ОБРАЗЕЦ 

До Универзитет „Гоце Делчев“ – Штип
Фонд за научно - истражувачка работа

Барање за финансирање на научно - истражувачки проект
Application form for financing of research projects

Дата на поднесување	
Проект Бр:	***(Се пополнува од Архивата на Универзитетот)***

Date of submission	
Project No:	***(Filled by the University authority)***

Наслов на проектот	**Развој на безбедни и надежни техники за податочната комуникација**
Клучни зборови	
FRASCATI класификација	**110 - 11000, 11007, 11011**

Proposal Title	**Development of Secure and Reliable Techniques for Data Communication**
Keywords	
FRASCATI classification	**110 - 11000, 11007, 11011**

ПРВ ДЕЛ/PART 1:

Апстракт (максимум 250 зборови)

Современиот човек се дружи на Интернет, слуша радио и гледа филмови од Интернет, чита електронски книги и весници, закажува хотели и авионски летови преку Интернет, електронски плаќа сметки, итн. Притоа, сајбер безбедноста и приватноста на луѓето постојано се загрозени и злонамерниците постојано наоѓаат нови начини на напаѓање, прислушкување, комуникација и координација на своите злонамерни дејствија.
Овој проект таргетира неколку различни аспекти на безбедноста и надежноста при податочната комуникација.
Две активности се поврзани со дигиталната стеганографија, и нивната цел е откривање на нови скриени канали во новите протоколи за трансфер на веб содржини, како HTTP/2 и QUIC, како и користење на нови анти-стеганографски техники кај дигиталните слики, со цел да се спречат терористите истите да ги користат за скриена комуникација. Крајна цел е да се добие модуларна алатка која би ја користеле сервисите за складирање во облак и веб апликациите кои нудат јавен сервис за слики.
Други две активности се поврзани со криптографијата, и притоа се планира развој на оптимални 8x8 S-кутии од мали квазигрупи од ред 4 или 8 или од бинарни квази-циклични кодови, развој на систем за е-гласање со користење на Биткоин технологијата, развој на круптосистем од Хил шифрата со CSPRNG, како и паралелна реазлизација на некои алгоритми поврзани со криптографските мерки кај S-кутиите.
Една активност опфаќа анализа и обработка на податоци од тестирања за компјутерска и мрежна безбедност со примена на алгоритми од Вештачката интелигенција.
Во врска со надежноста, планиран е дизајн на алгоритми за наоѓање на минимални пат и пресек вектори кај повеќе-состојбени транспортни системи.

Abstract (max 250 words)

Modern man hangs out on the Internet, listen to radio and watch movies from the Internet, read electronic books and newspapers, books flights and hotels through the Internet, makes electronic transactions, etc. The cyber security and privacy of people are constantly threatened and adversaries constantly found new means of attacking, eavesdropping, communicating and coordinating their malicious actions.
This project targets several different aspects of security and reliability in data communication.
Two activities are associated with digital steganography, and their goal is discovering of new covert channels in the new web transfer protocols, such as HTTP/2 and QUIC, as well as using new anti-steganographic techniques for digital images in order to prevent terrorists to use them for hidden communication. The ultimate goal is to obtain a modular tool that would use the cloud storage services and web applications that provide a public service for images.
Two other activities are related to cryptography, and include the development of optimal 8x8 S-boxes from small quasigroups of order 4 or 8, or from binary quasi-cyclic codes; development of an E-voting system using Bitcoin technology; development of Hill cipher cryptosystem with CSPRNG, and parallel realisation of some cryptographic algorithms related to cryptographic measures for S-boxes.
One activity involves the analysis and processing of data obtained by testing computer and network security, by using algorithms from artificial intelligence.
Regarding reliability, algorithm design is planned, for finding a minimal path and cut vectors for multi-state networks.

Детален опис на проектот:

Вовед

Дефинитивно Интернетот и компјутерските мрежи се ентитетите што го дефинираат нашето време и нештата што го обликуваат нашиот живот. Сепак TCP/IP складот со протоколи – основата на Интернетот, не е дизајниран со безбедноста во мислите. Тој е резултат на истражувањата и развојот на протоколите извршени врз експерименталната мрежа со комутација на пакети ARPANET во која биле вклучени универзитетите од САД, а претпоставката била дека никој од корисниците нема да преземе злонамерни акции. Денес корисници се луѓето од целиот свет и оваа претпоставка повеќе не важи. Сведоци сме на зголемениот развој и присуство на сајбер криминалот и постојаните упади и напади во компјутерските системи и мрежи.

TCP/IP складот со протоколи има многу безбедносни пропусти кои постојано се откриваат, а во последно време, мрежната стеганографија, или криењето на податоци во самите мрежни протоколи, зазема се поголем замав ([1-3]). Новите протоколи за трансфер на веб содржини, не се сеуште доволно проучени од овој аспект. Исто така, еден од најчестите начини за комуникација меѓу тероритите вклучува криење на пораки во слики кои се поставуваат на јавни сервиси [9], и до сега истражувачите се обидуваат со стеганализа да откријат дали во сликите има или нема скриено порака, што е доста тешка задача. Нашата цел е јавни сервиси за слики ослободени од скриени пораки.

Децентрализираните дигитални криптопари се повеќе стануваат начин на плаќање на Интернет, особено меѓу криминалците. Сведоци сме на нови примени на Биткоин [7] технологијата со низи од блокови (на пример, катастар базиран на низа од блокови), бидејќи во основа таа овозможува делена, доверлива и јавна колекција, која секој може да ја провери, но, никој не може сам да ја контролира. Една од целите е да се добие систем за е-гласање базиран на Биткоин технологијата со низи од блокови.

S-кутиите се главните градежни блокови на современите блок шифри, па постојано се истражуваат нови начини за добивање оптимални S-кутии од различен ред. Ќе се обидеме да добиеме оптимални 8x8 S-кутии на два начина: од мали квазигрупи и од бинарни квази-циклични кодови. За испитување на истите ќе бидат креирани паралелни алгоритми.

Тестирањето на безбедноста на компјутерските системи и мрежите продуцира големо количество на податоци, кои може да бидат анализирани со различни техники на вештачката интелигенција.

Во теоријата на надежност посебно место зазема анализата на надежност на транспортните системи. Проучувањето на надежноста на транспортните системи има голема примена во различни области: од техничките области до биолошките и економските области. Многу комплексни физички, технолошки, социјални, биолошки и економски системи можат да се претстават со форма на транспортни системи, каде што јазлите се објекти на системот, додека линковите ги претставуваат врските помеѓу објектите. Ние ќе ги разледуваме повеќе-состојбените двотерминални транспортни системи. Поточно наша цел ќе биде дизајнирање на нови и подобрување на веќе постоечките алгоритми за наоѓање на минимални пат и пресек вектори кај насочени и ненасочени повеќе - состојбени двотерминални транспортни системи.

Главниот недостаток на постоечките алгоритми за пресметување на минимални пат (или пресек) вектори е што со нив може да се добијат и кандидати за минимални пат (пресек) вектори што не се минимални пат (пресек) вектори. Овие кандидати се елиминираат со заемно споредување. Процедурата за заемно споредување на сите кандидати за минимални пат вектори е релативно скапа, ако се земе предвид дека бројот на кандидатите за минимални пат вектори е многу поголем од бројот на јазли или од бројот на линкови во транспортниот систем. Од овие причини ги анализираме својствата на минималните пат вектори за ниво d и ќе ја покажеме врската помеѓу минималните пат вектори за ниво d и протоци за ниво за d на транспортни системи. Овие врски ги искористивме за да развиеме стратегија за проверување дали некој кандидат за минимален пат вектор за ниво d е минимален пат вектор со временска комплексност O(|E|) (каде |E| е бројот на линкови), кај ненасочени [5] и насочени транспортни системи [6].

[1] S. ZANDER, G. ARMITAGE, P. BRANCH, A survey of covert channels and countermeasures in computer network protocols, *IEEE Communications Surveys and Tutorials*, 9(3), 44-57, (2007)

[2] W. MAZURCZYK, K. SZCZYPIORSKI, J. LUBACZ - The Spy Who Skyped Me - Four New Ways to Smuggle Messages Across the Internet, *IEEE Spectrum*, 40-43, November (2013)

[3] A. MILEVA, B. PANAJOTOV, Covert channels in TCP/IP protocol stack - extended version-. *Central European Journal of Computer Science*, ISSN 1896-1533, 4 (2). 45-66, (2014)

[4] A.Z. TIRKEL, R.G. Van SCHYNDEL, C.F. OSBORNE, A digital watermark, *Proceedings of ICIP 1994*, Austin Convention Center, Austin, Texas, Vol. II, pp. 86 –90 (1994)

[5] M.MIHOVA, N.STOJKOVIKJ, M. JOVANOV, E.STANKOV, Maximal Level Minimal Path Vectors of a Two-terminal Undirected Network, *IEEE Transactions on Reliability*, Vol. 65, Issue 1, ISSN 0018-9529, pp. 282 – 290, (2016) (**IF 2.278**).

[6] M.MIHOVA, N.STOJKOVIKJ, M. JOVANOV, E.STANKOV, On Maximal Level Minimal Path Vectors of a Two-Terminal Network, *Olympiads in Informatics*, Vol. 8, 133–144, 26th International Olympiad in Informatics,Taipei, Taiwan, (2014)

[7] S. NAKAMOTO, Bitcoin:A peer-to-peer electronic cash system. http://bitcoin.org/bitcoin.pdf, (2008)

[8] L. S. HILL, Cryptography in an algebraic alphabet, *American Mathematical Monthly*, vol. 36, no. 6, pp. 306–312, (1929)

[9] G. WEIMANN, How Modern Terrorism Uses the Internet , Special report 116, Unated States Institute of Peace, March (2004)

Предложени истражувања

Планираме да ги извршиме следниве активности во дадените временски рамки.

1. *Утврдување на нови скриени канали во мрежните протоколи*

   Последните години, мрежната стеганографија или криењето на податоци и користењето на скриени канали во мрежните протоколи, зазема се поголем замав. Скриен канал е било кој комуникациски канал, кој може да се искористи за трансфер на информации на начин кој ги нарушува безбедносните политики на даден систем. Скриените канали во мрежните протоколи можат нелегално да се користат за координација на DDoD напади, ширење на злонамерен код (како компјутерскиот црв W32.Morto, кој ги користи DNS записите за комуникација со неговиот C&C сервер), за скриена комуникација меѓу терористи и криминалци, индустриска шпионажа, но и за легални активности, како заобиколување на ограничувањето за користење на Интернет во некои земји (на пример, Infranet), безбедна комуникација за менаџирање со мрежа, заштита на авторски права и сл. Скриените канали во мрежните протоколи најчесто се добиваат со модификација на заглавјата и/или корисниот товар на протоколите (Protocol Data Unit - PDU) или со модификација на структурата на PDU тековите. Трудовите ([1-3]) нудат слика за состојбата со мрежната стеганографија денес.
   Целта на оваа активност е изнаоѓање на нови скриени канали во некои мрежни протоколи. Посебно ќе бидат анализирани новите верзии на протоколите за трансфер на веб содржини, како HTTP/2.0 и QUIC.

2. *Развој на анти-стеганографски техники за дигитални слики*

   Криењето на пораки во дигиталните слики поставени на јавни сервиси на Интернет, познато е дека е еден од најчестите начини за скриена комуникација на терористите и криминалците во светот. Најчесто се користи методата со модификација на најмалку значајните битови (Least Significant Bit - LSB) на сликата, но и некои други техники, како додавање на сигналот на пораката врз сигналот на сликата, и сл. Стеганализата, или откривањето на скриената информација е многу тешка задача и бара напорно истражување.
   Нашата цел не е да се открие дали има скриени информации во дадена слика, туку да се уништи и да се направи неупотреблива скриената порака, во моментот кога сликата се закачува на Интернет. Крајна цел е да се добие модуларна алатка која би ја користеле сервисите за складирање во облак и веб апликациите кои нудат јавен сервис за слики.

3. *Развој на неколку криптографски решенија*

   a. S-кутиите имаат основна улога во безбедноста на модерните блок шифри, бидејќи тие вообичаено се главниот нелинеарен дел во блок шифрата. Оптималните S-кутии ја прават шифрата отпорна на различни видови на напади. Целта е да се добијат оптимални 8x8 S-кутии од мали квазигрупи од ред 4 или 8 или од бинарни квази-циклични кодови. Ќе бидат испитувани диференцијалните и линеарните карактеристики на добиените S-кутии.
   b. Биткоинот [7] започна нова ера на дигиталните валути, при што блоковите од кои е изграден и самиот концепт денес наоѓаат нова примена во различни области (на пример, технологијата со низа блокови се користи за градење на безбедни логови). Целта на оваа активност е да се проучи дали безбеден систем за е-гласање може да се дизајнира со користење на Биткоин технологијата, и да се дефинираат процедурите и протоколот на користење кои би ја гарантирале главната безбедност и функционалните барања на таквиот систем. На крајот на проектот се очекува да се добие прототип.
   c. Денес Хил шифрата се смета како дел од класичната криптографија. Оваа шифра со замена е дефинирана во 1929 година од страна на Lester S. Hill [8], но во последно време е цел на понови трудови кои се обидуваат да најдат решение за нејзините слабости. Целта на оваа активност е анализа на користењето на Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) за генерирање на клучот матрица во Хил шифрата за секој блок од оригиналнатга порака кој треба да се шифрира.

4. *Дизајн на алгоритми за наоѓање на минимални пат и пресек вектори кај повеќе-состојбени транспортни системи*

   Целта е развој на алгоритми за наоѓање на минимални пат вектори во двотерминален повеќе - состојбен транспортен систем кои ќе имаат помала временска сложеност од постоечките алгоритми. Новите алгоритми ќе бидат базирани на теоретските резултати дадени во [5], и ќе се обидеме да ја проширими оваа теорија за да се подобрат алгоритмите за пресметување на минимални пат вектори.
   Исто така ќе бидат имплементирани и програми за алгоритмите, со чија помош ќе се вршат споредување на времињата на извршување на алгоритмите, со што и експериментално ќе бидат потврдени теоретските резултати до кои ќе дојдеме.

5. *Анализа и обработка на податоци од тестирања за компјутерска и мрежна безбедност*

   За оваа активност ќе бидат користени податоци добиени со душкање и скенирање на мрежа, лог-датотеки и сл. Примена на алгоритми од Вештачка интелигенција (машинско учење) за филтрирање, обработка и анализа на податоци за утврдување на генерални тенденции, дистрибуции и отстапки. Препознавање на облици во bigdata со примена на вештачки невронски мрежи, principal component analysis (PCA), алгоритми за податочно кластерирање (k-means и kNN кластерирање).

6. *Паралелна реализација на брзи (butterfly) алгоритми*

   Алгоритми на трансформација (Fourier-related transforms) имаат апликација во многу области, како криптографија, теорија на кодирање, компресија на податоци, податочни комуникации и т.н. За решавање на проблеми сврзани со споменатите области имаме потреба од ефективни алгоритми. Како се зголемува размерот на задачите, тие стануваат се по тешки и со премногу податоци. Некои алгоритми се попогодни за паралелна реализација. Всушност паралелното сметање преставува модел, при кој множество од задачи се процесираат едновремено (еднакви мали програми процесираат различни податоци), дејствувајќи по принципот на разделување на голема задача на мали под задачи кој се решаваат едновремено.

Временска рамка:
Месеци 1–6: Во оваа фаза се предвидени неколку активности:

- анализа на различните техники за криење на податоци во дигитални слики
- наоѓање на скриени канали во HTTP/2.0
- добивање на S-кутии од бинарни квази-циклични кодови
- собирање на безбедносни податоци од лог датотеки и различни скенирања
- развој на алгоритми за наоѓање на минимални пат вектори во двотерминален повеќе - состојбен транспортен систем кои ќе имаат помала временска сложеност од постоечките алгоритми

Месеци 7- 18: Во оваа фаза се предвидени следните активности:

- наоѓање на скриени канали во QUIK
- дизајн и развој на анти-стеганографски техники за дигитални слики
- обид за добивање на S-кутии од мали квазигрупи од ред 4 или 8
- анализа на користењето на CSPRNG во генерирање на клучот матрица за Хил шифрата
- анализа на добиени безбедносни податоци
- имплементирање на алгоритми за споредба на времињата на извршување кај двотерминални повеќе - состојбени транспортни системи

Месеци 19–24: Научно–истражувачките резултати ќе бидат презентирани на поширокатa јавност на неколку начини и тоа преку презентации на меѓународни и домашни конференции, а голем дел од резултатите ќе бидат публикувани како научни трудови во научни списанија.
На крајот на научно–истражувачкиот период ќе следи изработка на Извештај во кој ќе бидат прикажани сите достигнувања за време на истражувачкиот период.

Details of the proposal:

Introduction

Definitely, the Internet and computer networks are entities that define our time and the things that shape our lives. However, TCP/IP protocol stack - the foundation of the Internet, was not designed with security in mind. It is the result of research and development of experimental protocols performed on the packet switched network, ARPANET, involving US universities, and the assumption was that none of the users will take malicious actions. Today users are people all over the world and this assumption is no longer valid. We are witnessing increased development and the presence of cyber crime and repeated intrusions and attacks on computer systems and networks.

TCP/IP protocol stack has many security vulnerabilities that are constantly discovered, and lately, network steganography, or hiding data in network protocols themselves, is increasingly developed ([1-3]). The new web transfer protocols, are not yet sufficiently explored from this aspect. Furthermore, one of the most common means of communication among terrorists involves hiding messages in graphical files that are placed on public services [9], and now researchers are trying to use steganalysis to discover whether the images have hidden messages, which is quite difficult task. Our goal is public image services free from hidden messages.

Decentralized digital cryptocurrencies become a means of paying on the Internet, especially among criminals. We are witnesses of the new application of the Bitcoin [7] blockchain technology (eg. blockchain-based land registry), because, in essence it is a shared, trusted, public ledger that everyone can inspect, but which no single user controls. One of the project goal is obtaining of e-voting system based on a Bitcoin blockchain.

S-boxes are the main building blocks of modern block ciphers, and constantly new ways are explored, for obtaining optimal S-boxes of a different order. We will try to obtain optimal 8x8 S-boxes in two ways: from small quasigroups and from binary quasi-cyclic codes. For their analysis, parallel algorithms will be implemented.

Computer and network security tests produce a lots of data, that can be examined by different techniques from artificial intelligence.

In the theory of reliability an important place takes the analysis of network reliability. The study of the reliability of these systems is interesting for people of different disciplines: from the technological to economical and biological areas. Many complex physical, technological, social, biological and economic systems can be represented in the form of networks, where vertices are the entities of the system and the links represent the relational links among the entities. We will consider two terminal multi – state networks. Specifically, our goal, will be the development of a new algorithm, and improvement of existing algorithms for finding minimal path vectors or minimal cut vectors for directed and undirected multi – state network.

The main disadvantage of the existing algorithms for finding a minimal path (cut) vectors is that with them, candidates for a minimal path (cut) vectors which are not minimal are obtained. These candidates are eliminated by mutual comparison. This procedure is relatively expensive, because the number of minimal path vectors is much greater than the number of nodes and links in the network. For this reason, we analyze some properties of minimal path vectors to level d (d-MPs)that will show the connection between d-MPs and flow functions to level d on a given two-terminal network. This helps to develop a strategy for checking whether some candidate is a d-MP with time complexity $O(|E|)$ (where $|E|$ is a number of links), for directed and undirected network.

[10] S. ZANDER, G. ARMITAGE, P. BRANCH, A survey of covert channels and countermeasures in computer network protocols*, IEEE Communications Surveys and Tutorials*, 9(3), 44-57, (2007)

[11] W. MAZURCZYK, K. SZCZYPIORSKI, J. LUBACZ - The Spy Who Skyped Me - Four New Ways to Smuggle Messages Across the Internet, *IEEE Spectrum*, 40-43, November (2013)

[12] A. MILEVA, B. PANAJOTOV, Covert channels in TCP/IP protocol stack - extended version-. *Central European Journal of Computer Science*, ISSN 1896-1533, 4 (2). 45-66, (2014)

[13] A.Z. TIRKEL, R.G. Van SCHYNDEL, C.F. OSBORNE, A digital watermark, *Proceedings of ICIP 1994*, Austin Convention Center, Austin, Texas, Vol. II, pp. 86 –90 (1994)

[14] M.MIHOVA, N.STOJKOVIKJ, M. JOVANOV, E.STANKOV, Maximal Level Minimal Path Vectors of a Two-terminal Undirected Network, *IEEE Transactions on Reliability*, Vol. 65, Issue 1, ISSN 0018-9529, pp. 282 – 290, (2016) (**IF 2.278**).

[15] M.MIHOVA, N.STOJKOVIKJ, M. JOVANOV, E.STANKOV, On Maximal Level Minimal Path Vectors of a Two-Terminal Network, *Olympiads in Informatics*, Vol. 8, 133–144, 26th International Olympiad in Informatics,Taipei, Taiwan, (2014)

[16] S. NAKAMOTO, Bitcoin:A peer-to-peer electronic cash system. http://bitcoin.org/bitcoin.pdf, (2008)

[17] L. S. HILL, Cryptography in an algebraic alphabet, *American Mathematical Monthly*, vol. 36, no. 6, pp. 306–312, (1929)

[18] G. WEIMANN, How Modern Terrorism Uses the Internet , Special report 116, Unated States Institute of Peace, March (2004)

Research Project

In this project we plan to complete the following research activities within the indicated time frame.

1. *Finding new covert channels in network protocols*

   Last years, network steganography or hiding data and using of covert channels in network protocols, is rapidly expanding. A covert channel is any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy. Network-based covert channels can be used illegally to coordinate distributed denial of service attacks or spreading of malware (e.g., the worm W32.Morto used DNS records to communicate with its command and control server), for secret communication between terrorists and criminals, industrial espionage, but also legally, for circumvention of the limitation in using Internet in some countries (e.g., Infranet), secure network management communication, copyright protection, etc. Covert channels in the network protocols most often use modification of the protocol header and/or payload (Protocol Data Unit - PDU), or modification of the the structure of PDU streams. The papers ([1-3]) offer an image of the state of the art of network steganography.
   The goal of this activity is finding of new covert channels in some network protocols. Esspecially, a new web transfer protocols as HTTP/2.0 and QUIC will be analyzed.

2. *Development of anti-steganographic techniques for digital images*

   Hiding messages in digital images placed on public services on the Internet is a well known way of conveying a secret communication between terrorists and criminals in the world. Commonly, a Least Significant Bit – LSB method [4] is used, but also adding a message bearing signal to the image, etc. Steganalysis, the detection of this hidden information, is an inherently difficult problem and requires a thorough investigation.
   Our goal is not to find if tehre is a hiden information in a given image, but instead to destroy and to make unusable the hidden message, in the moment of the image uploading on the Internet. The final goal is obtaining of a modular tool, which storage cloud services and web applicationswith images public servises are going to use.

3. *Development of several cryptographic solutions*

   a. S-boxes have a fundamental role for the security of modern block ciphers because they are usually the main non-linear part in the block ciphers. Optimal S-boxes can make the cipher resistant against various kinds of attacks. The goal is to obtain an optimal 8x8 S-boxes from small quasigroups of order 4 or 8, or binary quasi-cyclic codes. We will investigate differential and linear characteristics of produced S-boxes.
   b. Bitcoin [7] started a new era of digital currencies, with its building blocks and underlying concepts finding new applications in different areas nowadays (e.g., blockchain technology is used to build secure logs). The goal of this task is to study if a secure e-voting system can be designed resorting to Bitcoin technology, and also to define the procedures and usage protocol that may guarantee the main security and functional requirements of such system. A prototype of the system is expected by the end of the task.
   c. The Hill cipher is nowadays considered one of the examples of classical cryptography. This substitution cipher was defined in 1929 by Lester S. Hill [8], but it has been the subject of some more recent publications, which aim to solve its weaknesses. The goal of this activity is an analysis of the usage of a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) to generate the matrix key of the Hill cipher for every plaintext block submitted to encryption.

4. *Algorithm design for finding minimal path and cut vectors for multi-state networks*

   Our research will be focused on development algorithms for finding minimal path vectors in two terminal network with lower time complexity from existing algorithms. New algorithms will be based on theoretical results given in [5], and expands the theory, to improve the method for computation of d-MP candidates.

Also, programs for the algorithms will be implemented. By using them we will make comparison of execution times of algorithms, therefore theoretical results that we obtained also will be experimentally proved.

5. *Computer and network security tests data acquisition and data processing*

   For this activity, data obtained by network sniffing and scanning, log-files, and etc, will be used. Application of artificial intelligence algorithms (machine learning) for data filtering, processing and analysis in order to recognize general trends, distribution and outliers. Pattern recognition in raw and big data by applying artificial neural networks, principal component analysis (PCA), algorithms for data clustering (k-means and kNN clustering).

6. *Parallel implementation of fast (butterfly) algorithms*

   Transforms algorithms (Fourier-related transforms) have application in many areas such as cryptography, coding theory, data compression, data communications, etc. For solving problems related to the mentioned areas we need efficient algorithms. How the scale of the task increasing becoming more and more difficult to solve, also have increasing of data. Some algorithms are more suitable for parallel implementation. In fact, parallel computing is a model in which a set of tasks are processed simultaneously (equal small programs process different data), acting on the principle different portions of the computation may be executed concurrently by different processors.

Timeframe for conducting the specified research activities:
Months 1–6: In this phase, the following activities will be conducted:

7. analysis of different techniques for data hiding in digital images
8. finding covert channels in HTTP/2.0
9. obtaing of optimal S-boxes from binary quasi-cyclic codes
10. acquisition of security data from log files and different scannings
11. development of algorithms for finding minimal path vectors in two terminal network with lower time complexity from existing algorithms

Months 7–18: In this phase, the following activities will be conducted:

12. finding covert channels in QUIK
13. design and development of anti-steganographic techniques for digital images
14. obtaing of optimal S-boxes from small quasigroups of order 4 or 8
15. analysis of the usage of a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) to generate the matrix key of the Hill cipher
16. analysis of obtained security data
17. implementation of algorithms for execution time comparision in two terminal multi-state networks

Months 19–24: Scientific results will be presented to the public in several ways, through presentations on the international and home conferences, and papers in journals. At the end, we will produse a Report for all our achivments in the research period.

ВТОР ДЕЛ/PART 2:
Истражувачки тим:

Главен истражувач(сите информации за главниот истражувач на не повеќе од две страници):

Име и презиме	**Александра Милева**
Титула	Доктор на информатички науки
Позиција	Вонреден професор
Адреса	"Крсте Мисирков" 10-А, 2000 Штип, Македонија
Тел / Факс:	++389 78 222 460
e-mail	aleksandra.mileva@ugd.edu.mk

Кратка биографија:
Образование:

- Доктор на информатички науки, Институт за информатика, ПМФ, УКИМ, 2010.
- Магистер на информатички науки, Институт за информатика, ПМФ, УКИМ ,2004.
- Дипломиран инженер по информатика, Институт за информатика, ПМФ, УКИМ,1998.

Работно искуство:

- Вонреден професор на Факултет за информатика при УГД, Штип, 2015 -
- Доцент на Факултет за информатика при УГД, Штип, 2010 - 2015
- Асистент на Факултет за информатика при УГД, Штип, 2007-2010
- Помлад асистент и асистент на Рударско-геолошки факултет при УКИМ, Штип, 2001-2007
- Демонстратор на Институт за информатика, ПМФ при УКИМ, Скопје, 1999-2001

Членство во професионални асоцијации: IEEE, ICT-ACT, Македонија
Член на програмски одбор:

- Tenth International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2016, 24-28 July, Nice, France
- Second International Workshop on Information Security, Assurance and Reliability in the Cloud, WISARC 2016, 6-9 December, Shangai, China (Program Co-Chair)
- Ninth International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2015
- International Mathematical Conference on Quasigroups and Loops, LOOPS '15, Ohrid, Macedonia, 2015.
- 7th ICT Innovations conference 2015, 1-4 October, 2015, Ohrid, Macedonia
- 6th ICT Innovations conference 2014, 9-12 September, 2014, Ohrid, Macedonia
- 2nd International Workshop on Behavioural Types (BEAT 2), 23-24 September, 2013, Madrid, Spain

Поле на научен интерес: Криптографија, компјутерска безбедност и безбедност на мрежи, мрежна стеганографија, теорија на квазигрупи

Трудови објавени во последните 5 години, со назначен импакт фактор за секој труд според JSR датабазата на Thomson Routers (доколку трудот е објавен во списание со импакт фактор)

[1] Mileva, Aleksandra and Dimitrova, Vesna and Velichkov, Vesselin (2016) Analysis of the Authenticated Cipher MORUS (v1). In: Pasalic, E., Knudsen, L. R. (Eds.): Cryptography and Information Security in the Balkans - Second International Conference, *BalkanCryptSec 2015*, Koper, Slovenia, September 3-4, 2015, Revised Selected Papers. *Lecture Notes in Computer Science*, vol. 9540, pp. 45-59. Springer International Publishing Switzerland. ISBN 978-3-319-29172-7

[2] Šuteva, Natasa and Mileva, Aleksandra and Loleski, Mario (2015) Finding Forensic Evidence for Several Web Attacks*. International Journal of Internet Technology and Secured Transactions*, Vol. 6 No. 1, pp. 64-78. Inderscience Publishers. ISSN 1748-569X.

[3] Radinski, Gligorcho and Mileva, Aleksandra (2015) Comparative Analysis of Several Real-Time Systems for Tracking People and/or Moving Objects using GPS*. In: 7th ICT Innovations Conference 2015*, 1-4 Oct 2015, Ohrid, Republic of Macedonia.

[4] Stojanov, Done, Koceski, Sašo, Mileva, Aleksandra, Koceska, Nataša and Martinovska Bande, Cveta (2014) "Towards computational improvement of DNA database indexing and short DNA query searching." *Biotechnology & Biotechnological Equipment* 28 (5). pp. 958-967. ISSN 1310-2818 **(IF (2013) = 0.379)**

[5] Mileva, Aleksandra and Panajotov, Boris (2014) Covert channels in TCP/IP protocol stack - extended version-. *Central European Journal of Computer Science*, 4 (2). pp. 45-66.

[6] Stojanov, Ivan, Mileva, Aleksandra and Stojanovic, Igor (2014) A New Property Coding in Text

Steganography of Microsoft Word Documents. In: *Securware 2014*: *The Eighth International Conference on Emerging Security Information, Systems and Technologies*, 16-20 Nov 2014, Lisbon, Portugal.
[7] Šuteva, Natasa, Mileva, Aleksandra and Loleski, Mario (2014) Computer Forensic Analysis of Some Web Attacks. In: *World Congress on Internet Security (WorldCIS 2014)*, 8-10 Dec 2014, London, UK.
[8] Mileva, Aleksandra and Markovski, Smile (2014) Quasigroup Representation of Some Lightweight Block Ciphers. *Quasigroups and related systems*, 22 (2). pp. 267-276. ISSN 1561-2848
[9] Mileva, Aleksandra (2014) New Developments in Quasigroup-Based Cryptography. In: *Multidisciplinary Perspectives in Cryptology and Information Security*. IGI Global, pp. 286-317. ISBN 9781466658080
[10] Mileva, Aleksandra (2014) Multipermutations in Crypto World: Different Faces of the Perfect Diffusion Layer. *Cryptology ePrint Archive* (85).
[11] Markovski, Smile, Mileva, Aleksandra and Dimitrova, Vesna (2014) SBIM(Q) - a Multivariate Polynomial Trapdoor Function over the Field of Rational Numbers. *Cryptology ePrint Archive* (739)
[12] Šuteva, Nataša, Anastasov, Dragan, and Mileva, Aleksandra (2014) One Unwanted Feature of Many Web Vulnerability Scanners. *Proceedings of the 11th International Conference for Informatics and Information Technology*, April 11-12, Bitola
[13] Stojanov, Done, Koceski, Saso, and Mileva, Aleksandra (2013). DNA FLAG: Fast Local Alignment Generating Methodology. *Romanian Biotechnological Letters* 18 (1). pp. 7881-7888. ISSN 1224 - 5984 **(IF (2011) = 0.349)**
[14] Šuteva, Nataša, Zlatkovski, Dragi, and Mileva, Aleksandra (2013) Evaluation and Testing of Several Free/Open Web Vulnerability Scanners. In: *10th International Conference for Informatics and Information Technology (CIIT 2013),* pp. 221-224, April 18-21, Bitola
[15] Mileva, Aleksandra and Markovski, Smile (2013) Quasigroup Representation of Some Feistel and Generalized Feistel Ciphers. In: *ICT Innovations 2012: Secure and Intelligent Systems*. Advances in Intelligent Systems and Computing, 207 . Springer Berlin Heidelberg, pp. 161-171. ISBN 978-3-642-37168-4
[16] Mileva, Aleksandra, and Markovski, Smile (2012) Shapeless quasigroup derived by Feistel orthomorphisms*. Glasnik Matematicki, 47 (2)*, 333-349. ISSN 0017-095X **(IF (2011) = 0.302)**
[17] Mileva, Aleksandra (2012) Analysis of Some Quasigroup Transformations as Boolean Functions. *Mathematica Balkanica*, 26 (3-4). pp. 359-368. ISSN 0205-3217
[18] Zlatkovski, Dragi, Šuteva, Natasa, and Mileva, Aleksandra (2012). SQL Injection test system for students. In: *9th International Conference for Informatics and Information Technology (CIIT 2012*), pp. 234-236, Bitola.
[19] Stojanov, Done, Mileva, Aleksandra, and Koceski, Saso, (2012) A new, space-efficient local pairwise alignment methodology. *Advanced Studies in Biology*, 4 (2), 85 – 93, ISSN 1313-9495

Учество во научноистражувачки проекти:

Наслов на проектот	Период	Финансиран од:	Улога во проектот (главен истражувач или учесник
Примена на квазигрупите во криптографијата и податочната комуникација	2016-2017	МОН, Билатерален проект со Кина	Главен истражувач
Примена на квазигрупи во дизајн на криптографски примитиви и кодови кои откриваат и поправаат грешки	2015-2016	ФИНКИ-УКИМ	Учесник
Точен и безбеден пренос на податоци со примена на алгебарски структури	2014-2015	ФИНКИ-УКИМ	Учесник
Развој на нови алгоритми и софтверска библиотека за примена во биомедицинското инженерство	2013 - 2014	УГД	Главен истражувач
ICT COST Action IC1306: Cryptography for Secure Digital Interaction	2014-2018	EU-COST	Координатор
ICT COST Action IC1201 Behavioural	2012-2016	EU-COST	Координатор

Types for Reliable Large-Scale Software Systems (BETTY)			

Задолженија во предлог-проектот со временска рамка:

Месеци 1–6: Таа ќе учествува во следните активности:

- анализа на различните техники за криење на податоци во дигитални слики
- наоѓање на скриени канали во HTTP/2.0

Месеци 7–18: Таа ќе учествува во следните активности:

- наоѓање на скриени канали во QUIK
- дизајн и развој на анти-стеганографски техники за дигитални слики
- обид за добивање на S-кутии од мали квазигрупи од ред 4 или 8
- анализа на користењето на CSPRNG во генерирање на клучот матрица за Хил шифрата

Месеци 19–24: Пишување на научни трудови во кои ќе бидат изложени добиените научни резултати, нивно доставување за печатење во меѓународни научни списанија и нивно презентирање на научни конференции.

Месеци 1–24: Менаџирање и администрирање на проектот. Изработка на крајниот Извештај.

Истражувач: (приложете посебен формулар за секој истражувач вклучен во проектот)

Име и презиме	**Педро Инацио**
Титула	Доктор на компјутерски науки и инженерство
Позиција	Доцент
Адреса	Departamento de Informática Universidade da Beira Interior Rua Marquês d'Ávila e Bolama 6201-001 Covilhã
Тел / Факс:	+351 964684969
e-mail	inacio@di.ubi.pt

Кратка биографија:
Pedro Ricardo Morais Inácio е роден во Covilhã, Португалија, во 1982. До сега се има стекнато со 5-годишен B.Sc. степен по математика/компјутерски науки и звање доктор на компјутерски науки и инженерство, од University of Beira Interior (UBI), Португалија, во 2005 и 2009 соодветно. Работата околу докторатот ја изведувал во компаниска околина на Nokia Siemens Networks Portugal S.A., со Ph.D грант од Португалската фондација за наука и технологии.

Тој е професор на компјутерски науки на UBI од 2010, каде предава предмети поврзани со безбедност на информации, програмирање на мобилни уреди и компјутерски базирани симулации, и тоа на додипломски, постдипломски и докторски студии во компјутерски науки и инженерство. Тековно е одговорен за програмата на додипломски студии по веб информатика. Инструктор е на UBI Cisco академијата.

Тој е IEEE сениор член и истражувач во Instituto de Telecomunicações (IT). Главните области на истражување му се безбедност на информации, компјутерски базирани симулации, и мониторинг, анализа и класификација на мрежниот сообраќај. Има над 30 публикации во форма на поглавја на книги и трудови во меѓународно оценувани книги, конференции и списанија. Често оценува трудови од IEEE, Springer, Wiley и Elsevier списанија. Член е на Технички програмски комитет на меѓународни конференции како ACM Symposium on Applied Computing - Track on Networking. Беше еден од едиторите на WISARC 2016.

Трудови објавени во последните 5 години, со назначен импакт фактор за секој труд според JSR датабазата на Thomson Routers (доколку трудот е објавен во списание со импакт фактор)

[1] Diogo A. B. Fernandes, Liliana F. B. Soares, João V. Gomes, Mário M. Freire, and Pedro R. M. Inácio, Security Issues in Cloud Environments - A Survey, International Journal of Information Security (IJIS), 13(2):113-170, April 2014. ISSN 1615-5262. Institute for Scientific Information (ISI) Impact Factor (2012): **0.480**.

[2] João V. Gomes, Pedro R. M. Inácio, Manuela Pereira, Mário M. Freire, and Paulo P. Monteiro, Identification of Peer-to-Peer VoIP Sessions Using Entropy and Codec Properties, IEEE Transactions on Parallel and Distributed Systems (IEEE TPDS), 24(10): 2004-2014, 2013. ISSN 1045-9219. ISI Impact Factor (2012): **1.796**.

[3] João V. Gomes, Pedro R. M. Inácio, Manuela Pereira, Mário M. Freire, and Paulo P. Monteiro, Detection and Classification of Peer-to-Peer Traffic: A Survey, ACM Computing Surveys (CSUR), 45(3):1-40, June 2013. ISSN 0360-0300. ISI Impact Factor (2011): **4.529**.

[4] Pedro R. M. Inácio, Mário M. Freire, Manuela Pereira, and Paulo P. Monteiro, Fast Synthesis of Persistent Fractional Brownian Motion, ACM Transactions on Modelling and Computer Simulation (TOMACS), 22(2): Article 11, 21 pages, March 2012. ISSN 1049-3301. ISI Impact Factor (2011): **1.114**.

[5] João V. Gomes, Pedro R. M. Inácio, Manuela Pereira, Mário M. Freire, and Paulo P. Monteiro, Exploring Behavioral Patterns Through Entropy in Multimedia Peer-to-Peer Traffic, The Computer Journal (Oxford University Press), 55(6): pp. 740-755, 2012. Corrigendum, 55(10): 1265-1265, 2012. ISI Impact Factor (2011): **0.785**.

Учество во научноистражувачки проекти:

Наслов на проектот	Период	Финансиран од:	Улога во проектот (главен истражувач или учесник
Hacker Fighter - Game-based approach to fight piracy and counterfeiting	September 2015 — August 2016	Office for Harmonization in the Internal Market (OHIM)	Information Technology specialist
QoEViS - Quality of Experience in Video Streaming	July 2014 – July 2015	Instituto de Telecomunicações	Учесник
TRAMANET - Traffic and Trust Management in Peer-to-Peer Networks	January 2008 – June 2011	Fundação para a Ciência e a Tecnologia (FCT)	Учесник
Active Security Mechanisms for Passive Optical Networks (PON) Point-to-Multipoint (P2M) Environment	April 2007 – June 2008	Agência da Inovação (ADI)	Leader of task 2.1

Задолженија во предлог-проектот со временска рамка:

Месеци 1–6: Анализа на барањата за системот за е-гласање. Идентификација и дефиниција на финкционални и безбедносни барања, модел на систем и напади. Дизајн на криптосистем со Хил шифра, базиран на CSPRNG.

Месеци 7–18: Предлог на систем за е-гласање (системски компоненти, криптографски примитиви, користење и процедурален протокол). Имплементирање на прототип.
Имплеменетација на криптосистем со Хил шифра. Споредба на предложената процедура за генерирање на матрицата клуч со други алгоритми опишани во литературата. Тестирање на шифрата.

Месеци 19–24: Научните резултати ќе бидат презентирани пред јавноста на неколку начини, преку презентација на научни и домашни конференции и трудови во списанија.

Истражувач: (приложете посебен формулар за секој истражувач вклучен во проектот)

Име и презиме	**Стефка Бујуклиева**
Титула	Doctor of Science in Mathematics
Позиција	Професор
Адреса	"Т. Трновски" 3, 5000, Велико Трново, Бугарија
Тел / Факс:	++359 888 131 165
e-mail	stefka@uni-vt.bg

Кратка биографија:

Образование:

- Доктор на науки, Софија, јуни 2008 (Теза: Само-дуални кодови и групи на автоморфизми).
- Ph.D., Великотрновски универзитет, октомври 1997 (Теза: Екстремни само-дуални кодови, ментор проф. д-р Васил Јоргов)
- Diploma in Mathematics, M.Sc., Софиски универзитет, јули 1988

Работно искуство:

- Раководител на катедра, Алгебра и Геометрија, Великотрновски универзитет "Св. Кирил и Методиј", 2003 -
- Редовен професор, Великотрновски универзитет "Св. Кирил и Методиј", 2012 -
- Вонреден професор, Великотрновски универзитет "Св. Кирил и Методиј", 2000-2011.
- Доцент, Великотрновски универзитет "Св. Кирил и Методиј", 1992-2000.
- Институтот по Математика и Информатика при БАН, 1988 - 1992

Членство во професионални асоцијации: Union of Bulgarian Mathematicians

Член на програмски одбор:

- International Workshop on Algebraic and Combinatorial Coding Theory, Kranevo, Bulgaria, June 2004.
- International Workshop on Algebraic and Combinatorial Coding Theory, Zvenigorod, Russia, September 2006.
- International Workshop on Algebraic and Combinatorial Coding Theory, Pamporovo, Bulgaria, June 2008.
- International Workshop on Algebraic and Combinatorial Coding Theory, Novosibirsk, RUSSIA, September 2010.
- Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory, Pomorie, Bulgaria, June 2012.
- Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory, Svetlogorsk, Russia, September 2014.
- Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory, Albena, Bulgaria, June 2016.
- Head of the Jury, National Mathematical Olympiad for University Students, Veliko Tarnovo, 2006.
- Member of the Jury, National Mathematical Olympiad for University Students, Sozopol, 2007.
- Member of the Organizing Committee, International Colloquium on Differential Geometry and its Related Fields, Veliko Tarnovo, Bulgaria, September 2010, 2012, 2014, 2016.
- Member of the Jury, National Mathematical Olympiad for University Students, Sofia, 2011.
- Head of the Jury, First National Olympiad on Computer Mathematics for University Students, Gabrovo, 2012.
- Member of the Juri, National Olympiads on Computer Mathematics for University Students, 2013, 2014, 2016.

Поле на научен интерес: Алгебра, Теорија на кодирањето и комбинаторика, Криптографија, Конечни полиња, Теорија на броевите.

Трудови објавени во последните 5 години, со назначен импакт фактор за секој труд според JSR датабазата на Thomson Routers (доколку трудот е објавен во списание со импакт фактор)

[1] S. Bouyuklieva and W. Willems, "Singly-even self-dual codes with minimal shadow", IEEE Trans. Inform. Theory, vol. 58, pp. 3856--3860, June 2012. Impact Factor (2012) **3.009**

[2] S. Bouyuklieva and I. Bouyukliev, "An algorithm for classification of binary self-dual codes", IEEE Trans. Inform. Theory, vol. 58, pp. 3933--3940, June 2012. Impact Factor (2012) **3.009**

[3] S. Bouyuklieva, N. Yankov, Jon-Lark Kim, "Classification of binary self-dual [48,24,10] codes with an

automorphism of odd prime order", Finite Fields and Their Applications, vol. 18, Issue 6, pp. 1104–1113, November 2012. 5-Year Impact Factor: 1.299, SCImago Journal Rank (SJR): **1.096**, Source Normalized Impact per Paper (SNIP): 1.344
[4] S. Bouyuklieva, I. Bouyukliev and M. Harada, "Some extremal self-dual codes and unimodular lattices in dimension 40", Finite Fields and Their Applications, vol. 21, pp. 67–83, 2013. 5-Year Impact Factor: 1.299, SCImago Journal Rank (SJR): **1.096**, Source Normalized Impact per Paper (SNIP): 1.344
[5] Stefka Bouyuklieva, Javier de la Cruz, Wolfgang Willems, "On the automorphism group of a binary self-dual [120,60,24] code", Applicable Algebra in Engineering, Communication and Computing, vol. 24, pp 201-214, August 2013. SJR – 2015 - 0.354, 5 Year Impact Factor – 2015 – **0.722**.
[6] S. Bouyuklieva, W. Willems, N. Yankov, On the automorphisms of order 15 for a binary self-dual [96,48,20] code, Designs, Codes and Cryptography, vol. 79, pp. 171-182, April 2016. Impact Factor **0.781**
[7] S. Bouyuklieva and W. Willems, "Connections between different types of binary self-dual codes", Proceedings of the International Workshop ACCT, Pomorie, Bulgaria, pp. 111-116, 2012.
[8] S. Bouyuklieva, "Applications of the Gaussian integers in coding theory", Prospects of Differential Geometry and its Related Fields, World Scientific, Proceedings of the 3rd International Colloquium on Differential Geometry and its Related Topics, Veliko Tarnovo, Bulgaria, pp. 39-49, 2012.
[9] S. Bouyuklieva and I. Bouyukliev, "On the binary quasi-cyclic codes", Proceedings of the International Workshop OCRT, Albena, Bulgaria, pp. 59-64, 2013.
[10] S. Bouyuklieva and N. Yankov, "Some binary self-dual codes having an automorphism of order 15", Proceedings of the International Workshop ACCT, Svetlogorsk, Russia, pp. 103-108, 2014.
[11] S. Bouyuklieva, R. Russeva and E. Karatash, "On some automorphisms of order 3 of the extremal binary codes", Fifteenth International Workshop ACCT, Albena, Bulgaria, 18-24 June 2016.
[12] D. Bikov, I. Bouyukliev and S. Bouyuklieva, "S-boxes from binary quasi-cyclic codes", Fifteenth International Workshop ACCT, Albena, Bulgaria, 18-24 June 2016.

Учество во научноистражувачки проекти:

Наслов на проектот	Период	Финансиран од:	Улога во проектот (главен истражувач или учесник
Алгебрични и геометрични модели в кодирането и криптографията и реализирането им чрез паралелни алгоритми	**2014-2016**	**ВТУ**	**главен истражувач**
Алгебрични, геометрични и стохастични приложения при защита на информацията	**2010-2012**	**ВТУ**	**главен истражувач**
Разработване на методи, модели, алгоритми и програми, свързани с линейни и адитивни кодове, използвани за защита на информацията	**2008-2009**	**ВТУ**	**главен истражувач**
Математически основи на информатиката: алгоритми, защита на информацията, геометрични методи и модели	**2007**	**ВТУ**	**главен истражувач**
Самоортогонални кодове и групи от автоморфизми	**2003-2005**	**Фонд "Научни изследвания", Министерство на образованието и науката, България**	**учесник**

Задолженија во предлог-проектот со временска рамка:

Месеци 1–6: Ќе учествува во истражувањето за добивање на S-кутии од бинарни квази-циклични кодови

Месеци 7–18: Ќе учествува во:

- Паралелна реализација на брзи алгоритми за пресметување на различни метрики кај S-кутии
- Обид за добивање на S-кутии од мали квазигрупи од ред 4 или 8

Месеци 19–24: Научните резултати ќе бидат презентирани на меѓународни и домашни конференции и печатени во меѓународни списанија.

Истражувач: (приложете посебен формулар за секој истражувач вклучен во проектот, минимум 2 учесници, **сите информации за истражувачите на не повеќе од две страници)**)

Име и презиме	**Наташа Стојковиќ**
Титула	Доктор на информатички науки
Позиција	Доцент
Адреса	Крсте Мисирков бб, Штип, Р. Македонија
Тел / Факс:	00 389 32 550 113
e-mail	natasa.maksimova@ugd.edu.mk

Кратка биографија:

Образование:

- Доктор на информатички науки, ФИНКИ, 2015.
- Магистер на информатички науки, ИИ, ПМФ, 2009.
- Дипломиран инженер по информатика, ИИ, ПМФ, 2002.
- Дипломиран професор по математика, ИМ, ПМФ, 2000.

Работно искуство:

- Доцент при УГД, Штип, 2016 -
- Асистент при УГД, Штип, 2010 - 2016
- Помлад асистент при УГД, Штип, 2007 - 2010
- Програмер во Максистем, Скопје , 2003 - 2008

Членство во професионални асоцијации:

- IEEE

Поле на научен интерес:

- Надежност на транспортни системи
- Моделирање и симулации
- Теорија на графови
- Операциони истражувања
- Веројатност и статистика

Трудови објавени во последните 5 години, со назначен импакт фактор за секој труд според JSR датабазата на Thomson Routers (доколку трудот е објавен во списание со импакт фактор)

[1] M.Mihova, N.Stojkovikj, M.Jovanov and E.Stankov “Maximal Level Minimal Path Vectors of a Two-terminal Undirected Network”, *IEEE Transactions on Reliability*, Vol. 65, Issue 1, ISSN 0018-9529, pp. 282 – 290,2016 (IF 2.278).

[2] M.Mihova, N.Stojkovikj, M.Jovanov and E.Stankov “On Maximal Level Minimal Path Vectors of a Two-Terminal Network”, Olympiads in Informatics, 2014, Vol. 8, 133–144, 26th International Olympiad in Informatics,Taipei, Taiwan.

[3] Mihova, M, Maksimova N "Estimation of minimal path vectors of multi state two terminal networks with cycles control", Mathematica Balkanica, Vol. 25 , Fasc 4, ISSN 0205-3217, pp. 437-447,2011

[4] M.Mihova, N. Maksimova, Kj. Gjorgjiev, “Optimal improving of network reliability: Reliability of the improved network”, Proceedings of the IV Congress of the Mathematicians of Republic of Macedonia, Skopje 2011 (247-257)

[5] M. Mihova and N.Stojkovikj, “Simulating the profit of work on multi state two terminal transportation system”, Proceedings of the 9th International Conference for Informatics and Information Techology (CIIT 2012),

[6] Mihova, M, Ilijoski B, Stojkovic N. "The Optimization of the Profit of a Parallel System with Independent Components and Linear Repairing Cost" , 2012 Web proceedings of ICT Innovations 2012 , Ohrid,ISSN 1857-7288, pp.507-516

[7] Martinovska, C, Maksimova N, Gacovski Z, "A Fuzzy Based Approach to Selecting Successful Contractor for Public Procurement", The 2nd International Conference, Science and technology in the Context of Sustainable, Ploesti, Romania,2011.

[8] Lazarova, L, Miteva, M, Stojkovic N. "The Black-Scholes model and valuation of the European Call option", Yearbook-Faculty of Computer Science 2013 . ISSN 1857-8691,pp 209-220

[9] N Stojkovik, L Lazarova, M Miteva.”Calculation of multi-state two terminal reliabilty” Yearbook-Faculty of Computer Science 2014 . ISSN 1857- 8691, pp 5-10

[10] A.Stojanova, N.Stojkovic and Dusan Bikov “Java IDEs for learning and understanding object oriented language”, Yearbook-Faculty of Computer Science 2012 . ISSN 1857-

8691,pp 232-240.
[11] Maksimova N, Suteva G, Jovanov V,"Fractions and Operation with fractions, Using of Interactive Table", Proceeding of 11th International Education Technology Conference (IETC), Istanbul, May 2011.
[12] Stojanova, Aleksandra and Stojkovic, Natasa and Bikov, Dusan, "*Tools for software visualization.*", Yearbook of the Faculty of Computer Science, 3 (3). pp. 47-55. ISSN 1857- 8691, 2015
[13] Natasa Stojkovic, Aleksandra Stojanova, Dusan Bikov, Gabriela Suteva: „Children dependence from internet" In proceedings of III Scientific – proffesional meeting „Education in 21st century" 2011, Bitola, ISBN 978-608-4616-24-5
[14] Natasa Stojkovic, Aleksandra Stojanova, Dusan Bikov, Gabriela Suteva: „Training using computer games" III Scientific – professional meeting In proceedings of III Scientific – professional meeting „Education in 21st century" 2011, Bitola, ISBN 978-608-4616-24-5
[15] Stojanova, Aleksandra and Zlatanovska, Biljana and Kocaleva, Mirjana and Miteva, Marija and Stojkovic, Natasa (2016) "Mathematica" as a tool for characterization and comparison of one parameter families of square mappings as dynamic systems. In: ITRO 2016, 10 June 2016, Zrenjanin, Serbia.
[16] Zlatanovska, Biljana and Stojanova, Aleksandra and Kocaleva, Mirjana and Stojkovic, Natasa and Krstev, Aleksandar (2016)"Mathematica as program support in the integral calculations", In: TIO 2016 - Technics and informatics in education, 28-29 May 2016, Čačak, Serbia.
[17] Stojkovic, Natasa and Stojanova, Aleksandra and Kocaleva, Mirjana and Zlatanovska, Biljana (2016) ", In: ITRO 2016, 10 June 2016, Zrenjanin, Serbia.
[18] Stojanovski, Strasko and Stojkovic, Natasa and Ananiev, Jovan and Kocaleva, Mirjana and Stojanova, Aleksandra and Zlatanovska, Biljana (2016) ,", In: ITRO 2015, 10 June 2016, Zrenjanin, Serbia.

Учество во научноистражувачки проекти:

Наслов на проектот	**Период**	**Финансиран од:**	**Улога во проектот (главен истражувач или учесник**
Развој на напредни техники на кооперативно локализирање и мапирање со мобилни роботи и нивна примена во прецизно земјоделие	2015-2018	УГД	Учесник

Задолженија во предлог-проектот со временска рамка:
Месеци 1–6: Ќе учествува во развојот на алгоритми за наоѓање на минимални пат вектори во двотерминален повеќе - состојбен транспортен систем кои ќе имаат помала временска сложеност од постоечките алгоритми

Месеци 7–18: Ќе учествува во имплементирањето на алгоритми за споредба на времињата на извршување кај двотерминални повеќе - состојбени транспортни системи

Месеци 21–24: Пишување на научни трудови во кои ќе бидат изложени добиените научни резултати, нивно доставување за печатење во меѓународни научни списанија и нивно презентирање на научни конференции (иако публикувањето на парцијалните резултати од проектот ќе се изведува во текот на целиот проект).

Истражувач: (приложете посебен формулар за секој истражувач вклучен во проектот)

Име и презиме	**Доне Стојанов**
Титула	Доктор на науки (компјутерска техника и информатика)
Позиција	Асистент
Адреса	Крсте Мисирков, бб, Штип, Р. Македонија
Тел / Факс:	00 38932550134
e-mail	done.stojanov@ugd.edu.mk

Кратка биографија:

Роден е на 15.01.1985 во Струмица. Во 2008 дипломирал на Факултет за електротехника и информациски технологии, Скопје. Во 2010 година се здобива со титула Магистер на софтверско инженерство, бранејќи ја темата, **"Биоинформатичка анализа на постоечки и нови модели на протеини"**. На 7.12.2015 година го брани докторскиот труд со наслов ,,**Алгоритми за порамнување и пребарување на ДНК секвенци**", со што се стекнува со научно звање доктор на науки. На 7ми Март 2016 е избран во наставно-научно звање доцент на Факултетот за информатика при УГД - Штип.

Трудови објавени во последните 5 години во стручни списанија кои се наоѓаат на меѓународно признатата листа СЦИ (SCI - Science citation index), со назначен импакт фактор за секој труд:

[1] Stojanov, Done and Madevska Bogdanova, Ana and Orzechowski, Tomasz (2016) *TMO: time and memory optimized algorithm applicable for more accurate alignment of trinucleotide repeat disorders associated genes.* Biotechnology & Biotechnological Equipment, 30 (2). pp. 388-403. ISSN 1310-2818 (**IF=0,373**)

[2] Stojanov, Done and Koceski, Saso and Mileva, Aleksandra and Koceska, Natasa and Martinovska Bande, Cveta (2014) *Towards computational improvement of DNA database indexing and short DNA query searching.* Biotechnology & Biotechnological Equipment, 28 (5). pp. 958-967. ISSN 1310-2818 (**IF=0,373**)

[3] Stojanov, Done and Koceski, Saso and Mileva, Aleksandra (2013) *FLAG: Fast Local Alignment Generating Methodology.* Romanian Biotechnological Letters, 18 (1). pp. 7881-7888. ISSN 1224 – 5984 (**IF=0,404**)

[4] Kocaleva, Mirjana and Stojanov, Done and Stojanovic, Igor and Zdravev, Zoran (2016) Pattern Recognition and Natural Language Processing: State of the Art. TEM Journal, 5 (2). pp. 236-240. ISSN 2217-8309 / 2217-8333 (Online)

[5] Stojanov, Done and Koceski, Saso (2014) Topological MRI Prostate Segmentation Method. Proceedings of the 2014 Federated Conference on Computer Science and Information Systems, 2. pp. 219-225. ISSN 2300-5963

[6] Stojanov, Done and Martinovska, Cveta (2014) Improved alignment of homologous DNA sequences. Annals of West University of Timişoara, ser. Biology, 16 (2). pp. 97-106. ISSN 1453-7680

[7] Stojanov, Done (2012) IC: Intelligent Clustering, a new time efficient data partitioning methodology. International Journal of Computer Science and Information Technologies, 3 (5). pp. 5065-5067. ISSN 0975-9646

[8] Stojanov, Done and Mileva, Aleksandra and Koceski, Saso (2012) A new, space-efficient local pairwise alignment methodology.Advanced Studies in Biology, 4 (2). pp. 85-93. ISSN 1313-9495

Учество во научноистражувачки проекти:

Наслов на проектот	Период	Финансиран од:	Улога во проектот (главен истражувач или учесник
Развој на нови алгоритми и софтверска библиотека за примена во биомедицинско инженерство	2013-2015	Универзитет ,,Гоце Делчев" - Штип	Млад истражувач

Задолженија во предлог-проектот со временска рамка:

Месеци 1–6: Собирање на безбедносни податоци од лог датотеки и различни скенирања

Месеци 7- 18: Анализа на добиени безбедносни податоци со различни техники од Вештачка интелигенција

Месеци 19–24: Научно–истражувачките резултати ќе бидат презентирани на поширокатa јавност на неколку начини и тоа преку презентации на меѓународни и домашни конференции, а голем дел од резултатите ќе бидат публикувани како научни трудови во научни списанија.

Млад истражувач: (приложете посебен формулар за секој млад истражувач вклучен во проектот, минимум 2 учесници)
сите информации за младиот истражувач на не повеќе од една страна)

Име и презиме	**Душан Биков**
Титула	Магистер по информатика. Информациони системи
Позиција	асистент
Адреса	ул. Крсте Мисирков 10-А, Штип, Македонија
Тел / Факс:	032 550 135
e-mail	dusan.bikov@ugd.edu.mk

Кратка биографија:
М-р Душан Биков е роден на 06.01.1987 година во Штип, каде што ги завршил основното и средното образование со одличен успех. Во академската 2005/2006 година се запишал на студиите по информатика, при Факултетот за математика и информатика Велико Трново, Бугарија. Дипломира во јули 2009. Во септември се запишува на постдипломски студии на истиот факултет. Во март 2011 го одбранил својот магистерски труд под наслов „*Analysis, simulation and application of cryptography on an elliptic curve in wireless sensor networks*“ под менторство на проф. д-р Стефка Бујуклиева со што се стекнува со звање магистер по информатика. Информациони системи. Во декември 2012 година на Факултетот за математика и информатика во Велико Трново, прифатена му е темата за докторска дисертација „*Algebraic cryptanalysis and design of cryptographic primitives*“ под менторство на проф. д-р Стефка Бујуклиева. Од септември 2011 година работи на Факултетот за информатичка во Штип како соработник-асистент.

Трудови објавени во последните 5 години, со назначен импакт фактор за секој труд според JSR датабазата на Thomson Routers (доколку трудот е објавен во списание со импакт фактор)

1. **D. Bikov**, I. Bouyukliev, S. Bouyuklieva, S-Boxes from Binary Quasi-Cyclic Codes, Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory, Albena, (2016)
2. **D. Bikov**, I. Bouyukliev, A. Stojanova, Benefit of Using Shared Memory in Implementation of Parallel FWT Algorithm with CUDA C on GPUs, Proceedings of 7th International Conference Information Technologies and Education Development, Zrenjanin, Serbia, (2016) pp.250-256, ISBN 978-86-7672-285-3
3. **Dusan Bikov**, Aleksandra Stojanova: „Using gpu matrix vector multiplication for computing walsh spectra". ETAI 2015, Ohrid
4. Iliya Bouyukliev, **Dusan Bikov**: „Applications of the binary representation of integers in algorithms for boolean functions". SMB 2015, Kamchia
5. **Dusan Bikov**, Stefka Bouyuklieva, Aleksandara Stojanova,: “S-boxes – parameters, characteristics and classifications”, Faculty of Computer Science, UGD Yearbook - Vol 1, No 2, 2013, pp. 47-52, ISSN: 1857- 8691, Stip, Macedonia
6. **Dusan Bikov**, Stefka Bouyuklieva, Aleksandra Stojanova: “Wireless Network Security and Cracking Security Key”, Jubilee Scientific Conference "50 Years University" St. Cyril and Methodius ", 2013, Veliko Tarnovo

Учество во научноистражувачки проекти:

Наслов на проектот	Период	Финансиран од:	Улога во проектот (главен истражувач или учесник
Сензорски мрежи за надгледување и контрола на производство на вино	**2014 - 2016**	**УГД**	**учесник**
Алгебрични и геометрични модели в кодирането и криптографията и реализирането им чрез паралелни алгоритми, ВТУ, договор № РД-09-422-13 от 09. 04. 2014 г.	**2014 - 2016**	**ВТУ - БГ**	**учесник**

Изработка на магистерски/докторски труд – наслов:

„**Algebraic cryptanalysis and design of cryptographic primitives**“ – докторски труд

Задолженија во предлог-проектот со временска рамка:

Месеци 1–6:

- Добивање на S-кутии од бинарни квази-циклични кодови

Месеци 7–18:

- Паралелна реализација на брзи алгоритми за пресметување на различни метрики кај S-кутии
- Обид за добивање на S-кутии од мали квазигрупи од ред 4 или 8

Месеци 19–24: Научните резултати ќе бидат презентирани на меѓународни и домашни конференции и печатени во меѓународни списанија.

Млад истражувач: (приложете посебен формулар за секој млад истражувач вклучен во проектот)

Име и презиме	**Горан Митковски**
Титула	Дипломиран инженер по информатика
Позиција	Студент на втор циклус
Адреса	Ѓорче Петров бб , Куманово
Тел / Факс:	077 984 779
e-mail	goran_mitkovski@yahoo.com

Кратка биографија:
Образование:

2006 - 2012 **Дипломиран инженер по Информатика**
Универзитет „Св. Кирил и Методиј“, Скопје, Македонија
Природно Математички Факултет – ПМФ
Институт за Информатика
Насока-Компјутерски Архитектури и Мрежи

2013- сега **Постдипломски Студии по Информатика Master**
Универзитет „Гоце Делчев“, Штип, Македонија
Факултет за Информатика
Насока-Софтверско Инженерство

2008 – 2010 **Сертификати**
Cisco Networking Academy, Скопје, Македонија
Courses in:

- CCNA Exploration: Network Fundamentals
- CCNA Exploration: Routing Protocols and Concepts
- CCNA Exploration: LAN Switching and Wireless
- CCNA Exploration: Accessing the WAN
- CCNA Exploration: Fundamentals of Wireless LANs

Работно искуство:

2010 – 2010 Volvo Македонија – Скопје
3 месеци пракса како рецепционер и одговорен за резервни делови.

2011 - сега Развивање на Софтвер во PHP CodeIgniter framework како фриленсер.

2011 - 2014 Pro Sound – Скопје, Македонија
Управување и одржување на компјутерски системи и аудио опрема.

2014 – сега К3 Телевизија: Реализатор на Програма, IT- Сектор, Техничко водство, Раководител на Техника.

Изработка на магистерски труд – наслов:
Развој на анти-стеганографски техники за дигитални слики

Задолженија во предлог-проектот со временска рамка:
Месеци 1–6: Анализа на различните техники за криење на податоци во дигитални слики.

Месеци 7–18: Дизајн и развој на анти-стеганографски техники за дигитални слики и нивно имплементирање како алатки.

Месеци 19–24: Пишување на научни трудови во кои ќе бидат изложени добиените научни резултати, нивно доставување за печатење во меѓународни научни списанија и нивно презентирање на научни конференции. Се очекува дека во рамките на овој проект ќе бидат добиени поголем дел од резултатите за нејзиниот магистерски труд.

Млад истражувач: (приложете посебен формулар за секој млад истражувач вклучен во проектот)

Име и презиме	**Билјана Димитрова**
Титула	Дипломиран инженер по електротехника и информациски технологии
Позиција	Студент на втор циклус
Адреса	Крсте Мисирков, бб, Штип, Р. Македонија
Тел / Факс:	+389 78 397 736
e-mail	biljana.dimitrova@ugd.edu.mk

Кратка биографија:
Билјана Димитрова е студент на втор циклус на студии на насоката Информациони технологии и системи на Факултет за информатика при Универзитетот Гоце Делчев – Штип. Има дипломирано на насоката Телекомуникации на Факултетот за електротехника и информациони технологии при Универзитетот Св. Кирил и Методиј – Скопје во 2010 година. Од 2010 година работи како специјалист за корисничка поддршка во одделот за електронски индекс на Универзитет Гоце Делчев – Штип, каде е вклучена во дизајн и изработка на комплексен систем за целосна електронска администрација на студенти и вработени. Поле на нејзини интереси се информациони системи, криптографија, стеганографија, безбедност на информациони системи, безбедност на мрежи. Моментално работи на истражување за методите на криење на податоци во новите протоколи за пренос на веб содржини.

Изработка на магистерски труд – наслов:
Криење на податоци во новите протоколи за пренос на веб содржини

Задолженија во предлог-проектот со временска рамка:

Месеци 1–6: Наоѓање на скриени канали во HTTP/2.0

Месеци 7–18: Наоѓање на скриени канали во QUIK

Месеци 19–24: Пишување на научни трудови во кои ќе бидат изложени добиените научни резултати, нивно доставување за печатење во меѓународни научни списанија и нивно презентирање на научни конференции. Се очекува дека во рамките на овој проект ќе бидат добиени поголем дел од резултатите за нејзиниот магистерски труд.

Researchers:

Principal researcher

Name Surname	**Aleksandra Mileva**
Title	**PhD in Computer Science**
Position	**Associate Professor**
Address	**"Krste Misirkov" 10-A, 2000, Štip, Macedonia**
Tel./Fax.	**++389 78 222 460**
e-mail	**aleksandra.mileva@ugd.edu.mk**

Short CV:

Education:

- PhD of computer science, Univ. "Ss. Cyril and Methodius", Faculty of Natural Sciences, 2010.
- Master of computer science, Univ. "Ss. Cyril and Methodius", Faculty of Natural Sciences, 2004.
- Graduated engineer of computer science, Univ. "Ss. Cyril and Methodius", Faculty of Natural Sciences, 1998.

Working positions:

- Associate Professor at Faculty of computer science at Univ. "Goce Delcev", Štip, 2015 - Assistant Professor at Faculty of computer science at Univ. "Goce Delcev", Štip, 2010 - 2015
- Teaching and research assistant at Faculty of computer science at Univ. "Goce Delcev", Štip, 2007-2010
- Younger assistant and teaching and research assistant at Faculty of mining and geology at Univ. "Ss. Cyril and Methodius", Štip, 2001-2007
- Demonstrator at Faculty of Natural Sciences at Univ. "Ss. Cyril and Methodius", Skopje, 1999-2001

Membership in professional associations: IEEE, ICT-ACT, Macedonia

Program committee member:

- Tenth International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2016, 24-28 July, Nice, France
- Second International Workshop on Information Security, Assurance and Reliability in the Cloud, WISARC 2016, 6-9 December, Shangai, China (Program Co-Chair)
- Ninth International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2015
- International Mathematical Conference on Quasigroups and Loops, LOOPS '15, Ohrid, Macedonia, 2015.
- 7th ICT Innovations conference 2015, 1-4 October, 2015, Ohrid, Macedonia
- 6th ICT Innovations conference 2014, 9-12 September, 2014, Ohrid, Macedonia
- 2nd International Workshop on Behavioural Types (BEAT 2), 23-24 September, 2013, Madrid, Spain

Scientifically-research fields of interest: Cryptography, Computer and network security, Digital steganography, Theory of quasigroups

Scientific papers published in the last 5 years, indicating the impact factor according to JSR database of Thomson Routers (if any) of the journals in which each paper was published

[1] Mileva, Aleksandra and Dimitrova, Vesna and Velichkov, Vesselin (2016) Analysis of the Authenticated Cipher MORUS (v1). In: Pasalic, E., Knudsen, L. R. (Eds.): Cryptography and Information Security in the Balkans - Second International Conference, *BalkanCryptSec 2015*, Koper, Slovenia, September 3-4, 2015, Revised Selected Papers. *Lecture Notes in Computer Science*, vol. 9540, pp. 45-59. Springer International Publishing Switzerland. ISBN 978-3-319-29172-7

[2] Šuteva, Natasa and Mileva, Aleksandra and Loleski, Mario (2015) Finding Forensic Evidence for Several Web Attacks*. International Journal of Internet Technology and Secured Transactions*, Vol. 6 No. 1, pp. 64-78. Inderscience Publishers. ISSN 1748-569X.

[3] Radinski, Gligorcho and Mileva, Aleksandra (2015) Comparative Analysis of Several Real-Time Systems for Tracking People and/or Moving Objects using GPS. *In: 7th ICT Innovations Conference 2015*, 1-4 Oct 2015, Ohrid, Republic of Macedonia.

[4] Stojanov, Done, Koceski, Sašo, Mileva, Aleksandra, Koceska, Nataša and Martinovska Bande, Cveta (2014) "Towards computational improvement of DNA database indexing and short DNA query searching." *Biotechnology & Biotechnological Equipment* 28 (5). pp. 958-967. ISSN 1310-2818 **(IF (2013) = 0.379)**

[5] Mileva, Aleksandra and Panajotov, Boris (2014) Covert channels in TCP/IP protocol stack - extended version-. *Central European Journal of Computer Science*, 4 (2). pp. 45-66.

[6] Stojanov, Ivan, Mileva, Aleksandra and Stojanovic, Igor (2014) A New Property Coding in Text

Steganography of Microsoft Word Documents. In: *Securware 2014*: *The Eighth International Conference on Emerging Security Information, Systems and Technologies*, 16-20 Nov 2014, Lisbon, Portugal.
[7] Šuteva, Natasa, Mileva, Aleksandra and Loleski, Mario (2014) Computer Forensic Analysis of Some Web Attacks. In: *World Congress on Internet Security (WorldCIS 2014)*, 8-10 Dec 2014, London, UK.
[8] Mileva, Aleksandra and Markovski, Smile (2014) Quasigroup Representation of Some Lightweight Block Ciphers. *Quasigroups and related systems*, 22 (2). pp. 267-276. ISSN 1561-2848
[9] Mileva, Aleksandra (2014) New Developments in Quasigroup-Based Cryptography. In: *Multidisciplinary Perspectives in Cryptology and Information Security*. IGI Global, pp. 286-317. ISBN 9781466658080
[10] Mileva, Aleksandra (2014) Multipermutations in Crypto World: Different Faces of the Perfect Diffusion Layer. *Cryptology ePrint Archive* (85).
[11] Markovski, Smile, Mileva, Aleksandra and Dimitrova, Vesna (2014) SBIM(Q) - a Multivariate Polynomial Trapdoor Function over the Field of Rational Numbers. *Cryptology ePrint Archive* (739)
[12] Šuteva, Nataša, Anastasov, Dragan, and Mileva, Aleksandra (2014) One Unwanted Feature of Many Web Vulnerability Scanners. *Proceedings of the 11th International Conference for Informatics and Information Technology*, April 11-12, Bitola
[13] Stojanov, Done, Koceski, Saso, and Mileva, Aleksandra (2013). DNA FLAG: Fast Local Alignment Generating Methodology. *Romanian Biotechnological Letters* 18 (1). pp. 7881-7888. ISSN 1224 - 5984 **(IF (2011) = 0.349)**
[14] Šuteva, Nataša, Zlatkovski, Dragi, and Mileva, Aleksandra (2013) Evaluation and Testing of Several Free/Open Web Vulnerability Scanners. In: *10th International Conference for Informatics and Information Technology (CIIT 2013),* pp. 221-224, April 18-21, Bitola
[15] Mileva, Aleksandra and Markovski, Smile (2013) Quasigroup Representation of Some Feistel and Generalized Feistel Ciphers. In: *ICT Innovations 2012: Secure and Intelligent Systems*. Advances in Intelligent Systems and Computing, 207 . Springer Berlin Heidelberg, pp. 161-171. ISBN 978-3-642-37168-4
[16] Mileva, Aleksandra, and Markovski, Smile (2012) Shapeless quasigroup derived by Feistel orthomorphisms*. Glasnik Matematicki, 47 (2)*, 333-349. ISSN 0017-095X **(IF (2011) = 0.302)**
[17] Mileva, Aleksandra (2012) Analysis of Some Quasigroup Transformations as Boolean Functions. *Mathematica Balkanica*, 26 (3-4). pp. 359-368. ISSN 0205-3217
[18] Zlatkovski, Dragi, Šuteva, Natasa, and Mileva, Aleksandra (2012). SQL Injection test system for students. In: *9th International Conference for Informatics and Information Technology (CIIT 2012*), pp. 234-236, Bitola.
[19] Stojanov, Done, Mileva, Aleksandra, and Koceski, Saso, (2012) A new, space-efficient local pairwise alignment methodology. *Advanced Studies in Biology*, 4 (2), 85 – 93, ISSN 1313-9495

Participation in research projects

Project title	Period	Financed by	Role in the project (PI or participant)
Application of Quasigroups in Cryptography and Data Communications	**2016 - 2017**	**MON, Bilateral project with China, P.R.**	**PI**
Application of quasigroups in design of cryptographic primitives and error-correcting and error-detecting codes	**2015-2016**	**FINKI-UKIM**	**Participant**
Correct and secure data transfer with application of algebraic structures	**2014-2015**	**FINKI-UKIM**	**Participant**
Development of novel algorithms and software library for biomedical engineering application	**2013 - 2014**	**UGD**	**PI**
ICT COST Action IC1306: Cryptography for Secure Digital Interaction	**2014-2018**	**EU-COST**	**MC member**
ICT COST Action IC1201 Behavioural Types for Reliable Large-Scale Software Systems (BETTY)	**2012-2016**	**EU-COST**	**MC member**

Tasks to be conducted in the frame of the project proposal (timetable)

Months 1–6: She will participate:

- analysis of different techniques for data hiding in digital images
- finding covert channels in HTTP/2.0

Months 7–18: She will participate:

- finding covert channels in QUIK
- design and development of anti-steganographic techniques for digital images
- obtaing of optimal S-boxes from small quasigroups of order 4 or 8
- analysis of the usage of a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) to generate the matrix key of the Hill cipher

Months 19–24: Scientific results will be presented to the public in several ways, through presentations on international and home conferences and papers in journals.

Months 1–24: Project management and administration. Writing of the final Report.

Senior Scientist/ Researcher

Name Surname	**Pedro R. M. Inácio**
Title	Ph.D in Computer Science and Engineering
Position	Assistant Professor, IEEE Senior Member
Address	Departamento de Informática Universidade da Beira Interior Rua Marquês d'Ávila e Bolama 6201-001 Covilhã
Tel./Fax.	+351 964684969
e-mail	inacio@di.ubi.pt

Short CV:

Pedro Ricardo Morais Inácio was born in Covilhã, Portugal, in 1982. Holds a 5-year B.Sc. degree in Mathematics/Computer Science and a Ph.D. degree in Computer Science and Engineering, obtained from the University of Beira Interior (UBI), Portugal, in 2005 and 2009 respectively. The Ph.D. work was performed in the enterprise environment of Nokia Siemens Networks Portugal S.A., through a Ph.D. grant from the Portuguese Foundation for Science and Technology.

He is a professor of Computer Science at UBI since 2010, where he lectures subjects related with information assurance and security, programming of mobile devices and computer based simulation, to graduate and undergraduate courses, namely to the B.Sc., M.Sc. and Ph.D. programmes in Computer Science and Engineering. He is currently the programme leader of the B.Sc. in Web Informatics. He is an instructor of the UBI Cisco Academy.

He is an IEEE senior member and a researcher of the Instituto de Telecomunicações (IT). His main research topics are information assurance and security, computer based simulation, and network traffic monitoring, analysis and classification. He has about 30 publications in the form of book chapters and papers in international peer-reviewed books, conferences and journals. He frequently reviews papers for IEEE, Springer, Wiley and Elsevier journals. He has been member of the Technical Program Committee of international conferences such as the ACM Symposium on Applied Computing - Track on Networking. He was one of the chairs of WISARC 2016.

Scientific papers published in the last 5 years, indicating the impact factor according to JSR database of Thomson Routers (if any) of the journals in which each paper was published

[6] Diogo A. B. Fernandes, Liliana F. B. Soares, João V. Gomes, Mário M. Freire, and Pedro R. M. Inácio, Security Issues in Cloud Environments - A Survey, International Journal of Information Security (IJIS), 13(2):113-170, April 2014. ISSN 1615-5262. Institute for Scientific Information (ISI) Impact Factor (2012): **0.480**.

[7] João V. Gomes, Pedro R. M. Inácio, Manuela Pereira, Mário M. Freire, and Paulo P. Monteiro, Identification of Peer-to-Peer VoIP Sessions Using Entropy and Codec Properties, IEEE Transactions on Parallel and Distributed Systems (IEEE TPDS), 24(10): 2004-2014, 2013. ISSN 1045-9219. ISI Impact Factor (2012): **1.796**.

[8] João V. Gomes, Pedro R. M. Inácio, Manuela Pereira, Mário M. Freire, and Paulo P. Monteiro, Detection and Classification of Peer-to-Peer Traffic: A Survey, ACM Computing Surveys (CSUR), 45(3):1-40, June 2013. ISSN 0360-0300. ISI Impact Factor (2011): **4.529**.

[9] Pedro R. M. Inácio, Mário M. Freire, Manuela Pereira, and Paulo P. Monteiro, Fast Synthesis of Persistent Fractional Brownian Motion, ACM Transactions on Modelling and Computer Simulation (TOMACS), 22(2): Article 11, 21 pages, March 2012. ISSN 1049-3301. ISI Impact Factor (2011): **1.114**.

[10] João V. Gomes, Pedro R. M. Inácio, Manuela Pereira, Mário M. Freire, and Paulo P. Monteiro, Exploring Behavioral Patterns Through Entropy in Multimedia Peer-to-Peer Traffic, The Computer Journal (Oxford University Press), 55(6): pp. 740-755, 2012. Corrigendum, 55(10): 1265-1265, 2012. ISI Impact Factor (2011): **0.785**.

Participation in research projects

Project title	Period	Financed by	Role in the project (PI or participant)
Hacker Fighter - Game-based approach to fight piracy and counterfeiting	September 2015 — August 2016	Office for Harmonization in the Internal Market (OHIM)	Information Technology specialist
QoEViS - Quality of Experience in Video Streaming	July 2014 – July 2015	Instituto de Telecomunicações	Researcher
TRAMANET - Traffic and Trust Management in Peer-to-Peer Networks	January 2008 – June 2011	Fundação para a Ciência e a Tecnologia (FCT)	Researcher
Active Security Mechanisms for Passive Optical Networks (PON) Point-to-Multipoint (P2M) Environment	April 2007 – June 2008	Agência da Inovação (ADI)	Leader of task 2.1

Tasks to be conducted in the frame of the project proposal (timetable)

Months 1–6: Requirement analysis of an e-voting system. Identification and definition of functional and security requirements, system and attack model. Contextualization with the objetives of the tasks.
Design of the Hill cipher crypto-system based on a CSPRNG.

Months 7–18: Proposal of the e-voting system (system components, cryptographic primitives, usage and procedural protocol). Implementation of the prototype.
Implementation of the Hill cipher crypto-system. Comparison of the proposed key matrix generation procedure with other algorithms described in the literature. Testing of the cipher.

Months 19–24: Scientific results will be presented to the public in several ways, through presentations on international and home conferences and papers in journals.

Senior Scientist/ Researcher

Name Surname	**Stefka Bouyuklieva**
Title	Doctor of Science in Mathematics
Position	Full Professor
Address	"T. Tarnovski" 3, 5000, Veliko Tarnovo, Bulgaria
Tel./Fax.	++359 888 131 165
e-mail	stefka@uni-vt.bg

Short CV:

Education:

- Doctor of Sciences, Sofia, June 2008 (Thesis: Self-dual codes and groups of automorphisms).
- Ph.D., Veliko Turnovo University, October 1997 (Thesis: Extremal self-dual codes, Advisor: Prof. Dr. Vassil Yorgov)
- Diploma in Mathematics, M.Sc., Sofia University, July 1988

Working positions:

- Head of Department of Algebra and Geometry, Veliko Tarnovo University, since 2003.
- Professor, Veliko Tarnovo University, since 2012.
- Associate Professor, Veliko Tarnovo University, 2000-2011.
- Assistant Professor, Veliko Tarnovo University, 1992-2000.
- Institute of Mathematics and Informatics, Bulgarian Academy of Sciences -- from September 1988, to February 1992.

Membership in professional associations: Union of Bulgarian Mathematicians

Program committee member:

- International Workshop on Algebraic and Combinatorial Coding Theory, Kranevo, Bulgaria, June 2004.
- International Workshop on Algebraic and Combinatorial Coding Theory, Zvenigorod, Russia, September 2006.
- International Workshop on Algebraic and Combinatorial Coding Theory, Pamporovo, Bulgaria, June 2008.
- International Workshop on Algebraic and Combinatorial Coding Theory, Novosibirsk, RUSSIA, September 2010.
- Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory, Pomorie, Bulgaria, June 2012.
- Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory, Svetlogorsk, Russia, September 2014.
- Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory, Albena, Bulgaria, June 2016.
- Head of the Jury, National Mathematical Olympiad for University Students, Veliko Tarnovo, 2006.
- Member of the Jury, National Mathematical Olympiad for University Students, Sozopol, 2007.
- Member of the Organizing Committee, International Colloquium on Differential Geometry and its Related Fields, Veliko Tarnovo, Bulgaria, September 2010, 2012, 2014, 2016.
- Member of the Jury, National Mathematical Olympiad for University Students, Sofia, 2011.
- Head of the Jury, First National Olympiad on Computer Mathematics for University Students, Gabrovo, 2012.
- Member of the Juri, National Olympiads on Computer Mathematics for University Students, 2013, 2014, 2016.

Scientifically-research fields of interest: Algebraic and Combinatorial Coding Theory, Cryptography, Finite Fields, Number Theory

Scientific papers published in the last 5 years, indicating the impact factor according to JSR database of Thomson Routers (if any) of the journals in which each paper was published

- S. Bouyuklieva and W. Willems, "Singly-even self-dual codes with minimal shadow", IEEE Trans. Inform. Theory, vol. 58, pp. 3856--3860, June 2012. Impact Factor (2012) 3.009
- S. Bouyuklieva and I. Bouyukliev, "An algorithm for classification of binary self-dual codes", IEEE Trans. Inform. Theory, vol. 58, pp. 3933--3940, June 2012. Impact Factor (2012) 3.009

- S. Bouyuklieva, N. Yankov, Jon-Lark Kim, "Classification of binary self-dual [48,24,10] codes with an automorphism of odd prime order", Finite Fields and Their Applications, vol. 18, Issue 6, pp. 1104–1113, November 2012. 5-Year Impact Factor: 1.299, SCImago Journal Rank (SJR): 1.096, Source Normalized Impact per Paper (SNIP): 1.344
- S. Bouyuklieva, I. Bouyukliev and M. Harada, "Some extremal self-dual codes and unimodular lattices in dimension 40", Finite Fields and Their Applications, vol. 21, pp. 67–83, 2013. 5-Year Impact Factor: 1.299, SCImago Journal Rank (SJR): 1.096, Source Normalized Impact per Paper (SNIP): 1.344
- Stefka Bouyuklieva, Javier de la Cruz, Wolfgang Willems, "On the automorphism group of a binary self-dual [120,60,24] code", Applicable Algebra in Engineering, Communication and Computing, vol. 24, pp 201-214, August 2013. SJR – 2015 - 0.354, 5 Year Impact Factor – 2015 – 0.722.
- S. Bouyuklieva, W. Willems, N. Yankov, On the automorphisms of order 15 for a binary self-dual [96,48,20] code, Designs, Codes and Cryptography, vol. 79, pp. 171-182, April 2016. Impact Factor 0.781
- S. Bouyuklieva and W. Willems, "Connections between different types of binary self-dual codes", Proceedings of the International Workshop ACCT, Pomorie, Bulgaria, pp. 111-116, 2012.
- S. Bouyuklieva, "Applications of the Gaussian integers in coding theory", Prospects of Differential Geometry and its Related Fields, World Scientific, Proceedings of the 3rd International Colloquium on Differential Geometry and its Related Topics, Veliko Tarnovo, Bulgaria, pp. 39-49, 2012.
- S. Bouyuklieva and I. Bouyukliev, "On the binary quasi-cyclic codes", Proceedings of the International Workshop OCRT, Albena, Bulgaria, pp. 59-64, 2013.
- S. Bouyuklieva and N. Yankov, "Some binary self-dual codes having an automorphism of order 15", Proceedings of the International Workshop ACCT, Svetlogorsk, Russia, pp. 103-108, 2014.
- S. Bouyuklieva, R. Russeva and E. Karatash, "On some automorphisms of order 3 of the extremal binary codes", Fifteenth International Workshop ACCT, Albena, Bulgaria, 18-24 June 2016.
- D. Bikov, I. Bouyukliev and S. Bouyuklieva, "S-boxes from binary quasi-cyclic codes", Fifteenth International Workshop ACCT, Albena, Bulgaria, 18-24 June 2016.

Participation in research projects

Project title	Period	Financed by	Role in the project (PI or participant)
Algebraic and geometric models in coding theory and cryptography and their realizations with parallel algorithms.	**2014-2016**	**VTU**	**PI**
Algebraic, geometric and stochastic applications in information security.	**2010-2012**	**VTU**	**PI**
Development of new methods, models, algorithms and programs for linear and additive codes, used for information security.	**2008-2009**	**VTU**	**PI**
Mathematical foundation of informatics: algorithms, information protection, geometrical models.	**2007**	**VTU**	**PI**
Self-orthogonal codes and groups of automorphisms	**2003-2005**	**Bulgarian Scientific Fond**	**participant**

Tasks to be conducted in the frame of the project proposal (timetable)

Months 1–6: She will participate in obtaining an optimal 8x8 S-boxes from binary quasi-cyclic codes.

Months 7–18:

- Paralel realisation of fast algorithms for different metrics for S-boxes
- Obtaining of optimal 8x8 S-boxes from small quasigroups of order 4 or 8.

Months 19–24: Scientific results will be presented to the public in several ways, through presentations on international and home conferences and papers in journals.

Senior Scientist/ Researcher

Name Surname	**Natasha Stojkovikj**
Title	PhD of computer science
Position	Assistant professor, Faculty of Computer Science, Goce Delcev University – Shtip
Address	Krste Misirkov, Shtip,Macedonia
Tel./Fax.	00 389 32 550 113
e-mail	natasa.maksimova@ugd.edu.mk

Short CV:
Education:

- PhD of Computer science, Faculty of Computer science and Engineering
- "St. Cyril and Methodius" University Skopje, Macedonia,2015.
- M.Sc of Computer science, Institute of Informatics, Faculty of Natural Sciences and Mathematics "St. Cyril and Methodius" University Skopje, Macedonia,2009.
- B.Sc of of Computer science, Institute of Informatics, Faculty of Natural Sciences and Mathematics "St. Cyril and Methodius" University Skopje, Macedonia,2002.
- Professor of Mathematics, Institute of Mathematics, Faculty of Natural Sciences and Mathematics "St. Cyril and Methodius" University Skopje, Macedonia ,2000

Working positions:

- Assistan Professor, Faculty of Computer Science, Goce Delcev University, Shtip, 2016-
- Assistant, Faculty of Computer Science, Goce Delcev University, Shtip, 2010-2016.
- Junior assistant, Faculty of Computer Science, Goce Delcev University, Shtip, 2007-2010.
- Senior programmer, Maksystem, Skopje, 2003 – 2008.

Scientifically-research fields of interest:

- Relability of networks
- Modeling and simulation
- Graph theory
- Operations research
- Probability and statistics

Scientific papers published in the last 5 years, indicating the impact factor according to JSR database of Thomson Routers (if any) of the journals in which each paper was published

[19] M.Mihova, N.Stojkovikj, M.Jovanov анд E.Stankov “Maximal Level Minimal Path Vectors of a Two-terminal Undirected Network”, *IEEE Transactions on Reliability*, Vol. 65, Issue 1, ISSN 0018-9529, pp. 282 – 290,2016 (IF 2.278).

[20] M.Mihova, N.Stojkovikj, M.Jovanov анд E.Stankov “On Maximal Level Minimal Path Vectors of a Two-Terminal Network”, Olympiads in Informatics, 2014, Vol. 8, 133–144, 26th International Olympiad in Informatics,Taipei, Taiwan.

[21] Mihova, M, Maksimova N "Estimation of minimal path vectors of multi state two terminal networks with cycles control", Mathematica Balkanica, Vol. 25 , Fasc 4, ISSN 0205-3217, pp. 437-447,2011

[22] M.Mihova, N. Maksimova, Kj. Gjorgjiev, “Optimal improving of network reliability: Reliability of the improved network”, Proceedings of the IV Congress of the Mathematicians of Republic of Macedonia, Skopje 2011 (247-257)

[23] M. Mihova and N.Stojkovikj, “Simulating the profit of work on multi state two terminal transportation system”, Proceedings of the 9th International Conference for Informatics and Information Techology (CIIT 2012),

[24] Mihova, M, Ilijoski B, Stojkovic N. "The Optimization of the Profit of a Parallel System with Independent Components and Linear Repairing Cost" , 2012 Web proceedings of ICT Innovations 2012 , Ohrid,ISSN 1857-7288, pp.507-516

[25] Martinovska, C, Maksimova N, Gacovski Z, "A Fuzzy Based Approach to Selecting Successful Contractor for Public Procurement", The 2nd International Conference, Science and technology in the Context of Sustainable, Ploesti, Romania,2011.

[26] Lazarova, L, Miteva, M, Stojkovic N. "The Black-Scholes model and valuation of the European Call option", Yearbook-Faculty of Computer Science 2013 . ISSN 1857-8691,pp 209-220

[27] N Stojkovik, L Lazarova, M Miteva.”Calculation of multi-state two terminal reliabilty” Yearbook-Faculty of Computer Science 2014 . ISSN 1857- 8691, pp 5-10

[28] A.Stojanova, N.Stojkovic and Dusan Bikov “Java IDEs for learning and understanding

object oriented language", Yearbook-Faculty of Computer Science 2012 . ISSN 1857-8691,pp 232-240.
[29] Maksimova N, Suteva G, Jovanov V,"Fractions and Operation with fractions, Using of Interactive Table", Proceeding of 11th International Education Technology Conference (IETC), Istanbul, May 2011.
[30] Stojanova, Aleksandra and Stojkovic, Natasa and Bikov, Dusan, "*Tools for software visualization.*", Yearbook of the Faculty of Computer Science, 3 (3). pp. 47-55. ISSN 1857- 8691, 2015
[31] Natasa Stojkovic, Aleksandra Stojanova, Dusan Bikov, Gabriela Suteva: „Children dependence from internet" In proceedings of III Scientific – proffesional meeting „Education in 21st century" 2011, Bitola, ISBN 978-608-4616-24-5
[32] Natasa Stojkovic, Aleksandra Stojanova, Dusan Bikov, Gabriela Suteva: „Training using computer games" III Scientific – professional meeting In proceedings of III Scientific – professional meeting „Education in 21st century" 2011, Bitola, ISBN 978-608-4616-24-5
[33] Stojanova, Aleksandra and Zlatanovska, Biljana and Kocaleva, Mirjana and Miteva, Marija and Stojkovic, Natasa (2016) "Mathematica" as a tool for characterization and comparison of one parameter families of square mappings as dynamic systems. In: ITRO 2016, 10 June 2016, Zrenjanin, Serbia.
[34] Zlatanovska, Biljana and Stojanova, Aleksandra and Kocaleva, Mirjana and Stojkovic, Natasa and Krstev, Aleksandar (2016)"Mathematica as program support in the integral calculations", In: TIO 2016 - Technics and informatics in education, 28-29 May 2016, Čačak, Serbia.
[35] Stojkovic, Natasa and Stojanova, Aleksandra and Kocaleva, Mirjana and Zlatanovska, Biljana (2016) ", In: ITRO 2016, 10 June 2016, Zrenjanin, Serbia.
[36] Stojanovski, Strasko and Stojkovic, Natasa and Ananiev, Jovan and Kocaleva, Mirjana and Stojanova, Aleksandra and Zlatanovska, Biljana (2016) ,", In: ITRO 2015, 10 June 2016, Zrenjanin, Serbia.

Participation in research projects

Project title	Period	Financed by	Role in the project (PI or participant)
Development of novel techiques for cooperative localization and mapping using mobile robots and their application in precise agriculture.	2015-2018	UGD	participant

Tasks to be conducted in the frame of the project proposal (timetable)

Months 1–6: She will take a part in the development of algorithms for finding minimal path vectors in two terminal network with lower time complexity from existing algorithms

Months 7–18: She will take part in the implementation of algorithms for execution time comparision in two terminal multi-state networks

Months 19–24: Writing of scientific papers with obtained scientific results, and their submission to journals or presentation to conferences (altrough publishing of the partial project results will be conducted during the whole project duration).

Researcher (*use separate sheets for each participant***)**

Name Surname	**Done Stojanov**
Title	Doctor of technical sciences (Computer science)
Position	Research and teaching assistant
Address	Ul. Krste Misirkov bb. 2000 Stip, Macedonia
Tel./Fax.	00 38932550134
e-mail	done.stojanov@ugd.edu.mk

Short CV:

Born on 15.01.1985 in Strumica. In 2008 has received bachelor degree from the Faculty of electrical engineering and information technologies in Skopje. In 2010 became master on ***Software engineering***, defending master thesis: ,,***Bioinformatical analysis of existing and new models of proteins***". On 7.12.2015 became doctor of computer science, defending PhD thesis: ,,***Algorithms for alignment and searching of DNA sequences***". On 7th of Март 2016 he is elected for Assistant Professor at the Faculty of computer science – University ,,Goce Delcev" Stip.

Scientific papers published in the last 5 years, indicating the impact factor according to JSR database of Thomson Routers (if any) of the journals in which each paper was published

[1] Stojanov, Done and Madevska Bogdanova, Ana and Orzechowski, Tomasz (2016) *TMO: time and memory optimized algorithm applicable for more accurate alignment of trinucleotide repeat disorders associated genes.* Biotechnology & Biotechnological Equipment, 30 (2). pp. 388-403. ISSN 1310-2818 (**IF=0,373**)

[2] Stojanov, Done and Koceski, Saso and Mileva, Aleksandra and Koceska, Natasa and Martinovska Bande, Cveta (2014) *Towards computational improvement of DNA database indexing and short DNA query searching.* Biotechnology & Biotechnological Equipment, 28 (5). pp. 958-967. ISSN 1310-2818 (**IF=0,373**)

[3] Stojanov, Done and Koceski, Saso and Mileva, Aleksandra (2013) *FLAG: Fast Local Alignment Generating Methodology.* Romanian Biotechnological Letters, 18 (1). pp. 7881-7888. ISSN 1224 – 5984 (**IF=0,404**)

[4] Kocaleva, Mirjana and Stojanov, Done and Stojanovic, Igor and Zdravev, Zoran (2016) Pattern Recognition and Natural Language Processing: State of the Art. TEM Journal, 5 (2). pp. 236-240. ISSN 2217-8309 / 2217-8333 (Online)

[5] Stojanov, Done and Koceski, Saso (2014) Topological MRI Prostate Segmentation Method. Proceedings of the 2014 Federated Conference on Computer Science and Information Systems, 2. pp. 219-225. ISSN 2300-5963

[6] Stojanov, Done and Martinovska, Cveta (2014) Improved alignment of homologous DNA sequences. Annals of West University of Timişoara, ser. Biology, 16 (2). pp. 97-106. ISSN 1453-7680

[7] Stojanov, Done (2012) IC: Intelligent Clustering, a new time efficient data partitioning methodology. International Journal of Computer Science and Information Technologies, 3 (5). pp. 5065-5067. ISSN 0975-9646

[8] Stojanov, Done and Mileva, Aleksandra and Koceski, Saso (2012) A new, space-efficient local pairwise alignment methodology.Advanced Studies in Biology, 4 (2). pp. 85-93. ISSN 1313-9495

Participation in research projects

Project title	Period	Financed by	Role in the project (PI or participant)
Development of novel algorithms and software library for biomedical engineering application	2013-2015	University ,,Goce Delcev" - Stip	Young researcher

Tasks to be conducted in the frame of the project proposal (timetable)

Months 1–6: He will participate in acquisition of security data from log files and different scannings

Months 7–18: He will participate in analysis of obtained security data with different techniques from Artifical Intelligence

Months 18–24: Writing of scientific papers with obtained scientific results, and their submission to journals or presentation to conferences (altrough publishing of the partial project results will be conducted during the whole project duration).

Junior researcher (*use separate sheets for each participant, minimum 2 participants***)**

Name Surname	**Dusan Bikov**
Title	**MSc**
Position	**Teaching assistant**
Address	**str. „Krste Misirkov“ No.10-A, Stip, R.Macedonia**
Tel./Fax.	**032 550 135**
e-mail	**dusan.bikov@ugd.edu.mk**

Short CV:

MSc Dusan Bikov is born on 06.01.1987 in Stip, where he finished his primary and secondary education with excellent success. In the academic 2005/2006 year he enrolled in the studies of Faculty of Mathematics and Computer Science, Veliko Tarnovo, Bulgaria, department of Computer Science. He graduated in July 2009. In September he enrolled postgraduate studies at the same faculty. Graduated in 2011, defending the master thesis in the field of cryptography with title “Analysis, simulation and application of cryptography on an elliptic curve in wireless sensor networks” under the supervision of Prof. Stefka Bouyuklieva. In December, 2012 the title of Dusan’s PhD thesis “Algebraic Cryptanalysis and design of cryptographic primitives” was accepted at the Faculty of Mathematics and Computer Science in Veliko Tarnovo, under the supervision of p Prof. Stefka Bouyuklieva. From September, 2011 he works as teaching assistant at the Faculty of Computer Science in Stip.

Scientific papers published in the last 5 years, indicating the impact factor according to JSR database of Thomson Routers (if any) of the journals in which each paper was published

1. **D. Bikov**, I. Bouyukliev, S. Bouyuklieva, S-Boxes from Binary Quasi-Cyclic Codes, Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory, Albena, (2016)
2. **D. Bikov**, I. Bouyukliev, A. Stojanova, Benefit of Using Shared Memory in Implementation of Parallel FWT Algorithm with CUDA C on GPUs, Proceedings of 7th International Conference Information Technologies and Education Development, Zrenjanin, Serbia, (2016) pp.250-256, ISBN 978-86-7672-285-3
3. **Dusan Bikov**, Aleksandra Stojanova: „Using gpu matrix vector multiplication for computing walsh spectra". ETAI 2015, Ohrid
4. Iliya Bouyukliev, **Dusan Bikov**: „Applications of the binary representation of integers in algorithms for boolean functions". SMB 2015, Kamchia
5. **Dusan Bikov**, Stefka Bouyuklieva, Aleksandara Stojanova,: “S-boxes – parameters, characteristics and classifications”, Faculty of Computer Science, UGD Yearbook - Vol 1, No 2, 2013, pp. 47-52, ISSN: 1857- 8691, Stip, Macedonia
6. **Dusan Bikov**, Stefka Bouyuklieva, Aleksandra Stojanova: “Wireless Network Security and Cracking Security Key”, Jubilee Scientific Conference "50 Years University" St. Cyril and Methodius ", 2013, Veliko Tarnovo

Participation in research projects

Project title	Period	Financed by	Role in the project (PI or participant)
Sensor networks for monitoring and controlling vine production	**2014-2016**	**UGD**	**participant**
Algebraic and geometric models in coding and cryptography and their realization through parallel algorithms, VTU Science Fund under Contract RD-09-422-13/09.04.2014	**2014-2016**	**VTU - BG**	**participant**

Title of the MSci or PhD theses

“***Algebraic Cryptanalysis and design of cryptographic primitives***” – PhD thesis

Tasks to be conducted in the frame of the project proposal (timetable)

Months 1–6: He will participate in obtaining an optimal 8x8 S-boxes from binary quasi-cyclic codes.

Months 7–18:

- Paralel realisation of fast algorithms for different metrics for S-boxes
- Obtaining of optimal 8x8 S-boxes from small quasigroups of order 4 or 8.

Months 19–24: Scientific results will be presented to the public in several ways, through presentations on international and home conferences and papers in journals.

Junior researcher (*use separate sheets for each participant***)**

Name Surname	**Goran Mitkovski**
Title	BSc in Computer science
Position	Student on postgraduate studies
Address	Gjorche Petrov bb, Kumanovo
Tel./Fax.	077 984 779
e-mail	goran_mitkovski@yahoo.com

Short CV:
Education and Professional Development:

2006 - 2012 **Bachelors Degree in IT Engineering**
St. Cyril and Methodius University, Skopje, Macedonia
Faculty of Mathematics and Natural Sciences
Department: Computer Architectures and Networks

2013- present **Master studies in IT**
Goce Delcev University, Shtip, Macedonia
Faculty of Computer Science
Department: Software Engineering

2008 – 2010 **Certified IT Technician**
Cisco Networking Academy, Skopje, Macedonia
Courses in:

- CCNA Exploration: Network Fundamentals
- CCNA Exploration: Routing Protocols and Concepts
- CCNA Exploration: LAN Switching and Wireless
- CCNA Exploration: Accessing the WAN
- CCNA Exploration: Fundamentals of Wireless LANs

Working Experience:

2010 – 2010 Company: Volvo Makedonija – Skopje
3 months of practice as receptionist and spare part responsibilities.

2011 – present Software developing in PHP CodeIgniter framework as freelancer.

2011 – 2014 Company: Pro Sound – Skopje
Responsibilities: Maintenance and management of computer systems and audio equipment.

2014 – present Company: K3 Television –Kumanovo
Responsibilities: Maintenance and management of IT sector and technical lead.

Title of the MSci or PhD theses
Development of anti-Steganography techniques for digital images

Tasks to be conducted in the frame of the project proposal (timetable)

Months 1–6: Analysis of different techniques for data hiding in digital images

Months 7–18: Design and development of anti-steganographic techniques for digital images and their implementation as a tools.

Months 19–24: Writing of scientific papers with obtained scientific results, and their submission to journals or presentation to conferences. We expect in the frame of this project to obtain most of the results needed for his master thesis.

Junior researcher (*use separate sheets for each participant***)**

Name Surname	**Biljana Dimitrova**
Title	BSc in Electrical Engineering and Information Technology
Position	Student on postgraduate studies
Address	Ul. Krste Misirkov bb. 2000 Stip, Macedonia
Tel./Fax.	+389 78 397 736
e-mail	biljana.dimitrova@ugd.edu.mk

Short CV:

Biljana Dimitrova is a student on postgraduate studies in Information Technology and Systems at the Faculty of Informatics at the University Goce Delchev - Stip. She graduated in the field of Telecommunications in Faculty of Electrical Engineering and Information Technology at the University Ss. Cyril and Methodius - Skopje in 2010. Since 2010 she worked as a specialist in the customer support department for electronic index of Goce Delchev University - Stip, which is included in the design and production of complex system for complete electronic administration of students and personnel. Field of her interests are information systems, cryptography, steganography, security of information systems, and security of networks. Currently is working on researching on methods of hiding the data in the new protocols for transfer web content.

Title of the MSci or PhD theses

Data Hiding in the new protocols for transfer of web contents

Tasks to be conducted in the frame of the project proposal (timetable)

Months 1–6: Finding covert channels in HTTP/2.0

Months 7–18: Finding covert channels in QUIK

Months 19–24: Writing of scientific papers with obtained scientific results, and their submission to journals or presentation to conferences. We expect in the frame of this project to obtain most of the results needed for his master thesis.

Истражувачка инфраструктура

Истражувачки капацитети/опрема

Дадете детален опис на инфраструктурата и опремата која ќе биде на располагање на истражувачите во институциите кои учествуваат во проектот

На Факултетот за компјутерски науки на Универзитетот "Гоце Делчев" има шест целосно опремени компјутерски лаборатории кои се користат за истражување и настава.
Овој факултет ја има на располагање и следнава мрежна опрема која може да се користи за потребите на овој проект:

1-Cisco Catalyst Core Switch 4507R; 5 - Cisco L2/L3 Switch 3560G 48p PoE; 2 - Cisco L2 Switch 2960 48p PoE; 1-Cisco ASA 5505; 1-Cisco Router 2811; 1-Cisco Wireless LAN Controller 4400;1-Cisco NAC Guest Server; 10 - Cisco WiFi Aironet 1131 Access Points; 1 - Cisco DMM server; 2-Cisco DMP 4310G;1-Extreme Networks L2/L3 x450e 48p PoE Switch;2 -3Com L2/L3 4500G 48p PoE Switch.

Покрај тоа, следната инфраструктура за складирање на податоци ќе се користи за чување на добиените податоци: IBM x3550 M3; IBM x3690 X5; IBM DS4800 Storrage; IBM TS3100 Tape Library; EMC Clarion AX-4 Storrage
Со оглед на географска оддалеченост меѓу партнерите во проектот; за да се олесни комуникацијата, да се обезбедат постојани контакти меѓу учесниците во проектот и да се намалат трошоците за патувања и комуникациските трошоци, следнава видео-конференциска опрема ќе биде ставена на располагање за целите проектот: Polycom VSS2000; Polycom MCU RMX2000; Polycom GK CM5000; Polycom HD 7001 endpoints.

Research infrastructure

Facilities available in the Researchers Team's laboratory (if applicable)

Provide a detailed list of the infrastructure and equipment available and necessary for the proposed research

The Faculty of Computer science at the University "Goce Delcev" has six fully equipped computer laboratories used for research and teaching.

The faculty has on its disposal the following network equipment which may be used in the eHealth social network development, evaluation and simulations:

1-Cisco Catalyst Core Switch 4507R; 5 - Cisco L2/L3 Switch 3560G 48p PoE; 2 - Cisco L2 Switch 2960 48p PoE; 1-Cisco ASA 5505; 1-Cisco Router 2811; 1-Cisco Wireless LAN Controller 4400;1-Cisco NAC Guest Server; 10 - Cisco WiFi Aironet 1131 Access Points; 1 - Cisco DMM server; 2-Cisco DMP 4310G;1-Extreme Networks L2/L3 x450e 48p PoE Switch;2 -3Com L2/L3 4500G 48p PoE Switch.

Moreover, the following data storage equipment will be used in the development process and for storage of measured sensor data: IBM x3550 M3; IBM x3690 X5; IBM DS4800 Storrage; IBM TS3100 Tape Library; EMC Clarion AX-4 Storrage

Considering the geographical distance between project partners; to facilitate permanent contacts between the project participants and to reduce the travel and communication costs, the following video-conferencing equipment will be at disposal for the project purposes: Polycom VSS2000; Polycom MCU RMX2000; Polycom GK CM5000; Polycom HD 7001 endpoints.

It has on its disposal several smart phones with developer licences, equipped with different operating systems (Andriod, Windows Phone 7, iOS).

Финансиски план:

Трошоци (во МКД)

Бр.	Вид на трошок	Прва година	Втора година	Вкупно
420	Патување во земјата и странство	100.000	100.000	200.000
426	Семинари и конференции	70.000	70.000	140.000
480	Купување на опрема	30.000	30.000	60.000
ВКУПНИ ТРОШОЦИ		200.000	200.000	400.000
Лабораторија				
Лабораториски материјал (ситен лабораториски инвентар)				

Financial Plan

Expenditures (in MKD)

No.	Purpose	First year	Second year	Overall
420	Travel at home and abroad	100.000	100.000	200.000
426	Seminars, conferences	70.000	70.000	140.000
480	Equipment buying	30.000	30.000	60.000
TOTAL COSTS		200.000	200.000	400.000
Laboratory				
Small laboratory equipment				

Анекс 1

Наслов на проектот:
Развој на безбедни и надежни техники за податочната комуникација
Проект Бр: _____

Согласност на истражувачите и институциите вклучени во проектот (од сите истражувачи вклучени во проектот - по потреба да се зголеми бројот на соодветните полиња)**:**

Главен истражувач: (Име, потпис и датум)	**проф. д-р Александра Милева**
Истражувач: (Име, потпис и датум)	**доц. д-р Pedro R. M. Inácio**
Истражувач: (Име, потпис и датум)	**проф. д-р Stefka Bouyuklieva**
Истражувач: (Име, потпис и датум)	**доц. д-р Наташа Стојковиќ**
Истражувач: (Име, потпис и датум)	**доц. д-р Доне Стојанов**
Млад истражувач: (Име, потпис и датум)	**м-р Душан Биков**
Млад истражувач: (Име, потпис и датум)	**Горан Митковски**
Млад истражувач: (Име, потпис и датум)	**Билјана Димитрова**
Раководител на институцијата на главниот истражувач	**Име и презиме, звање: Цвета Мартиновска Банде, ред. проф.** **Институција: Факултет за информатика, Универзитет “Гоце Делчев” - Штип** **Потпис и печат**
Раководител на институцијата на останатите истражувачи	**Име и презиме, звање: Цвета Мартиновска Банде, ред. проф.** **Институција: Факултет за информатика, Универзитет “Гоце Делчев” - Штип** **Потпис и печат**

Head of the institution of the other researchers	**Name and surname, title:**
	Institution: Faculty of Engineering, University of Beira Interior, Portugal
	Signature and seal
Head of the institution of the other researchers	**Name and surname, title: Miroslav Galabov, Assoc. Prof. Dr.**
	Institution: Faculty of mathematics and informatics, University of Veliko Turnovo "St Cyril and St. Methodius" - Veliko Turnovo, Bulgaria
	Signature and seal

Анекс 2

И з ј а в а

Јас Александра Милева како главен истражувач, под морална и материјална одговорност изјавувам дека предложениот научен проект не се финансира од други извори на финансирање.

Датум	**Потпис**