Project ON144018
"Advanced Methods in Cryptology and Information Processing"

Projekat ON144018
"Nove Metode u Kriptologiji i Procesiranju Informacija"

REZIME OSNOVNIH REZULTATA PROJEKTA TOKOM 2006. i 2007. GODINE

Planirana osnovna namera ovog projekta je da pruži nove doprinose metodama i tehnikama za procesiranje informacija sa posebnim fokusom na zaštitu informacija. Saglasno navedenom, osnovni istraživački pravci projekta su: (a) kriptologija, (b) modelovanje i kodovanje informacija, (c) bezbednost informacija i (d) korespodentni pravci primenjene matematike. Planirani osnovni cilj projekta je da pruži kolekciju novih rezultata u domenima (a)-(d) i da ostvari njihovo publikovanje, pre svega u za oblast najznačajnijim naučnim časopisima, i prikazivanje na različitim medjunarodnim naučnim forumima.

Aktivnosti na projektu tokom 2006. i 2007. godine su realizovane u okvirima planiranih domena i u punoj saglasnosti sa planiranim ciljevima. Niz rezultata projekta je objavljen tokom 2006. i 2007. godine u formi radova u medjunarodnim i vodećim medjunarodnim časopisima i u drugim za oblast projekta značajnim publikacijama.

Objavljeno je više od 70 rezulta od čega više od 35 radova kategorije rada u časopisu.

Ostvareno je i objavljeno:
- 13 rezultata kategorije rada u vodećim medjunarodnim časopisima (kategorija R51);
- 17 rezultata kategorije rada u medjunarodnim časopisima (kategorija R52);
- 3 rezultat u formi poglavlja u monografiji medjunarodnog značaja (R22);
- 7 rezultata rada u nacionalnom casopisu
- 1 rezultat kategorije "magistarski rad";
- više od 30 rezultata u drugim publikacijam (zbornici medjunarodnih i nacionalnih konferencija i drugo).

Navedeno direktno pokazuje veoma visok kvalitet i nivo ostvarenih rezultata i predstavlja respektivnu osnovu za dalje aktivnosti.

Značaj pravaca unutar kojih su predmeti istrazivanja na projektu ilustruje i činjenica da se oni nalaze medju pravcima dve veoma ugledne medjunarodne asocijacije IACR (International Association for Cryptologic Research) i IFIP (International Federation for Informnation Processing) koje su nosioci većeg broja eminentnih medjunarodnih publikacija i konferencija.

Takodje se ukazuje da značaj ostvarenih rezultata direktna proizilazi i iz značaja procesiranja i zaštite informacija u kontekstu informacionih tehnologija i informacionog društva. Očekuje se da odredjeni rezultati projekta budu osnova za razvoj odredjenih komponenti za efikasne sisteme za zaštitu informacija i obradu odredjenih podataka.

Posebno se ukazuje na ostvarenu veoma intenzivnu medjunarodnu naučnu saradnju sa sledećim institucijama:
- Research Center for Information Security, National Institute AIST, Tokyo, Japan,
- University of Exeter, Department of Computer Science, Exeter, U.K.
- University of Tokyo, IIS, Japan
- Centre for Image Analysis, SLU, Uppsala, Sweden
- University of Hawaii, Department of Electrical Engineering, Honolulu, USA

Navedene medjunarodne saradnje su rezultovale u nizu zajedičkih radova.

REALIZACIJA CILJEVA ISTRAŽIVANJA U 2006. i 2007. GODINI.

Najznačajniji rezultati projekta ostvareni su u domenima kriptologije/informacione-bezbednosti i modelovanja/kodovanja informacija.

U nastavku se daje sumarni prikaz najznačajnijih rezultata projekta grupisanih po predmetnim oblastima istraživanja.

I. KRIPTOLOGIJA i BEZBEDNOST INFORMACIJA

Ostvareno je i objavljeno:
- 6 rezultata kategorije rada u vodećim medjunarodnim časopisima (kategorija R51);
- 8 rezultata kategorije rada u medjunarodnim časopisima (kategorija R52);
- 1 rezultat u formi poglavlja u monografiji medjunarodnog značaja (R22);
- 1 rezultat kategorije "magistarski rad";
- 30 rezultata u drugim publikacijam (nacionalni časopisi, zbornici medjunarodnih i nacionalnih konferencija i drugo).

Rezultati ostvareni u domenima kriptologije i bezbednosti informacija su u okvirima sledećih osnovnih pravaca:
- Nove metode i tehnike za analizu osnovnih kriptografskih komponenata;
- Novi pristupi za dizajn odredjenih šifarskih metoda za zaštitu tajnosti podataka;
- Nove tehnike za upravljanje kriptografskim ključevima;
- Primene kritpografskih metoda za zaštitu podataka u medicinskim informacionim sistemima.

U nastavku se ukazuje na najznačajnije partikularne rezultate ostvarene u okvirima navedenih pravaca.

U domenu novih metoda i tehnika za analizu osnovnih kriptografskih komponenata, razvijene su i objavljene:
- Nove analize klase metoda zasnovanih na dekodovanju binarnih blok kodova koje su opšti alat za procenu kriptografske sigurnosti odredjenih generatora binarnih pseudoslučajnih nizova;
- Nove tehnike zasnovane na rešavanju predefinisanih konzistentnih nelinearnih algearskih jednačina nad GF(2) i probabilističkih predefinisanih konzistentnih linearnih jednačina nad GF(2) za procenu kriptografske sigurnosti nekih klasa generatora pseudoslučajnih binarnih nizova i protokola za autentifikaciju na bazi LPN problema;
- Nove tehnike za procenu nivoa sigurnosti odredjenih klasa metoda za distribuciju kriptografskih ključeva; Ove tehnike se zasnivaju na rodjendanskom paradoksu i generalisanom pristupu za rešavanje nelinearnih jednačina na bazi vremensko-memorijskih kompromisa (trgovina); Pokazane su kriptografske slabosti nekih tehnika za distribuciju kriptografskih ključeva zasnovanih na grafovima tipa drveta i metodama za pokrivanje podskupova.

U domenu novih pristupa za dizajn odredjenih šifarskih metoda za zaštitu tajnosti podataka pokazana je i objavljena matematička (informaciono-teorijska) osnova za ostvarivanje visoke sigurnosti zaštite tajnosti podataka u odredjenim šifarskim sistemima zasnovanim na kvantnim (fotonskim) tehnikama. Predloženo ostvarivanje visoke sigurnosti zasnovano je na matematički optimizovanoj maksimizaciji efekata kvantnih šumova primenom prilagodjenih tehnika kodovanja.

U domenu novih tehnika za upravljanje kriptografskim ključevima razvijeni su i objavljeni:
- Novi metodi za upravljanje primenom koncepta vremenskog ograničavanja važnosti vezanog za grafovske strukture tipa binarnog drveta;
- Novi pristupi za distribuciju ključeva na bazi hibridnih sistema sa statičkim i dinamičkim elementima.

II. MODELOVANJE i KODOVANJE INFORMACIJA.

Ostvareno je i objavljeno:
- 7 rezultata kategorije rada u vodećim medjunarodnim časopisima (kategorija R51);
- 8 rezultata kategorije rada u medjunarodnim časopisima (kategorija R52);
- 2 rezultat u formi poglavlja u monografiji medjunarodnog značaja (R22);
- 1 rezultat u zborniku medjunarodne konferencije.

Istraživacke aktivnosti vezane za probleme digitalne analize slike rezultovale su u sledećem. Definisano je nekoliko novih deskriptora planarnih oblika (konveksnost, izduženost, orijentabilnost) u cilju omogućavanja efikasnijeg klasifikovanja i prepoznavanja realnih objekata predstavljenih na digitalnoj slici. Kreirani su i algoritmi za efikasno računanje definisanih deskriptora. Pored tačnog računanja novodefinisanih deskriptora posmatrani su i postupci za njihovu približnu ocenu. Data su neka od rešenja za računanje izduženosti i orijentacije oblika čiji pojedini delovi nisu "vidljivi" na slici (zbog preklapanja sa drugim objektima ili zbog slabog kvaliteta slike, recimo). Dobijeni su i obećavajući početni rezultati u radu sa objektima koji se, po svojoj prirodi, sastoje od više nepovezanih komponenti (grupa ljudi, jata ptica, itd.). Dobijena

teoretska rešenja su verifikovana na širokoj klasi primera: od klasifikacije mikroorganizama pa do, recimo, personalne identifikacije uz pomoć rukopisa (potpisa).

Matematički alat razvijen za potrebe rešavanja problema iz obrade i analize digitalne slike, pokazao se vrlo primenljivim i u karakterizaciji takozvanih "threshold" funkcija koje se intenzivno koriste u teoriji neuralnih mreža. Precizno je opisan skup diskretnih momenata koji jednoznačno karakterišu multi-linearne threshold funkcije. Iz tako dobijene karakterizacije izvedene su ocene za broj multilinearnih threshold funkcija u zavisnosti od broja korišćenih threshold nivoa, dimenzije posmatranog prostora i broja dopuštenih vrednosti za promenljive.

Iako motivisani vrlo praktičnim problemima, neki od problema vezanih za ocenu kapaciteta digitalnih slika date veličine, ili pak problema vezanih za ocenu zavisnosti postignute preciznosti u funkciji rezolucije analizirane slike, pokazali su se kao teški, ali i interesantni, matematički problemi. Neke od dobijenih ocena vezane za digitalne krugove popravljaju prethodno poznate rezultate, dok neki od rezultata daju prve netrivijalne ocene vezane za broj različitih konfiguracija koje nastaju digitalizacijom realnih krugova u proizvoljnom položaju u odnosu na digitalizacionu rešetku.

U oblasti modelovanja za računarske obrade slike u fokusu su bila istraživanja koja se odnose na fazi-reprezentacije digitalnih objekata. Predložen je novi skup deskriptora oblika prilagodjen fazi-segmentovanim oblicima. Razvijena je metoda defazifikacije zasnovana na minimizaciji rastojanja izmedju fazi-skupova, pri čemu predložena funkcija rastojanja uzima u obzir i lokalna, i globalna svojstva objekta. Razvijen je algoritam za defazifikaciju - segmentaciju – na povećanoj rezoluciji, što dodatno doprinosi atraktivnosti i primenljivosti ovog postupka. Ispitivana je i primenljivost nekoliko različitih metoda numeričke optimizacije u defazifikaciji. Rad na poboljšanom metodu za estimaciju dužine linije, korišćenjem informacije sadržane u tzv. grey-level reprezentacijama, je u toku.

OSTALI SPECIFIČNI REZULTATI

(1) UČEŠĆA NA MEDJUNARODNIM NAUČNIM SKUPOVIMA

Tokom 2006. i 2007. godine održana su sledeća plenarna predavanja kategorije plenarnog rada po pozivu i tutorijala:

[1] M. Mihaljević, "Decimation Based Correlation and Algebraic Attacks and Design of Boolean Functions", Invited Plenary Talk, Advanced Study Institute on Boolean Functions in Cryptology and Information Security, Moscow, Sept. 2007 (to appear as a book\chapter in IOS Press Book Series "NATO Security through Science Series: Information and Communication Security", Eds. B. Prenell and O. Logachev; http://www.iospress.nl/)

[2] M. Mihaljević, "Certain Elements for Security Evaluation of Stream Ciphers",

Plenary Invited Talk by Cryptology Research Society of India,
National Workshop on Cryptology, India, Mumbai-Pune, 08-10 September 2006.

[3] M. Mihaljević, "An Algorithm for Solving the LPN Problem and its Application to Security Evaluation of the HB Protocols for RFID Authentication",
Plenary Invited Talk, IPA Cryptography Workshop 2006, Tokyo, Japan, October 4, 2006.

[4] M. Marković, „An Overview of Secure and Authenticated Remote Access to Central Sites," Invited Plenary Talk;
Workshop on Data Access to Micro-Data (WDA), Nuernberg, August 20-21, 2007.

[5] M. Marković, "Data Protection Technics and Cryptographic Protocols in Modern Computer Networks",
Tutorial, 13th International Conference on Telecommunications, ICT 2006,
Madeira, Portugal, May 9-12, 2006.

[6] M. Marković, "Data Protection Techniques, Cryptographic Protocols and PKI Systems in Modern Computer Networks," Tutorial, in Proc. of IWSSIP & EC-SIPMCS 2007 Conference, Maribor, Slovenia, June 26-30, 2007.

[7] M. Marković, „Cryptographic Protocols in Modern Computer Networks – Combining Authentication and Secure Payment," Tutorial,
IAS 2007 – The Third International Symposium on Information Assurance and Security, Manchester, UK, August 29-31, 2007.

Takodje, Miodrag Mihaljević je obavljao dužnost člana programskog komiteta za ISITA2006 (Int. Symp. on Information Theory and Appl.) i SSS2007.

Joviša Žunić je neke od rezultata predstavio na 5 medjunarodnih konferencija.

(2) MEDJUNARODNA SARADNJA

Posebno se ukazuje na ostvarenu veoma intenzivnu medjunarodnu naučnu saradnju sa sledećim institucijama:
- Research Center for Information Security, National Institute AIST, Tokyo, Japan,
- University of Exeter, Department of Computer Science, Exeter, U.K.
- University of Tokyo, IIS, Japan
- Centre for Image Analysis, SLU, Uppsala, Sweden
- University of Hawaii, Department of Electrical Engineering, Honolulu, USA;
- Research Labs, Telecom Italia, Torino, Italija.

Tokom 2006. i 2007. učesnici projekta su realizovali ukupno više od 30 meseci zajedničkih istraživackih aktivnosti u navedenim institucijama sa kojima se ostvaruje medjunarodna saradnja. Posebno se ukazuje da su sve boravke u navedenim institucijama finansirale ove institucije.

Navedene medjunarodne saradnje su rezultovale u više od 20 zajedičkih radova kategorije rada u vodećem medjunarodnom časopisu ili medjunarodnom časopisu.

(3) EDITORSKI I RECENZENTSKI RAD

Učesnici projekta su tokom 2006. i 2007. godine više od 50 puta obavljali recenzentske dužnosti za eminentne medjunarodne časopise i konferencije kao i editorsku dužnost u dva časopisa i članstvo u programskim komitetima prema sledećem (izabrani ilustrativni primeri)

Joviša Žunić je obavljao editorske dužnosti za sledeća dva časopisa:
- Pattern Recognition (Elsevier) i
- IEEE Transactions on Pattern Analysis and Machine Intelligence
- International Journal of Parallel, Emergent and Distributed Systems (Taylor & Francis).

Miodrag Mihaljević je obavljao recenzentske dužnosti za:
- IEEE Transactions on Information Theory (4 recenzije);
- Design, Codes and Cryptography (2 recenzije)
- IEEE Transactions on Computer Aid Design (1 recenzija) ;
- IEEE Communications Letters (7 recenzija)
- Lecture Notes in Coputer Science (11 recenzija)
- IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences (2 recenzije)
- Journal of Systems and Software, Elsevier (1 recenzija)
- Journal of Mathematical Cryptology (1 recenzija)
- recenziranje radova za sledeće medjunarodne konferencije ISITA 2006, IEEE ISIT 2007, IEEE ICC 2007, WCC 2007, ACISP 2007, SSS 2007 (više od 20 radova ukupno)

Nataša Sladoje je obavljala recenzentske dužnosti za:
- Image and Vision Computing, Elsevier (1 recenzija);
- Pattern Recognition Letters, Elsevier (3 recenzije);
- IEEE Trans on Image Processing (2 recenzije);
- Pattern Recognition and Image Analysis, Springer (1 recenzija)

Takodje, Miodrag Mihaljević je obavljao dužnost člana programskog komiteta za ISITA2006 (Int. Symp. on Information Theory and Appl.) i SSS2007 (9th International Symposium on Stabilization, Safety, and Security of Distributed Systems).

(4) PRIMENLJIVOST REZULTATA

Rezultati ostvareni u domenima kriptologije i bezbednosti informacija su od direktnog aplikativnog značaja za procenu kriptografske sigurnosti nekih komponentnih elemenata mehanizama za ostvarivanje bezbednosti informacija i za dizajn nekih usavršenih kriptografskih elemenata.
Kao ilustracija ukazuje se na i sledeće:
- Neki rezultati projekta su bili osnova za aktivnosti na dizajnu mehanizama za bezbednost informacija u okviru FP6 projekta No. 026548, ADHOCSYS i radovi rezultati projekta su bili reference za dokumente ADHOCSYS projekta.
- Neki rezultati projekta su bili reference za FP6 projekat SWEB (Secure, interoperable cross border m-services contributing towards a trustful European cooperation with the non-EU member Western Balkan countries) IST / Specific Targeted Research Project (STREP) IST-2005-044979.
- Neki rezultati projekta su bili polazište za analizu mehanizama sigurnosti u GSM sistemu mobilne telefonije Telekoma Srbije (Ugovor MI-SANU i Telekom Srbija, 2007. godina).

Primenljivost rezultata ostvarenih u domenu modelovanja i kodovanja informacija je velika u oblasti digitalnog procesiranja slika, a kao ilustracija se navodi oblast mdicine, gde postoji sve veća potreba za automatizovanim postupcima za analizu velike količine podataka dobijenih sa savremenih dijagnostičkih uredjaja (CT, MR, PET). Prethodno potvrdjuje i uspešna saradnja na projektu "Medical Imaging and Medical Information Processing" u okviru CEEPUS II programa, koji Nataša Sladoje ima sa kolegama sa nekoliko centralno-evropskih univerziteta.

Lista glavnih rezultata projekta u 2006.-2007. godini

I. Radovi u časopisima

I.1 Publikacije kategorije rada u medjunarodnom i vodećem medjunarodnom časopisu (R52 i R51)

godina 2007.

[1] M. Mihaljević, M. Fossorier and H. Imai,
"Security Evaluation of Certain Broadcast Encryption Schemes Employing a Generalized Time-Memory-Data Trade-Off",
IEEE Communications Letters, vol. 11, no. 12, pp. 988-990, Dec. 2007.
Digital Object Identifier (DOI) 10.1109/LCOMM.2007.071029.
(ISSN 1089-7798; Impact Factor in Year 2005: 1.058
ISI Category: Telecommunications; 15. od 59;
kategorija R51a - 8 bodova)

[2] M. Fossorier, M. Mihaljević and H. Imai,
"Modeling Block Encoding Approaches for Fast Correlation Attack",
IEEE Transactions on Information Theory, vol. 53, no. 12, pp. 4728-4737, Dec. 2007.
DOI 10.1109/TIT.2007.909164
(ISSN 0018-9448; Impact Factor in Year 2005: 2.183
ISI Category: Computer Science; Information Systems; 11. od 83;
kategorija R51a - 8 bodova)

[3] M. Mihaljević,
"Generic framework for the secure Yuen 2000 quantum-encryption protocol employing the wire-tap channel approach",
Physical Review A, vol. 75, pp. 052334_1-5, May 2007.
(ISSN 1050-2947; Impact Factor in Year 2006: 3.047
ISI Category: Physics Atomic; 5. od 31;
kategorija R51a - 8 bodova))

[4] M. Mihaljević, M. Fossorier and H. Imai,
"Birthday Paradox Based Security Analysis of Certain Broadcast Encryption Schemes",
IEICE Transactions on Fundamentals of Electronics Communications
and Computer Sciences, vol. E90-A, pp. 1248-1251, June 2007.
(ISSN 0916-8508; Impact Factor in Year 2005: 0.330
ISI Category: Computer Science; Information Systems;
kategorija R52 - 3 boda)

[5] M. N. Huxley, J. Žunić:,
"The Number of n-Point Digital Discs,"
IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29 (no. 1), pp. 159-161, Jan. 2007
(ISSN: 0162-8828, Impact Factor in Year 2006: 4.306;
ISI Category: Computer Science; Artificial Inteligence; 2. od 85;
kategorija R51a - 8 bodova)

[6] P.L. Rosin and J. Žunić,
"Probabilistic convexity measure",
IET Image Processing, vol. 1, no. 2, pp. 182-188, Jun 2007.
(ranije IEE Proceedings - Vision Image and Signal Processing
ISSN: 1350-245X; Impact Factor in Year 2006: 0.461;
ISI Category: Electr. Electronics Eng.;
kategorija R2 - 3 boda)

[7] J. Žunić and P.L. Rosin,
"Convexity Measure for Shapes with Partially Extracted Boundaries",
IET Electronics Letters, vol. 43, no. 7, pp. 380-382, March 2007.
(ranije Electronics Letters ISSN: 1350-245X; Impact Factor in Year 2006: 1.063;
ISI Category: Electr. Electronics Eng.; 69. od 206
kategorija R51b - 5 bodova)

[8] M. Stojmenović and J. Žunić,
"New measure for shape elongation",
Lecture Notes in Computer Science, vol. 4478, pp. 572-579, July 2007.
(ISSN 0302-9743; Impact Factor in Year 2004: 0.513
ISI Category: Computer Science - Theory and Methods;
kategorija R52 - 3 boda)

[9] J. Žunić and P.L. Rosin,
"A Definition for Orientation for Multiple Component Shapes",
Lecture Notes in Computer Science, vol. 4673 pp. 677-685, August 2007.
(ISSN 0302-9743; Impact Factor in Year 2004: 0.513
ISI Category: Computer Science - Theory and Methods;
kategorija R52 - 3 boda)

[10] S. Ghilezan, J. Pantović, J. Žunić:
"Separating Points by Parallel Hyperplanes - Characterization Problem"
IEEE Transactions on Neural Networks, vol. 18, no. 5, pp. 1356-1363, Sept. 2007.
(ISSN: 1045-9227, I.f. (2005) 2.205, I.f. (2004) 2.170)
(ISSN 1045-9227; Impact Factor in Year 2006: 2.620
ISI Category: Computer Science - Theory and Methods; 5. od 75;
kategorija R51a - 8 bodova)

[11] N. Sladoje and J. Lindblad,
"Representation and reconstruction of fuzzy disks by moments",
FUZZY SETS AND SYSTEMS 158 (5): pp. 517-534, 2007
(doi:10.1016/j.fss.2006.09.017
<http://dx.doi.org/10.1016/j.fss.2006.09.017>
(ISSN 0165-0114; Impact Factor in Year 2006: 1.181;
ISI Category: Mathematics Applied; 29. od 150;
kategorija R51a - 8 bodova)

[12] P. Blagojević and A. Dimitrijević-Blagojević,
"Using equivariant obstruction theory in combinatorial geometry",
Topology and its Applications, vol. 154, pp. 2635-2655, 2007.
(ISSN 0166-8641; Impact Factor in Year 2006: 0.388
ISI Category: Mathematics Applied;
kategorija R52 - 3 boda)

[13] J.Dj. Golić, "Exact Probabilistic Analysis of Memoryless Combiners",
IEEE Transactions on Information Theory, vol. 53, no. 11, pp. 3958-3972, Nov. 2007.
(ISSN 0018-9448; Impact Factor in Year 2005: 2.183
ISI Category: Computer Science; Information Systems; 11. od 83;
kategorija R51a - 8 bodova)

godina 2006

[14] M. Fossorier, M. Mihaljević, H. Imai, Y. Cui and K. Matsuura,
"An Algorithm for Solving the LPN Problem and its Application to
Security Evaluation of the HB Protocols for RFID Authentication",
Lecture Notes in Computer Science, vol.4329, pp. 48-62, Dec. 2006.
(ISSN 0302-9743; Impact Factor in Year 2004: 0.513;
ISI-SCI Category: Computer Science - Theory and Methods;
kategorija R52 - 3 boda)

[15] M. Mihaljević, M. Fossorier and H. Imai,
"Security Weaknesses of Certain Broadcast Encryption Schemes",
Lecture Notes in Computer Science, vol. 3919, pp. 228-245, July 2006,
(ISSN 0302-9743; Impact Factor in Year 2004: 0.513;
ISI-SCI Category: Computer Science - Theory and Methods;
kategorija R52 - 3 boda)

[16] M. Mihaljević, M. Fossorier and H. Imai,
"A NovelBroadcast Encryption Based on Time-Bound Cryptographic Keys",
Lecture Notes in Computer Science, vol. 3919, pp. 258-276, July 2006.
(ISSN 0302-9743; Impact Factor in Year 2004: 0.513;
ISI-SCI Category: Computer Science - Theory and Methods;
kategorija R52 - 3 boda)

[17] J. Wang, M. Mihaljević, L. Harn, and H. Imai,
"A Hierarchical Key Management Approach for Secure Multicast",
Lecture Notes in Computer Science, vol. 3894, pp. 422-434, March 2006.
(ISSN 0302-9743; Impact Factor in Year 2004: 0.513;
ISI-SCI Category: Computer Science - Theory and Methods;
kategorija R52 - 3 boda)

[18] M. Mihaljević, M. Fossorier and H. Imai,
"A General Formulation of Algebraic and Fast Correlation Attacks
Based on Dedicated Sample Decimation",
Lecture Notes in Computer Science, vol. 3857, pp. 203-214, Feb. 2006.
(ISSN 0302-9743; Impact Factor in Year 2004: 0.513;
ISI-SCI Category: Computer Science - Theory and Methods;
kategorija R52 - 3 boda)

[19] J. Žunić, L. Kopanja and J.E.Fieldsend,
"Notes on shape orientation where the standard method does not work",
Pattern Recognition, vol. 39 (5), pp. 856-865, May 2006
(ISSN: 0031-3203; Impact Factor in Year 2005: 2.153;
ISI Category: Computer Science; Artificial Inteligence; 17. od 79;
kategorija R51a - 8 bodova)

[20] M.N. Huxley and J. Žunić,
"Different digitisations of displaced discs",
Foundations of Computational Mathematics, vol.6 (2), pp. 255-268, May 2006
(ISSN 1615-3375; Impact Factor in Year 2006: 1.269;
ISI Category: Mathematics Applied; 23. od 150;
kategorija R51a - 8 bodova)

[21] J. Žunić, P.L. Rosin, and L. Kopanja,
"Shape Orientability",
Lecture Notes In Computer Science, vol. 3852, pp. 11–20, Feb. 2006.
(ISSN 0302-9743; Impact Factor in Year 2004: 0.513;
ISI-SCI Category: Computer Science - Theory and Methods;
kategorija R52 - 3 boda)

[22] R. Klette and J. Žunić,
"On Discrete Moments of Unbounded Order",
Lecture Notes In Computer Science, vol. 4245, pp. 367-378, 2006.
(ISSN 0302-9743; Impact Factor in Year 2004: 0.513;
ISI-SCI Category: Computer Science - Theory and Methods;
kategorija R52 - 3 boda)

[23] J. Žunić, P. L. Rosin, L. Kopanja,
"On the Orientability of Shapes",
IEEE Transactions on Image Processing, vol 15, no. 11, pp. 3478-3487, 2006.
(ISSN: 1057-7149; Impact Factor in Year 2006: 2.715 ;
ISI Category: Computer Science; Artificial Inteligence; 5. od 85;
kategorija R51a - 8 bodova)

[24] J. Žunić,
"Boundary Based Orientation of Polygonal Shapes",
Lecture Notes in Computer Science, vol. 4319, pp. 108-117. Dec. 2006.
(ISSN 0302-9743; Impact Factor in Year 2004: 0.513;
ISI-SCI Category: Computer Science - Theory and Methods;
kategorija R52 - 3 boda)

[25] J. Lindblad and N. Sladoje,
"Feature Based Defuzzification at Increased Spatial Resolution",
Lecture Notes In Computer Science, vol. 4040, pp. 131-143, June 2006.
(ISSN 0302-9743; Impact Factor in Year 2004: 0.513;
ISI-SCI Category: Computer Science - Theory and Methods;
kategorija R52 - 3 boda)

[26] J. Lindblad, N. Sladoje, T. Lukić,
“Feature Based Defuzzification in Z2 and Z3 Using a Scale Space Approach”,
Lecture Notes in Computer Science, vol. 4245, pp. 379 – 390, 2006.
(ISSN 0302-9743; Impact Factor in Year 2004: 0.513;

ISI-SCI Category: Computer Science - Theory and Methods;
kategorija R52 - 3 boda)

[27] M. Marković,
“On Secure E-Health Systems,”
Lecture Notes In Computer Science, vol. 4302, pp. 360-374, Dec. 2006.
(ISSN 0302-9743; Impact Factor in Year 2004: 0.513;
ISI-SCI Category: Computer Science - Theory and Methods;
kategorija R52 - 3 boda)

[28] J.Dj. Golić and R. Menicocci,
"Statistical Distinguishers for Irregularly Decimated Linear Recurring Sequences",
IEEE Transsactions on Information Theory, vol. 52, NO. 3, pp. 1153-1159, March 2006
(ISSN 0018-9448; Impact Factor in Year 2005: 2.183
ISI Category: Computer Science; Information Systems; 11. od 83;
kategorija R51a - 8 bodova)

[29] J.Dj. Golić,
"Vectorial Boolean Functions and Induced Algebraic Equations",
IEEE Transsactions on Information Theory, vol. 52, NO. 2, pp. 528-537, Feb 2006
(ISSN 0018-9448; Impact Factor in Year 2005: 2.183
ISI Category: Computer Science; Information Systems; 11. od 83;
kategorija R51a - 8 bodova)

[30] J.Dj. Golić,
"Fibonacci numbers and decimation of binary sequences",
FIBONACCI QUARTERLY 44 (3): 216-223 AUG 2006
(ISSN 0015-0517; Impact Factor in Year 2005: 0.140;
ISI Category: Mathematics;
kategorija R52 - 3 boda)

I.2 Radovi u casopisima koji nisu na SCI listi (a koje Ministarstvo priznaje)

godina 2007

[31] A. Krapež,
"A note on Belousov Quasigroups",
Quasigroups and Related Systems 15, pp. 291-294, 2007.
(ISSN: 1561-2848)

[32] A. Krapež,
"Quadratic level quasigroup equations with four variables I",
Publications de l’Institut Mathématique, vol. 81(95), pp. 43-57, 2007.
(ISSN: 0350-1302)

[33] A. Krapež,
"Some significant results of Janez Ušan",
Novi Sad Journal of Mathematics, Vol. 37, No. 2, pp. 1-10, 2007.
http://www.im.ns.ac.yu/NSJOM/Papers/37_2/NSJOM_37_2_001_010.pdf
(ISSN: 1450-5444)

godina 2006

[34] P.V.M. Blagojević, A.S. Dimitrijević-Blagojević and M.S. Milošević,
"Equipartition of Sphere Measures by Hyperplanes",
Filomat, vol. 20, no. 1, pp. 1-11, 2006
(ISSN 0354-5180, available at: http://www.pmf.ni.ac.yu/sajt/publikacije/filomat_20.html)

[35] P.V.M. Blagojević, A.S. Dimitrijević-Blagojević and M.S. Milošević,
"Weighted Partitions of of Sphere Measures by Hyperplanes",
Filomat, vol. 20, no. 1, pp. 13-22, 2006
(ISSN 0354-5180, available at: http://www.pmf.ni.ac.yu/sajt/publikacije/filomat_20.html)

[36] V. Korać,
"SPAM",
Arheologija i prirodne nauke, No. 1, str. 137-150, 2006.
ISSN 1452-7448, COBISS.SR-ID 136747788
(dostupno : http://www.viminacium.org.yu/ELibrary/arch_sci/Volume_1/)

[37] V. Korać,
"Mobilni E-komerc",
Arheologija i prirodne nauke, No. 2, str. 129-144, 2006.
ISSN 1452-7448, COBISS.SR-ID 136747788
(dostupno : http://www.viminacium.org.yu/ELibrary/arch_sci/Volume_2/)

II. Poglavlja u monografijama medjunarodnog značaja (R22)

godina 2007.

[38] S. Ghilezan, J. Pantović, J. Žunić,
Parttioning finite d-dimensional integer grids with applications,
chapter in: Approximation Algorithms and Metaheuristics (editor T.F.Gonzales),
pp. 55-1 - 55-15, Chapman & Hall/CRC, Taylor and Francis Group, May 2007.
(kategorija R22: 3 boda)

godina 2006.

[39] M. N. Huxley, R. Klette and J. Žunić:
"Precision of Geometric Moments in Picture Analysis",
chapter in Geometric Properties from Incomplete Data, editors: R. Klette, R. Kozera, L. Noakes, J. Weickert, pp. 221-235, Kluwer Publisher, 2006.
(kategorija R22: 3 boda)

[40] M. Marković, Z. Savić, B. Kovačević,
"Secure Mobile Health Systems: Principles and Solutions", chapter in the book M-Health, Emerging Mobile Health Systems, pp. 81-106; Series: International Topics in Biomedical Engineering Istepanian, Robert; Laxminarayan, Swamy; Pattichis, Constantinos S. (Eds.)
2006, XXX, 624 p. 182 illus., Hardcover,
(ISBN 978-0-387-26558-2 (Print); 978-0-387-26559-9 (Online))
(kategorija R22: 3 boda)

III. Ostali rezultati (Pozvana predavanja,
radovi na domaćim i medjunarodnim naučnim skupovima,
uvodna izaganja, disertacije, …)

godina 2007

[41] M. Mihaljević,
"Decimation Based Correlation and Algebraic Attacks and Design of Boolean Functions",
Invited Plenary Talk, Advanced Study Institute on Boolean Functions in Cryptology and Information Security, Moscow, Sept. 2007 (to appear as a book\chapter in IOS Press Book Series "NATO Security through Science Series: Information and Communication Security", Eds. B. Prenell and O. Logachev; http://www.iospress.nl/)

[42] M.P.C. Fossorier, M.J. Mihaljević and H. Imai,
"Decimation Based Fast Correlation Attack", 2007 IEEE Int. Symp. Inform. Theory - ISIT'2007, Nice, France, June 2007, Proceedings, pp. 456-460. (ISBN 1-4244-1429-6).

[43] M. Mihaljević, H. Watanabe and H. Imai,
"A Low Complexity Authentication Technique Based on Binary Channel with Deletion, Insertion and Complementing", HISC 2007, Hawaii, May 29-31, 2007, Proceedings, pp. 95-100. (ISBN 978-4-902087-25-3; CD ISBN: 978-4-902787-25-3)

[44] M. Mihaljević, M. Fossorier, and H. Imai,
"Security Evaluation of Certain Broadcast Encryption Models
Employing a Dedicated Time-Memory Trade-Off Approach", HISC 2007,
Hawaii, May 29-31, 2007, Proceedings, pp. 125-129. (ISBN
978-4-902087-25-3; CD ISBN: 978-4-902787-25-3)

[45] J. Lindblad, T. Lukić and N. Sladoje,
"Defuzzification by Feature Distance Minimization Based on DC Programming",
5th IEEE International Symposium on Image and Signal Precessing and
Analysis - ISPA 2007, Istanbul, Turkey, Sept. 2007, Proceedings, pp. 373-378.
(ISBN: 978-953-184-116-0)

[46] V. Korać,
"INFRASTRUKTURA SA JAVNIM KLJUČEVIMA U FUNKCIJI ZAŠTITE
INFORMACIONOG TOKA I ELEKTRONSKOG POSLOVANJA",
Magistarski rad, Univerzitet Singidunum, Dec. 2007.

[47] G. Djordjevic, M. Marković,
“On Optimization of Miller-Rabin Primality Test on TI TMS320C54x Signal Processors,”
in Proc. of IWSSIP & EC-SIPMCS 2007 Conference, Maribor, Slovenia, June 26-30, 2007.

[48] G. Djordjevic, M. Marković,
„Simulation and JAVA Programming of Secure Mobile Web Services,”
Balcor 2007, Balkan Conference on Operational Research, Zlatibor, Oktobar 2007.

[49] M. Marković,
“Data Protection Techniques, Cryptographic Protocols and PKI Systems in Modern Computer
Networks,” Tutorial, in Proc. of IWSSIP & EC-SIPMCS 2007 Conference,
Maribor, Slovenia, June 26-30, 2007.

[50] M. Marković,
„Cryptographic Protocols in Modern Computer Networks – Combining Authentication and Secure
Payment,“ Tutorial, IAS 2007 – The Third International Symposium on Information Assurance
and Security, Manchester, UK, August 29-31, 2007.

[51] M. Marković,
„An Overview of Secure and Authenticated Remote Access to Central Sites,“
Invited Plenary Talk; Workshop on Data Access to Micro-Data (WDA), Nuernberg,
August 20-21, 2007.

[52] M. Marković,
„M-Government – Primena mobilnih uredaja u e-upravi,“
Pozvani rad, Infoteh 2007, Vrnjačka Banja, 30. maj 2007.

[53] M. Marković,
„Kombinovani sistemi jake autentikacije korisnika i sigurnih placanja,“

Pozvani rad, Infoteh 2007, Vrnjačka Banja, 30. maj 2007.

[54] M. Marković,
„Primena elektronskog potpisa u Srbiji“, Pozvani rad,
ArhivInfo 2007, Zlatibor, 12.09.2007.

[55] M. Marković,
„Secure e-Health Systems,“ Pozvani rad,
ISDOS 2007, Novi Sad, 8.-9. Oktobar 2007.

godina 2006.

[56] M. Marković, M. Kilibarda and A. Milošević,
"PKI Consolidation Project and Multiapplicative Smart Payment Cards",
ISSE 2006 Securing Electronic Business Processes
(Highlights of the Information Security Solutions Europe 2006 Conference),
Sachar Paulus, Norbert Pohlmann, Helmut Reimer, (Eds.), pp. 249-258.
(ISBN-13: 978-3-8348-0213-2. Vieweg, 2006).

[57] M. Marković and G. Djordjević,
"On Implementation Aspects of Standard Asymmetric and
Symmetric Cryptographic Algorithms on TI Signal Processors",
in Proceedings of the Second International Workshop on Security,
Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2006),
29 June 2006, Lyon, France. (IEEE Computer Society Press,
P.Georgiadis, J.Lopez, S.Gritzalis, and G.F.Marias (Eds.), pp. 57-62.
(ISBN-13: 978-0-7695-2549-5).

[58] M. Marković,
"Data Protection Technics and Cryptographic Protocols in Modern Computer Networks",
Tutorial, 13th International Conference on Telecommunications, ICT 2006,
Madeira, Portugal, May 9-12, 2006.

[59] M. Marković,
"Combining Authentication with Secure Payment",
in Proc. of Cartes 2006, Paris, Nov. 7-9, Invited lecture.

[60] M. Marković and G. Djordjević,
"On Optimizing Standard Cryptographic Algorithms on TI Fixed Point Signal Processors",
In Proc. of ICT 2006 Conference, Madeira, Portugal, May 9-12, 2006.

[61] M. Marković,
"Multiaplikativne EMV platne kartice",
Infoteh, Vrnjačka Banja, 13.06.2006. Pozvani rad.

[62] M. Marković,
"Elektronski servisi u zemljama Evropske Unije – Smernice za razvoj e-uprave u Srbiji",
Infoteh, Vrnjačka Banja, 13.06.2006. Pozvani rad.

[63] M. Marković,
“Infrastruktura e-uprave,” ISDOS, Zlatibor, 05.10.2006. Pozvani rad.

[64] M. Kilibarda, M. Marković,
“Projekat konsolidacije PKI sistema i multiaplikativne kartice u Banca Intesa ad Beograd,”
Zbornik radova Bankifo 2006, Palić, 8-10 novembar, 2006.

[65] A. Jevremović, M. Veinović,
"ZAŠTITA PODATAKA NA IP NIVOU POD LINUX OS"
Zbornik radova 50. Konferencije za ETRAN, Beograd, 6-8. juna 2006, tom III, str. 114-117.
Proc. 50th ETRAN Conference, Belgrade, June 6-8, 2006, Vol. III, pp. 114-117.

[66] A. Jevremović, M. Veinović,
"IPsec – analiza uticaja algoritma za šifrovanje na saobraćaj u LAN mrežama",
14. telekomunikacioni forum TELFOR 2006, Srbija, Beograd, novembar 21.-23. 2006,
Zbornik radova, str. 596-599.

[67] V. Stakić, M. Veinović,
"Prevodjenje uz pomoć kompjutera",
14. telekomunikacioni forum TELFOR 2006, Srbija, Beograd, novembar 21.-23. 2006,
Zbornik radova, str. 612-615.

[68] I. Franc, M. Veinović,
"Elektronski studentski indeks",
14. telekomunikacioni forum TELFOR 2006, Srbija, Beograd, novembar 21.-23. 2006,
Zbornik radova, str. 645-648.

[69] M. Mihaljević,
"On Certain Techniques for Cryptanalysis Based on Decoding Approaches",
Invited Talk, University of Hawaii at Manoa, Department of Electrical Engineering,
USA, November 28, 2006.

[70] M. Mihaljević,
"An Algorithm for Solving the LPN Problem and its Application to
Security Evaluation of the HB Protocols for RFID Authentication",
Plenary Invited Talk, IPA Cryptography Workshop 2006, Tokyo, Japan, October 4, 2006.

[71] M. Mihaljević,
"Certain Elements for Security Evaluation of Stream Ciphers",
Plenary Invited Talk by Cryptology Research Society of India,
National Workshop on Cryptology, India, Mumbai-Pune, 08-10 September 2006.