Project ON144018: "Advanced Methods in Cryptology and Information Processing"

List of the Main Project Results in the Year 2006

I. Journal Class Papers

[1] M. Fossorier, M. Mihaljevic, 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;
Impact Factor in Year 2005: 0.402)

[2] M. Mihaljevic, 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;
Impact Factor in Year 2005: 0.402)

[3] M. Mihaljevic, 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;
Impact Factor in Year 2005: 0.402)

[4] J. Wang, M. Mihaljevic, 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;
Impact Factor in Year 2005: 0.402)

[5] M. Mihaljevic, 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;
Impact Factor in Year 2005: 0.402)

[6] J. Zunic, 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)

[7] M.N. Huxley and J. Zunic,
"Different digitisations of displaced discs",
Foundations of Computational Mathematics, vol.6 (2), pp. 255-268, May 2006
(ISSN 0925-9856; Impact Factor in Year 2005: 0.880;
Impact Factor u 2004 bio 1.500

[8] J. Zunic, P. L. Rosin and 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 2004: 2.011;
Impact Factor in Year 2005: 2.428)

[9] J.Zunic, 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;
Impact Factor in Year 2005: 0.402)

[10] R. Klette and J. Zunic,
"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;
Impact Factor in Year 2005: 0.402)

[11] J. Zunic,
"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;
Impact Factor in Year 2005: 0.402)

[12] J. Dj. Golic 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)

[13] J. Dj. Golic,
"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)

[14] J. Pieprzyk, X.-M. Zhang, and J.Dj. Golic,
"Characterisations of Extended Resiliency and Extended Immunity of S-Boxes",
Lecture Notes In Computer Science, vol. 3935, pp. 210-228, June 2006.
(ISSN 0302-9743; Impact Factor in Year 2004: 0.513;
Impact Factor in Year 2005: 0.402)

[15] N. Sladoje and J. Lindblad,
“Representation and reconstruction of fuzzy disks by moments”,

Fuzzy Sets and Systems, 2006.
Available online October 24, 2006, 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 2004: 0.734;
Impact Factor in Year 2005: 1.039)

[16] 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;
Impact Factor in Year 2005: 0.402)

[17] J. Lindblad, N. Sladoje, T. Lukic,
"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;
Impact Factor in Year 2005: 0.402)

[18] M.Markovic, "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;
Impact Factor in Year 2005: 0.402)

[19] P.V.M. Blagojevic, A.S. Dimitrijevic-Blagojevic and M.S. Milosevic,
"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)

[20] P.V.M. Blagojevic, A.S. Dimitrijevic-Blagojevic and M.S. Milosevic,
"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)

II. International Book Chapters

[21] M.Markovic, Z.Savic and B.Kovacevic,
"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: 0-387-26558-9.

[22] M. N. Huxley, R. Klette and J. Zunic:
"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.

III. Other Results: Invited Talks, International and National Conference Papers, Tutorials, ...

[23] M.Markovic, M.Kilibarda and A.Miloševic,
"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).

[24] M.Markovic and G.Đordevic,
"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).

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

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

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

[28] M. Markovic,
"Multiaplikativne EMV platne kartice",
Infoteh, Vrnjacka Banja, 13.06.2006. Pozivni rad.

[29] M. Markovic,
"Elektronski servisi u zemljama Evropske Unije – Smernice za razvoj e-uprave u Srbiji",
Infoteh, Vrnjacka Banja, 13.06.2006. Pozivni rad.

[30] M. Markovic,
“Infrastruktura e-uprave,” ISDOS, Zlatibor, 05.10.2006. Pozivni rad.

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

[32] A. Jevremovic, M. Veinovic,
"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.

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

[34] V. Stakic, M. Veinovic,
"Prevodjenje uz pomoc kompjutera",
14. telekomunikacioni forum TELFOR 2006, Srbija, Beograd, novembar 21.-23. 2006, Zbornik radova, str. 612-615.

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

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

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

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