипартитном графу, и то како оних са тврдим тако и оних са меким одлучивањем, пре свега алгоритам са сумирањима и производима (*Sum Product Algorithm, SPA*). Посебан нагласак стављен је на анализу комплексности наведених декодера и идентификована је потреба за декодером који би уз ниску комплексност имплементације (користећи тврдо одлучивање) обезбедио перформансе блиске онима које обезбеђују сложени итеративни алгоритми високе комплексности.

У четвртој глави детаљно је анализиран до сада најједноставнији познати алгоритам за итеративно декодовање LDPC и MDPC кодова, познат под називом бит флипинг (*Bit Flipping, WBF*). Затим су изложене две модификације овог алгоритма које су погодне за примену у каналу са шумом, кад је декодеру познато не само на ком биту се појавила грешка већ и интензитет грешке. Један од ових алгоритама је тежински бит флипинг (*Weighted Bit Flipping, WBF*) код кога се побољшање перформанси постиже увођењем тежинских коефицијената, а други је градијентни бит флипинг (*Gradient Descent Bit Flipping, GDBF*) код кога се у циљу побољшања конвергенције при свакој итерацији у обзир узима иницијална вредност из канала. У овој глави GDBF алгоритам је прилагођен раду у бинарном симетричном каналу, а затим је предложен нови алгоритам код кога је у одлучивање о флиповању унет одређени ниво случајности. Пробабилистички градијентни бит-флипинг алгоритам (*Probabilistic Gradient Descent Bit Flipping, PGDBF*) оригинално подразумева коришћење већег броја генератора случајних бинарних секвенци и кола за максимизацију, али је у наставку описано да се максимизација може ефикасно реализовати у форми узастопних поређења са прагом, а да се имплементација декодера може знатно поједноставити ако се више случајних секвенци изведе из једног генератора случајне секвенце.

У истој глави показано је на који начин PGDBF декодер успева да исправи неке критичне структуре грешака из канала и дати су нумерички резултати који показују супериорност предложеног приступа у односу на претходно описан декодере са тврдим одлучивањем. Показано је да се додатно побољшање перформанси може остварити помоћу вишеструких покушаја декодовања уз случајну реиницијализацију (*Multiple Decoding attempts and Random re-Initializations,* MUDRI), што је посебно значајно ако декодовање може да се обави у великом броју итерација. Показано је да је предложени декодер веома робустан у случају када постоје хардверске грешке у логичким колима помоћу којих је декодер реализован, што отвара могућност имплементације алгоритма у енергетски ефикасном декодеру који је реализован помоћу компоненти које раде са малим напајањима (*subthreshold* режим рада). На крају овог дела рада, описана је једна могућа процедура за ефикасну имплементацију алгоритма на FPGA платформи, помоћу које се значајно штеде хардверски ресурси без битне деградације перформанси.

У петој глави анализирана је примена развијених декодера у McEliece криптосистему. Процењене су перформансе више LDPC/MDPC кодова за случај када је примењен стандардни *SPA* алгоритам декодовања, као и за случај када су примењени итеративни декодери са тврдим одлучивањем који су развијени и описани у овој дисертацији. Предложено је неколико конфигурација декодера којим се остварује компромис између кашњења при декодовању и перформанси декодера (велике поузданости декодовања која обезбеђује високи ниво сигурности криптосистема). Детаљно је анализирана комплексност предложених декодера. Коначно, анализирана је отпорност предложеног криптосистема на врсте напада који се најчешће користе при криптоанализи McEliece криптосистема.

У шестој глави дисертације изложени су најзначајнији закључци.

3. ОЦЕНА ДИСЕРТАЦИЈЕ

3.1. Савременост и оригиналност

Докторска дисертација припада тренутно актуелној области криптографије. У ужем смислу, дисертација се бави криптосистемима са јавним и тајним кључевима (асиметрични криптосистемима) заснованим на примени заштитних кодова. 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.

Предмет анализе у дисертацији је модификација McEliece криптосистема тако да се постигне побољшана сигурност алгоритма уз поједностављену имплементацију. У тези је показано да се ово може постићи коришћењем алгоритама декодовања мале комплексности који имају потенцијал да обезбеде велики проток корисничких података без погоршања сигурности криптосистема. Ови алгоритми декодовања су развијени као оригинални допринос дисертације. Познато је да се у случају примене кодова са малом густином провере парности (*Low Density Parity Check*, LDPC) 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. Сигурност криптосистема директно је одређена немогућношћу препознавања фамилије кодова из пресретнуте секвенце и перформансама примењеног декодера. Уколико декодер има већу могућност корекције грешака, могуће је унети 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.

Докторска дисертација је за циљ имала развој нових алгоритама за декодовање LDPC кодова који треба да имају значајно мању комплексност од алгоритама са меким декодовањем, као што је SPA алгоритам, који у телекомуникационим применама представља стандардно решење. Са друге стране, показано је да развијени алгоритми имају боље перформансе од бит-флипинг алгоритма који у телекомуникационим применама обезбеђује протоке реда Tb/s али су његове способности у погледу корекције грешака врло скромне. Предложено решење притом има велику флексибилност јер се помоћу њега може обезбедити компромис између сигурности криптосистема и протока доступног крајњем кориснику.

Осим тога, у дисертацији је дата свеобухватна анализа отпорности предложеног криптосистема на стандардне методе који се користе при криптоанализи асиметричних криптосистема. Показано је да развијени алгоритми декодовања представљају кључни елемент за унапређење сигурности криптосистема. Такође, у дисертацији је показано да су ови алгоритми погодни и за примену на енергетски ефикасном хардверу код кога се смањењем напајања логичких кола унутар декодера обезбеђује смањена дисипација енергије у декодеру.

3.2. Осврт на референтну и коришћену литературу

Током израде дисертације кандидат је детаљно истражио постојећу релевантну литературу и коректно навео радове који су у вези са темом дисертације. Наведено је укупно 134 библиографске референце. Литература садржи најновије радове релевантне за проблематику истражену у дисертацији, при чему је Omran Al Rasheed аутор или коаутор 9 радова.

3.3. Опис и адекватност примењених научних метода

Методологија истраживања у оквиру докторске дисертације састојала се у следећем:

- Детаљно је анализирана постојећа литература у области асиметричних криптосистема. Посебна пажња је посвећена анализи криптосистема са јавним и тајним кључевима заснованим на примени заштитних кодова.
- Применом опште теорије анализе асиметричних криптосистема, извршена је детаљна анализа McEliece криптосистема. Показано је да овај криптосистем има мању комплексност реализације и обезбеђује два до три пута веће корисничке протоке од RSA криптосистема, који представља најчешће примењивани асиметрични криптосистем. Полазећи од претпоставке да замена алгебарских *Goppa* кодова LDPC кодовима може у великој мери смањити величину тајног кључа, размотрена је примена ове класе кодова у McEliece криптосистему.
- На основу алгебарске теорије кодовања показано је да LDPC кодови са великом дужином кодне речи могу декодовати уз умерену комплексност, ово решење има потенцијал да буде основа криптосистема мале комплексности. Стога је извршена детаљна анализа итеративних алгоритама декодовања, посебно оних са тврдим декодовањем за које је комплексност посебно мала због чињенице да се они могу реализовати помоћу елементарних логичких кола.

- Теорија графова примењена је да би се открио разлог због кога итеративни декодери не постижу перформансе које би се могле постићи применом декодовања са максималном веродостојношћу (*Maximum Likelihood, ML*). Показано је да основни разлог због кога ови алгоритми имају лоше перформансе представља присуство специфичних структура у бипартитном графу којим се описује код, познатих под називом *trapping set*.
- Користећи основне постулате теорије вероватноће и имајући у виду закључке о присуству подграфова који спречавају конвергенцију бит-флипинг алгоритма, развијене су његове модификације које обезбеђују знатно успешније декодовање LDPC/MDPC кодова. Показано је да ови алгоритми поседују особину реконфигурабилности, јер обезбеђују добар компромис између перформанси, комплексности и времена потребног за декодовање.
- Развијен је независни Монте-Карло симулациони модел помоћу кога су добијени нумерички резултати за разне LDPC/MDPC кодове и разне алгоритме декодовања. Симулациона анализа извршена је у програмским пакетима *Visual Studio* и *Matlab*.
- McEliece криптосистем који за основу има LDPC/MDPC кодове и нови алгоритам декодовања тестиран је на уобичајене нападе, који се обично користе при криптоанализи.

Примењена методологија у потпуности одговара стандардима научно-истраживачког рада и у сагласности је са циљевима дефинисаним на почетку израде дисертације.

3.4. Применљивост остварених резултата

У докторској дисертацији развијени су нови алгоритми за итеративно декодовање LDPC/MDPC кодова, који имају знатно боље перформансе од постојећих алгоритама са тврдим одлучивањем. Предложени алгоритми се могу применити у било ком телекомуникационом систему у ком је потребно додатно повећање поузданости комуникације уз ниску комплексност реализације.

Детаљно је размотрена могућа примена развијених алгоритама декодовања у McEliece криптосистему. Показано је да је погодним избором параметара могуће обезбедити повећање сигурности криптосистема за малу комплексност, али по цену смањеног корисничког протока. Исти ниво сигурности се може постићи и без смањења протока, али по цену повећања комплексности декодера (која је притом још увек мања него у случају SPA декодера). Поред примене у криптосистемима, развијени алгоритми се могу искористити и за повећање стабилности записа у меморијама код којих се користе заштитни кодови. Развијени алгоритми су посебно погодни за примену у случају када је напајање компоненти у декодеру редуковано у циљу повећања енергетске ефикасности.

3.5. Оцена достигнутих способности кандидата за самостални научни рад

Кандидат је приликом израде дисертације показао систематичност, способност за препознавање отворених питања у научној литератури и зрелост при анализи и решавању проблема. Посебно треба истаћи да је област асиметричних криптосистема заснованих на примени заштитних кодова веома актуелна. Неки од добијених резултата представљају решење отворених проблема који су постојали у литератури или њихово унапређење, као и анализу проблема на које до сада није постојао осврт у доступној литератури. Доприноси дисертације у овој области су оригинални, савремени и потврђују способност кандидата за самосталан истраживачки рад.

4. ОСТВАРЕНИ НАУЧНИ ДОПРИНОС

4.1. Приказ остварених научних доприноса

Научни допринос докторске дисертације огледа се у развоју оригиналног алгоритма за итеративно декодовање LDPC/MDPC кодова, чиме се омогућен развој криптосистема који има велику реконфигурабилност.

Конкретно научни доприноси остварени у дисертацији су следећи:

- Основни допринос представља развој нових алгоритама за декодовање LDPC кодова, који имају знатно боље перформансе од BF алгоритма и нижу комплексност реализације у односу на SPA алгоритам.
- Алгоритми декодовања су дизајнирани са циљем да буду отпорни 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, примена алгоритма ниске комплексности који је отпоран на хардверске грешке омогућава имплементацију енергетски ефикасних декодера.
- Показано је да је алгоритам у стању да исправи типове грешака који су неотклоњиви у постојећим декодерима са тврдим одлучивањем. Алгоритам декодовања дизајниран је тако да омогући знатно побољшање перформанси у *error floor* режиму рада, чак и у случају примене кодова мале дужине.
- Развијени алгоритам за декодовање директно омогућава развој унапређене варијанте McEliece криптосистема, код које се обезбеђује повећана сигурност и мања комплексност реализације у односу на тренутно постојећа решења.
- Предложена модификација McEliece криптосистема 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. Као директна последица особина развијеног алгоритма, доступни кориснички проток при примени посматраног криптосистема са јавним и тајним кључевима увећан је приближно бар десет пута у односу на тренутно постојећа решења. Алтернативно, у случају када није приоритет да се кориснику обезбеди велики проток, решење омогућава велику сигурност комуникације уз изузетно малу комплексност криптосистема.

4.2. Критичка анализа резултата истраживања

Увидом у циљеве истраживања, полазне претпоставке и остварене резултате констатујемо да је кандидат успешно одговорио на сва значајна питања из проблематике која је анализирана у дисертацији. Оригинално је развијен алгоритам за итеративно декодовање LDPC/MDPC кодова, којим се обезбеђује повећана сигурност асиметричних криптосистема уз умерену комплексност реализације. Анализом резултата приказаних у дисертацији констатујемо да су приказани оригинални и савремени резултати.

4.3. Верификација научних доприноса

У току истраживачког рада у области теме докторске дисертације Omran Al Rasheed је као аутор или коаутор објавио два рада у међународним часописима са SCI листе (оба категорије M22), при чему је кандидат првопотписани аутор на једном раду. Поред тога, два рада су публикована у часописима националног значаја и шест радова је презентовано на конференцијама међународног значаја .

Радови публиковани у страном часопису (М22):

[1] O. Al Rasheed, P. Ivanis, and B. Vasic, "Fault-Tolerant Probabilistic Gradient-Descent Bit Flipping Decoder," *IEEE Communications Letters*, vol. 18, iss. 9, pp. 1487–1490, September 2014 (ISSN: 1089-7798, IF=1.268, DOI: 10.1109/LCOMM.2014.2344031, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6868233).

[2] S. Brkic, O. Al Rasheed, P. Ivanis, B. Vasic, "On Fault-Tolerance of the Gallager B Decoder under Data-Dependent Gate Failures," *IEEE Communications Letters*, vol. 19, iss. 8, pp. 1299–1302, Avgust 2015 (ISSN: 1089-7798, IF=1.268, DOI: 10.1109/LCOMM.2015.2442981, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7120101).

Радови публиковани у домаћем часопису (М53):

[3] 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).

[4] 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 штампани у целини (М33):

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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).

[10] O. Al Rasheed, P. Ivaniš, "Complexity and Performance of QC-MDPC Code-Based McEliece Cryptosystems", in *Proc IEEE TELSIKS 2015*, Nis, Serbia, October 14^{th}-17^{th}, 2015, pp. 209-216.

5. ЗАКЉУЧАК И ПРЕДЛОГ

На основу чињеница изложених у овом реферату, Комисија је закључила да је докторска дисертација кандидата Omran Al Rasheed под називом **„Алгоритми декодовања мале комплексности погодни за примену у асиметричним криптосистемима" („Low complexity decoding algorithms suitable for application in asymmetric cryptosystems")** у целини написана у складу са образложењем наведеним у пријави теме и садржи све елементе који се захтевају Правилником о докторским студијама Електротехничког факултета Универзитета у Београду.

У дисертацији је детаљно приказан оригинални приступ унапређења једне класе асиметричних криптосистема базираних на заштитним кодовима. Предложено је коришћење LDPC кодова, за које постоји развијено више итеративних поступака декодовања чија комплексност расте линеарно са порастом дужине кодне речи. У дисертацији је развијен нови алгоритам за декодовање заснован на тврдим одлукама којим се обезбеђује додатно побољшање перформанси за ниску комплексност реализације. Показано је да се применом овог алгоритма може повећати сигурност криптосистема уз велике протоке доступне крајњем кориснику. Резултате проистекле из истраживања спроведеном у оквиру докторске дисертације кандидат је објавио у водећим међународним часописима са SCI листе и часописима националног значаја, као и презентовао стручној јавности на конференцијама међународног значаја.

На основу увида у докторску дисертацију и објављене радове кандидата, Комисија констатује да дисертација **„Алгоритми декодовања мале комплексности погодни за примену у асиметричним криптосистемима" („Low complexity decoding algorithms suitable for application in asymmetric cryptosystems")** кандидата Omran Al Rasheed садржи оригиналне научне доприносе.

У складу са напред изнетим, Комисија констатује да је Omran Al Rasheed, дипломирани инжењер електротехнике, испунио све услове предвиђене Законом о високом образовању, Статутом и Правилником о докторским студијама Електротехничког факултета Универзитета у Београду. Комисија предлаже Наставно-научном већу Електротехничког факултета у Београду да се овај реферат прихвати, и у складу са законском процедуром упути Већу научних области техничких наука Универзитета у Београду на коначно усвајање и давање одобрења кандидату да приступи усменој одбрани.

У Београду, 01.02.2014. године

ЧЛАНОВИ КОМИСИЈЕ

др Предраг Н. 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 Александра Смиљанић, редовни професор
Универзитет у Београду – Електротехнички факултет

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