Projekat 1625 :
Nove matematičke metode za kriptografsku zaštitu i modelovanje informacija

Izvestaj o radu u 2005. godini

rukovodilac projekta
Dr Miodrag Mihaljevic, naucni svetnik

Predmet istraživanja

Projekat pripada oblasti matematickih metoda za procesiranje informacija i obuhvata istrazivacke aktivnosti na sledeca dva pravca veoma bitna za mnoge primene u informacionim tehnologijama: metode za kriptografsku zastitu informacija i metode za modelovanje informacija pod kojima se podrazumevaju odredjene metode za matematicko reprezentovanje informacija i informacionih sistema kao i neke metode za digitalnu obradu informacija. Metode za kriptografsku zastitu informacija obuhvataju metode za konstrukciju zastite i metode za analizu sigurnosti zastite. Metode za modelovanje informacija obuhvataju: informacione sadrzaje u slici i govoru, i metode za modelovanje slozenih sistema.

Sadržaj istraživanja

Tokom 2005. godine, istrazivacke aktivnosti su se odvijale u okvirima sledecih istrazivackih tema:
- kriptologija: metodi za proveru sigurnosti i nove dizajne kriptografskih primitiva;
- metode za analizu i modelovanje informacionih sadrzaja;
- metode za analizu i dizajn informacionih sistema;
- metode za zastitu informacija.

Medjunarodna naucna saradnja

Tokom 2005. godine realizovana je i intenzivna medjunarodna saradnja koja je kao dominantno ukljucivala:

- The University of Tokyo, Japan (nosilac saradnje M. Mihaljevic): kriptologija;
- University of Exeter, UK (nosilac saradnje J. Zunic): modelovanje digitalnih objekata;
- Swedish University of Agricultural Sciences, Centre for Image Analysis, Uppsala, Sweden (nosilac saradnje N. Sladoje) : modelovanje digitalnih objekata;
- EU, FP6 (nosilac saradnje M. Mihaljevic): zastita informacija u ad-hok mrezama.

Rezime ostvarenih rezultata

Tokom 2005. godine objavljeno je ukupno 30 radova, a struktura objavljenog je sledeca:
- dvanaest (12) rezultata kategorije rada u medjunarodnom ili vodecem medjunarodnom casopisu (kategorija R52 i R51)
- jedan (1) rezultat kategorije poglavlja u monografiji medjunarodnog znacaja
- pet (5) rezultata kategorije rada ne medjunarodnom naucnom skupu stampanom u celini,
- jedan (1) rezultat kategorije doktorska disertacija;
- jedanaest (11) rezultata kategorije rada nacionalnog znacaja.

Najznacajniji rezultati su ostvareni u okvirima sledecih istrazivackih pravaca:
- nove metode za proveru kriptografske sigurnosti generatora pseudoslucajnih nizova;
- nove metode za upravljanje kriptografskim kljucevima;
- nove metode za analizu i modelovanje digitalnih objekata.

Zakljucak

Projektne aktivnosti su rralizovane u punoj saglasnosti sa planom rada na projektu. Realizovani su svi planirani ciljevi, a ostvareni obim publikovanja rezultata projekta znacajno prevazilazi planirano.
Realizovana je i intenzivna medjunaroda saradnja sa ciljem participiranja ucesnika projekta u srodnim inostranim projektima. Uspesnost istrazivanja koja su bila predmet projekta ilustruje i cinjenica da su rezultati projekta 1625 sustinski doprineli ukljucivanju MI SANU kao partnera u FP6 EU projekat „AdHocSys” radi ucesca u resavanju odredjenih problema zastite informacija.

Spisak objavljenih rezultata

I . Journal Class Papers
Radovi kategorije R52 i R51
(medjunarodni i vodeci medjunarodni casopis)

[1] M. Mihaljevic, M.P.C. Fossorier and H. Imai,
"Key management with minimized secret storage employing an erasure channel approach",
IEEE Communications Letters, vol. 9, pp. 741-743, Aug. 2005.

[2] M. Mihaljevic and H. Imai,
"The decimated sample based improved algebraic attacks on nonlinear filters",
Lecture Notes in Computer Science, vol. 3352, pp. 310-323, Jan 2005.

[3] M. Mihaljevic, M. Fossorier and H. Imai,
"Cryptanalysis of keystream generator by decimated sample based
algebraic and fast correlation attacks",
Lecture Notes in Computer Science}, vol. 3797, pp. 155-168, Dec. 2005.

[4] J. Zunic,
"On the number of ways to occupy n lattice points by balls
in d-dimensional space",
Journal of Number Theory, vol. 110 (2), pp. 396-402, Feb 2005.

[5] P.L. Rosin and J. Zunic, "Measuring rectilinearity",
Computer Vision Image Understanding, Vol. 99, No. 2, pp 175-188, Aug. 2005.

[6] J. Zunic and L. Kopanja.
"On Shape Orientation when the Standard Method Does not Work",
Lecture Notes in Computer Science, Vol. 3773, pp 825-836, 2005.

[7] N. Sladoje, I. Nystrom and P.K. Saha,
"Measurements of digitized objects with fuzzy borders in 2D and 3D",
IMAGE AND VISION COMPUTING 23 (2): 123-132 FEB 1 2005.

[8] J. Chanussot, I. Nystrom and N. Sladoje,
"Shape signatures of fuzzy star-shaped sets based on distance
from the centroid",
PATTERN RECOGNITION LETTERS 26 (6): 735-746 MAY 1 2005.

[9] N. Sladoje and J. Lindblad,
“Estimation of moments of digitized Objects with fuzzy borders“,
ICIAP 2005, Lecture Notes in Computer Science, vol. 3617, pp. 188-195,
Sept. 2005.

[10] J. Golic and P. Hawkes,
"Vectorial approach to fast correlation attacks",
DESIGNS CODES AND CRYPTOGRAPHY, vol. 35 (1), pp. 5-19, APR 2005.

[11] J. Golic,
"Embedding Probabilities for the Alternating Step Generator",
IEEE Trans. Inform. Theory, vol. 51, pp. 2543-2553, July 2005.

[12] F.J. Ovalle-Martinez, I. Stojmenovic, F. Garcia-Nocetti F, et al.
"Finding minimum transmission radii for preserving connectivity and
constructing minimal spanning trees in ad hoc and sensor networks",
JOURNAL OF PARALLEL AND DISTRIBUTED COMPUTING 65 (2): 132-141
FEB 2005.

II. International Book Chapters
Radovi kategorije R22: Poglavlja u medjunarodnim monografijama

[1] A. Ngom, I. Stojmenovic, and J. Zunic.
"On the Computing Capacity of Multiple-Valued Multiple Threshold Perceptrons",
chapter in: Handbook of Bioinspired Algorithms and Applications,
S. Olariu, A. Zomaya (eds.)
pp. 425-450, Chapman & Hall/CRC, 2005.

III. The International Conference Class Papers
Radovi kategorije R54 (medjunarodna naucna konferencija)

[1] M.P.C. Fossorier, M. Mihaljevic and H. Imai,
"A Unified Analysis for the Fast Correlation Attack",
2005 IEEE Int. Symp. Inform. Theory - ISIT'2005,
Adelaide, Australia, Sept. 2005,
Proceedings, pp. 2012-2015 (ISBN 0-7803-9151-9).

[2] M. Mihaljevic, M.P.C. Fossorier and H. Imai,
"A Novel Approach to Algebraic and
Fast Correlation Attacks for Cryptanalysis of Certain
Keystream Generators",
HISC 2005 - 2005 Hawaii,
IEICE and SITA Joint Conference on Information Theory,
Hawaii, USA, May 2005, Proceedings, pp. 183-188
(ISBN 4-902087-13-8).

[3] M. Mihaljevic and H. Imai,
"Novel method for implementation of certain key management schemes
to minimize secret storage",
IEEE CCNC 2005, Las Vegas, USA, January 2005, Proceedings, pp. 54-59
(ISBN Softbound: 0-7803-8784-8; ISBN CD-Rom: 0-7803-87845-6.)

[4] Z. Banjac, B. Kovacevic,
"Robust Parameter and Scale Factor Estimation in Nonstationary
and Impulsive Noise Environment",
EUROCON 2005, IEEE region 8 conf., Belgrade, 2005.

[5] M. Markovic and G. Djordjevic,
"On optimizing DSP implementation of standard symmetrical
cryptographic algorithms",
EURASIP EC-SIP-M 2005, June 2005, Smolenice, Slovak Republic.

IV. PhD Disertation
Doktorske Teze

[1] N. Sladoje, "On Analysis of Discrete Spatial Fuzzy Sets in
2 and 3 Dimensions", Doctorial Thesis No. 2005:112,
Swedish University of Agricultural Sciences, Centre for Image Analysis,
Uppsala, Sweden, Nov. 2005 (ISBN 91-576-6911-2)

V. Other Publications
Ostalo

[1] B. Kovacevic, Z. Banjac,
Adaptivni Digitalni Filtri,
ISBN: 86-7466-219-6.Akademska misao, Beograd, 2005.

[2] V. Spasic,
Matematicko modeliranje slozenih zivih sistema,
Beograd 2005, ISBN 86-85903-01-7, CORBISS.SR-ID 123728908
(monografija obima 223 str.)

[3] V. Spasic,
Programiranje i primene, Beograd 2005,
ISBN 86-85903-00-9, CORBISS.SR-ID 123725580
(monografski poslediplomski univerzitetski udzbenik obima 260 str.)

[4] V. Spasic,
Internet sistem za domen informisanja sa interaktivnim savetovalistem,
Internet publikovano, www.glosarijum.com (publikovan softver).

[5] M. Markovic,
"Elektronski potpis: Osvrt na Zakon o elektronskom
potpisu i odgovarajuca podzakonska akta",
E-trgovina 2005, Palic, 20.-22.04.2005. Pozivni rad.

[6] M. Markovic,
"Multiaplikativne smart kartice i Internet bankarstvo Delta banke",
Technobank 2005, Beograd, 25. i 26. april 2005. Pozivni rad.

[7] M. Markovic,
"Zakon o elektronskom potpisu: podzakonska akta i
procedura implementacije Zakona u Srbiji",
Infotech 2005, Vrnjacka Banja, 06.-10.06.2005. Pozivni rad.

[8] M. Markovic,
"Implementacija Zakona o elektronskom potpisu i
podzakonskih akata za njegovo sprovo?nje",
IS DOS 2005, Vrnjacka Banja, 19.-21.09.2005. Pozivni rad.

[9] M. Markovic,
"MV MIGRACIJA: IZAZOVI I MOGUCNOSTI",
INFOFEST 2005, Specijalna sesija, 30. Septembar 2005.

[10] M. Markovic,
"Uspostava nacionalne PKI infrastrukture za primenu
kvalifikovanog elektronskog potpisa u Srbiji",

Smart e-Government 2005, Beograd, 18.-19.10.2005. Pozivni rad.

[11] M. Markovic,
"Uticaj Zakona o elektronskom potpisu na rad banaka",
Nova Bankarska Vizija3, Ohrid, 11.-14.05.2005.