

**НАСТАВНО-НАУЧНОМ ВЕЋУ
ФАКУЛТЕТА ТЕХНИЧКИХ НАУКА
У КОСОВСКОЈ МИТРОВИЦИ**

На седници од 28.01.2008. године, Наставно-научно веће Факултета техничких наука у Косовској Митровици, именovalo нас је у Комисију за писање извештаја за оцену и одбрану урађене докторске дисертације кандидата мр Милоша Банђура, дипломираног инжењера електротехнике. Проучили смо поднети рад под насловом: "**Прилог шифарском кодовању дигитализованих порука**", на основу чега Наставно-научном већу подносимо следећи

ИЗВЕШТАЈ

А. Биографски подаци о кандидату

Милош Банђур рођен је 16.09.1966. године у Приштини. Основну школу завршио је у Косову Пољу са одличним успехом. Прва два разреда средњег усмереног образовања похађао је у Косову Пољу, а трећи и четврти у ОВЦТЗ "Миладин Поповић" у Приштини, које је завршио као ђак генерације.

Електротехнички факултет у Приштини, одсек Електроника и телекомуникације, уписао је 1985. године, а завршио у пролеће 1993. године, са просечном оценом 9,43 (девет, четрдесет три).

Школске 1993/94. године уписао је последипломске студије на Електротехничком факултету у Београду, на смеру Дигитални пренос информација. Све испите положио је оценом 10 (десет). Магистарску тезу под насловом "Компаративна анализа метода прве и друге генерације за кодовање слика", на Електротехничком факултету у Београду, одбранио је 30.05.2001. године.

Од 01.04.1994. године ради на Електротехничком факултету у Приштини, као асистент-приправник на Катедри за телекомуникације и информатику. У континуитету је изводио нумеричке вежбе из предмета "Дигиталне телекомуникације" и "Телекомуникациона техника", а повремено и из других предмета са исте катедре.

У звању асистента на ЕТФ-у Универзитета у Приштини у Косовској Митровици, касније на Факултету техничких наука, Одсеку за електротехнику, Катедри за електронику, аутоматику, телекомуникације и информатику, налази се од 15. октобра 2001. године.

Мр Милош Банђур има 4 (четри) рада објављена у међународним часописима, 2 (два) рада на међународним конференцијама и 3 (три) рада на домаћим конференцијама. До сада је учествовао на 2 (два) научна пројекта које је финансирало Министарство за науку Р. Србије.

Б. Анализа рада

Предмет докторске дисертације кандидата је синтеза новог шифарског система који припада симетричним шифарским системима, односно системима са тајним кључем.

Постоје савршене шифре које су савршено отпорне према покушајима неовлашћеног коришћења шифрованих података и које припадају различитим класама савршености. Обзиром да дужина кључа (кључевног низа) код ове и оваквих шифара зависи од дужине отвореног текста и теоријски може бити бесконачна и обзиром да је избор кључа из скупа свих могућих кључева (кључевних низова) случајан, оне захтевају чување велике количине података везане за кључ и користе се само у ситуацијама када је количина података мала, а њихова важност т.ј. тајност неприкосновена.

У свим осталим случајевима, користе се шифре које нису савршене у теоријском смислу и које поседују различит степен практичне отпорности према криптонападима. Не постоји једна шифра која је одговарајућа за све намене. Избор метода шифровања (то јест криптографског алгоритма и режима његовог коришћења), зависи од карактеристика преношене информације (њене вредности, обима, начина представљања, потребне брзине преноса и т.д.), као и могућности власника да заштити своју информацију (вредност примењене техничке апаратуре, погодност коришћења, поузаност функционисања и т.д.). Постоји више видова информације коју треба заштитити: текстовна, телефонска, телевизијска, компјутерска и т.д., при чему сваки вид има своје особености које треба узети у обзир приликом избора метода шифровања. Велики значај има обим и потребна брзина преноса информације, као и заштићеност канала везе у односу на сметње. Све ово суштински утиче на избор криптографског алгоритма и организацију заштићене везе.

У принципу, безбедност података заснива се на тајности (непознавању) кључа дешифровања. Међутим, допунска резерва безбедности додатно се увећава држањем у тајности криптографског алгоритма (што се у неким областима примене и чини). Обзиром да је вероватноћа упознавања са неким криптографским алгоритмом растућа функција времена његове експлоатације, логична је стална потреба генерисања нових криптографских алгоритама и њиховог усавршавања у циљу повећања информационе безбедности. Чињеница да једном шифровано саопштење може бити поново шифровано неком другом шифром у циљу повећања поузданости шифровања, свакој новој шифри, тачније новом шифарском алгоритму, отвара огромне могућности за примену у смислу модификације постојећих или конструкције потпуно нових композиционих шифара.

Напред наведено у потпуности оправдава предмет докторске дисертације кандидата.

Дисертација се састоји из седам поглавља, при чему су прво и седмо поглавље, увод и закључак, респективно.

У другом поглављу, кроз навођење занимљивих детаља из развојног пута криптографије од глинених таблица у Месопотамији, са шифрованом рецептуром за глазуру грнчарских производа, из 20-ог века п.н.е., све до проналаска асиметричних криптосистема и шифровања са јавним кључем, у време опште експанзије рачунарских мрежа, кандидат је на занимљив начин

читаоцу рада укратко описао развојни пут криптографије и приближио њен значај у целокупној историји људске комуникације.

У трећем поглављу извршена је класификација шифара према различитим критеријумима (основама). Најпре су, према типу трансформације који се примењује над отвореним текстом, шифре подељене на шифре замене, транспозиционе и композиционе, а затим је користећи друге основе кандидат разгранао класификацију шифара. Задатак саме класификације као и потреба за озбиљнијим бављењем шифрама захтевају њихово математичко моделовање, тако да је у оквиру истог поглавља, поред формалног модела шифре, кандидат увео математичке моделе основних класа шифара и могуће моделе отворених текстова. Сматрамо да је презентовањем неких веома познатих шифара, које припадају различитим класама, као и описивањем принципа реализације неких сложенијих класа шифарских система кандидат успео да у потпуности заокружи целину трећег поглавља.

Поузданост шифара је предмет четвртог поглавља. Тајност података који су шифровани заснива се на тајности (непознавању) кључа за њихово дешифровање. Овај принцип заснован је на чињеници да пре или касније, процури мање или више детаља о коришћеном шифарском систему. Кандидат је дефинисао различите пасивне криптонападе од стране неовлашћеног корисника (противника) у криптографији са тајним кључем, са циљем да противник дође до отвореног саопштења или информације о кључу. Уведени су и разматрени појмови теоријске и практичне отпорности шифре према нападу на основу једног шифрованог текста. Теоријска отпорност шифре не узима у обзир сложеност поступка сламања шифре и реалне временске губитке већ само да ли у принципу постоји могућност да се из ухваћеног шифрованог текста добије било каква информација о отвореном тексту или кључу. Ако ухваћени шифровани текст не пружа противнику било какву информацију о њему одговарајућем отвореном тексту, са изузетком можда његове дужине, шифра је савршена (по Клоду Шенону). Размотрени су и активни криптонапади од стране противника у смислу имитације или замене саопштења и уведена је мера отпорности шифарског система у односу на њих. Због постојања сметњи у каналу везе могућа су изобличења или губитак појединих преношених знакова, што за различите шифре има различите последице. Кандидат је овде изложио оне особине шифре због којих услед губитка, додавања или замене појединих знакова у преносу, не долази до простирања грешке при дешифровању.

Кандидат, идеалним односом сажетости и свеобухватности, у петом поглављу обрађује савршене шифре. Савршене шифре обезбеђују најбољу заштиту, јер се информација о отвореном тексту коју би криптоаналитичар могао да добије на основу ухваћеног криптограма не разликује од општепознате априорне информације о отвореном тексту. Клод Шенон је окарактерисао шифре које су савршене у односу на напад на основу једног шифрованог текста. После Шенона појам савршене шифре уопштен је и за неке друге криптонападе.

У овом поглављу, осим савршених по К. Шенону обрађују се особине којима располажу: шифре савршене по К. Шенону отпорне на подметање (имитацију или замену) шифрованог саопштења; шифре савршено отпорне на напад на основу неуређеног скупа криптограма добијених истим кључем ($U(L)$ – отпорне шифре); $U(L)$ – отпорне шифре које поседују најбоље параметре отпорности у односу на подметање; шифре савршено отпорне према нападу на основу неуређеног скупа криптограма од којих неки могу бити добијени

шифровањем истог отвореног текста различитим кључевима ($S(L)$ – отпорне шифре); шифре савршено отпорне за уређене скупове отворених и шифрованих текстова ($O(L)$ – отпорне шифре); шифре савршено отпорне у односу на напад на основу познатог отвореног текста ($M(L)$ – отпорне шифре); шифре савршене по кључу.

У шестом поглављу кандидат је изложио и анализирао сопствено решење шифарског система. У циљу једноставнијег поимања предложеног шифарског алгоритма пошао је од најједноставнијег модела шифре у коме су азбуке отвореног и шифрованог саопштења идентичне и где се сваки знак отвореног текста појединачно шифрује. Користећи описани модел шифре изложио је сопствени основни метод шифровања (шифарски алгоритам у најједноставнијем режиму) и анализирао са аспекта отпорности на декриптовање.

Од свих n различитих симбола неке азбуке у произвољном редоследу формира се кодни прстен. Шифрован симбол, тачније његов нумерацијски израз, представља број неуспелих компарација које су избројане бројачем у поступку проналажења симбола на кодном прстену који је идентичан симболу који се шифрује, при чему поређења вршимо редом у смеру казаљке на сату, почев од позиције на кодном прстену на којој је пронађен претходно кодовани симбол.

Кандидат је извео израз за расподелу вероватноћа симбола у тексту шифрованом на напред изложен начин и анализирао основни метод шифровања. Резултат таквог разматрања је закључак да описани основни метод, обзиром да потенцијално сваки симбол азбуке отвореног текста може да преслика у било који симбол азбуке шифрованог текста и обзиром на трансформацију статистичких особина отвореног текста, квалитативно је најближи табличним гама шифрама са добро осмишљеним кључевним низом (гамом).

Унапређени метод шифровања који је у наставку поглавља описан и анализиран, а који се заснива на истој идеји шифровања (основном методу), елиминише слабост основног метода по питању биграма идентичних симбола и унапређује статистичке карактеристике шифрованог текста, што је математички доказано. Метод користи више кодних прстенова, чије је активирање у поступку шифровања детерминисано кључем (кључевним низом) као распоређивачем.

Употребом више кодних прстенова, усложени су трансформација статистичких особина отвореног текста и успостављање зависности између отвореног и шифрованог текста. Расподела вероватноћа симбола у шифрованом тексту постаје сложенија али и уједначенија (равномернија) у односу на ону која се постиже основном методом, употребом само једног кодног прстена.

У раду је математички доказано, да када се стекну услови да се, два симбола која се један за другим кодују на истом кодном прстену, могу сматрати статистички независним (број кодних прстенова повећа до одговарајућег броја и правилно изабере кључевни низ) сви симболи у шифрованом тексту постају једнаковероватни. Познато је да је униформна расподела симбола најнезгоднија за задатак декриптовања.

У раду је изложен метод савршене шифре, заснован на идеји кодовања по кодном прстену и изведен доказ савршености на тај начин генерисане шифре. Савршена шифра која се на овај начин реализује је ендоморфна савршена шифра са минималним бројем кључева.

Заправо, за савршену шифру се каже да је то шифра са неограниченим кључем. Кључ је случајан и дугачак колико и отворени текст, а пошто се отворени текст теоријски може протезати до у бесконачност и кључевни низ мора бити бесконачно (довољно) дуг. За шифровање се користи једна реализација из скупа свих могућих кључевних низова одговарајуће дужине, па је битно да је број различитих чланова (кључева) из којих се реализује кључевни низ минималан, јер је на тај начин и скуп свих могућих реализација кључевних низова минималан. Овим се гломазност кључа и чување велике количине података везане за кључ своде на најмању могућу меру.

На крају, кандидат је извршио уопштавање шифарског модела за предложени алгоритам шифровања.

В. Закључак и предлог

На основу напред изложене детаљне анализе предметне докторске дисертације, Комисија сматра да је предлагањем новог оригиналног шифарског система кандидат дао научни допринос.

Кандидат је изложио основни метод шифровања, заснован на сопственој идеји и анализирао га са аспекта отпорности на дешифровање.

На основу уочених недостатака основног шифарског метода кандидат је синтетизовао унапређени метод шифровања и извршио његову криптоанализу.

Кандидат је синтетизовао и метод савршене шифре који користи елементе предложеног шифарског алгоритама и доказао савршеност на тај начин генерисане шифре. Синтетизована савршена шифра је ендоморфна савршена шифра са минималним бројем кључева, што је посебно значајно, јер је минималан број кључева важан услов практичне реализације савршених шифара.

На крају, извршено је уопштавање шифарског модела за предложени шифарски алгоритам.

Напред наведеним, научни допринос кандидата представља евидентну целину.

Зато Комисија предлаже Наставно-научном већу да, докторску дисертацију под насловом "Прилог шифарском кодовању дигитализованих порука", кандидата мр Милоша Банђура, дипломираног инжењера електротехнике, прихвати и одобри њену усмену одбрану.

Чланови Комисије

Др Мирослав Лутовац, ред. проф.

Др Милорад Мирковић, ред. проф.

Др Ристо Бојовић, ванред. проф.