Miodrag J. Mihaljević
Biografski Podaci (CV) i izabrana Bibliografija

Summary

MIODRAG J. MIHALJEVIĆ is a Research Professor and the Deputy Director with the Mathematical Institute, Serbian Academy of Sciences and Arts, Belgrade. His main research interests include cryptology, information security and blockchain technology. He has published more than 100 research articles in the leading international journals and conference proceedings and over 200 publications in total. He is co-inventor of eight granted patents in Japan, U.S., and China. He has organized and played principal investigator roles in over ten national projects and has participated in over ten international research projects. Since 1997, he has been holding long-term visiting positions at the universities and research institutes in Japan, including The University of Tokyo, Sony Research Labs, the National Institute AIST, and Chuo University, Tokyo. In 2013, he received the National Award of the Serbian Academy of Sciences and Arts for ten years achievements. Since 2014, he has been an Elected Member of the Academia Europaea. In the four consecutive years 2020, 2021, 2022. And 2023, Dr. Mihaljevic is included in the ranked list colloquially known as "World's Top 2% Scientists" (by Elsevier and Stanford University) regarding his career achievements. He is an Elected Member of the Serbian Academy of Sciences and Arts from 2021. For more information, please visit https://www.sanu.ac.rs/en/member/mihaljevic-miodrag/

Obrazovanje, izbori i zaposlenje

Završio Elektrotehnički fakultet, Univerziteta u Beogradu 1979., magistrirao je jula 1981., doktorirao juna 1990. Stekao zvanje naučnog savetnika 1999. godine u Matematičkom institutu (MI) SANU i Ministarstvu nauke Republike Srbije. Od septembra 1979. do maja 1998. radio je u vojnom Institutu za primenjenu matematiku i elektroniku, koji je bio federalna institucija za zaštitu informacija u SFRJ, gde je, između ostalog, bio predsednik naučnog veća od 1994. Od 1992. je i spoljni saradnik MI-SANU, a od maja 1998. radi kao stalno zaposlen u MI-SANU. Od marta 2015. je zamenik direktora MI-SANU, a od januara 2021. je i rukovodilac Sektora za računarstvo u MI-SANU. Radni odnos M. Mihaljevića u MI-SANU je produžen do novembra 2025., prema članu 100, Zakona o nauci, Republike Srbije.

Oblast rada

Oblast rada i naučno-tehničkih dostignuća M. Mihaljevića je informaciona bezbednost&privatnost i blokčejn thnologija koji su danas opšte prepoznati kao oblasti od ključnog značaja za razvoj i primene informaciono-komunikacionih tehnologija. Glavna dostignuća su u domenima evaluacije, dizajna i primena kriptografskih algoritama za ostvarivanje informacione bezbednosti u informaciono-komunikacionim sistemima kao i napredne tehnike i primene blokčejn tehnologije.

Rukovođenje projektima.

U MI-SANU, M. Mihaljević je organizovao i rukovodio projektima osnovnih istraživanja realizovanim tokom 1993-1995, 1996-2000, 2002-2005, 2006-2010, i 2011-2019 godine, i projektima tehnološkog razvoja tokom 1998-2000 i 2002-2004 godine i III potprojektom 2011-2018 godine (koje su finansirala ministrastva Vlade Republike Srbije) u kojima je bio i jedan od vodećih realizatora. Svi ovi projekti su imali veoma uspešne realizacije, tokom kojih je, između ostalog, objavljeno i više od 300 radova u vodećim međunarodnim časopisima i odbranjeno više od 10 doktorskih disertacija. Takođe, M. Mihaljević je organizovao i rukovodio i više od 10 projekata koje su realizovani kroz bilateralne ugovore MI-SANU sa državnim i privrednim institucijama uključujući Vladu Republike Srbije, Centralnu banku Crne Gore i Telekom Srbija, u kojima je takođe bio i jedan od glavnih realizatora. Kao ilustracija projekata koje je organizovao i kojima je rukovodio M. Mihaljević, navode se sledeći projekti osnovnih idstraživanja „Novi prilozi tehnikama kriptologije, procesiranja slika i algebarske topologije za informacionu bezbednost“ (2011-2018), „Nove metode u kriptologiji i procesiranju informacija“ (2006-2010), „Nove metode za kriptografsku zaštitu i modelovanje informacija“ (2002-2005), i projekat tehnološkog razvoja „Softverski sistem za kriptografsku zasštitu elektronskih arihva“ (2002-2004).

Međunarodna saradnja

M. Mihaljević je realizovao međunarodnu saradnju, kao deo realizacije projekata kojima je rukovodio, i u kojima je bio jedan od vodećih istraživača, a koja je započela 1997. godine i koja traje i dalje. Ova međunarodna saradnja je realizovana ili se realizuje u sledećim okvirima: FP6 okvirnog programa EU (2006-2009 godina), Tempus projekta (2009-2011 godina), COST akcija (2014-2018 godina), Japansko-Indijskog strateškog projekta u oblasti kriptologije (2009-2012 godina), i učešća po pozivu u realizaciji više od 10 projekata u Japanu, SAD i Singapuru (1997-2021 godina).

M. Mihaljević je u funkciji našeg istraživačkog razvoja i promocije naših istraživačkih potencijala od 1997. godine imao više gostujućih pozicija po pozivu u Japanu: “Visiting Researcher” na The University of Tokyo, SONY Computer Science Laboratories, SONY Coropiration Research Laboratories, “Visiting Foreign Professor” na The University of Tokyo, “Invited Senior Research Scientist” u National Institute AIST, “Researcher/Professor” na Chuo University, i “Project Professor” na The University of Tokyo. Tekuće, M. Mihaljević je učesnik dvogodišnjeg projekta (2021-2022 godina) iz oblasti blokčejn tehnologije koji se realizuje u okviru Shandong Academy of Science, Kina, saglasno krovnom ugovoru sa MI-SANU.

Načno-stručne reference

M. Mihaljević je autor preko 230 javno objavljenih referenci uključujući sledeće: editor jedne monografije i autorstvo više od 10 poglavlja u monografijama, više od 70 radova u časopisim, više od 50 radova na međunarodnim konferencijama, više od 20 predavanje po pozivu, 8 međunarodno priznatih patenata (Japan, SAD, Kina) i više od 40 tehničkih rešenja. Posebno se ukazuje da kumulativna lista razmatranih 230 javno objavljenih ostvarenja M.

Mihaljevića ne uključuje rezultate koji nisu javno dostupni zato što su vlasništvo državnih ili poslovnih institucija.
Njegova citiranost, bez autocitata, je: više od 1000 puta u WoS i više od 1500 puta u Scopus-u.

Nagrade i priznanja

M. Mihaljević je je dobitnik više priznanja i nagrada uključujući i sledeće:
- Uvršćen je po ukupnim karijernim rezultatima na rang liste kolokvijano posnate kao "World's Top 2% Scientists by Stanford University" (i unutar je 1.6% najboljih u oblasti Networks & Telecommunications) za 2019., 2020., 2021. i 2022. godinu.
- Izabran je dopisnog člana Srpske akademije nauka i umetnosti (SANU) 2021. godine za odeljenje tehničkih nauka
- Izabran za člana Academia Europaea sa sedištem u Londonu i sada je jedan od 17 članova (među kojima je i 5 članova SANU) ove akademije iz Srbije (2014. godina);
- Jedan od dobitnika Nagrade SANU u oblasti matematike i srodnih nauka 2013. godine za njegova desetogodišnja dostignuća 2003-2012 u oblasti kriptologije i informacione bezbednosti (2013. godina);
- Nagrada Ministarstva nauke i tehnološkog razvoja Republike Srbije za izuzetne rezultate u oblasti osnovnih istraživanja ostvarene 2002.-2003. godine (2004. godina);
- Nagrada iz Generalštaba JNA za doktorsku disertaciju (1990. godana) ;
- "Medalja rada" za višegodišnje ukupne radne rezultate (1989. godina);
- "Majska nagrada" grada Beograda kao jednom od tri u generaciji prvo-diplomirana inženjera na Elektrotehničkom fakultetu u Beogradu (1979. godana).

Biografske i bibliografske informacije su raspoložive i na sledećim linkovima:

SANU

https://www.sanu.ac.rs/en/member/mihaljevic-miodrag/
https://www.sanu.ac.rs/clan/mihaljevic-miodrag/

MI-SANU

https://www.mi.sanu.ac.rs/cv/cvmihaljevic.htm
https://www.mi.sanu.ac.rs/cv/pubmihaljevic.htm
https://www.mi.sanu.ac.rs/novi_sajt/NationalCenterCyberSecurityPrivacy/index.php

Repozitorijum rezultata MI-SANU

http://researchrepository.mi.sanu.ac.rs/cris/rp/rp00003

Miodrag J. Mihaljevic – Lista izabranih reference

(raspoloživa na: https://www.mi.sanu.ac.rs/cv/pubmihaljevic.htm)

Selected Patents

1. **Japan Patent JP 6667174 B2 : M.J. Mihaljevic** and K. Matsuura,
   Communication Data Encryption/decryption Method And System,
   February 2020.

2. **Japan Patent JP 6602210 B2:** K. Matsuura and **M.J. Mihaljevic,**
   Authentication System and Method,,
   November, 2019.

3. **Japan Patent JP 4863283 B2**: **M.J. Mihaljevic** and H. Watanabe
   Authentication system using light-weight authentication protocol,
   November 18, 2011.

4. **United States Patent US 8023649 B2**: **M.J. Mihaljevic** and J. Abe
   Method and apparatus for cellular automata based generation of pseudorandom sequences with controllable period,
   September 20, 2011.
   available at
   http://worldwide.espacenet.com/publicationDetails/originalDocument?FT=D&date=20110920&DB=EPODOC&locale=en_EP&CC=US&NR=8023649B2&KC=B2

5. **China Patent CN 1698306 B2**: **M.J. Mihaljevic** and J. Abe

Data processing method,
October 06, 2010.
available at
http://worldwide.espacenet.com/publicationDetails/originalDocument?FT=D&date=20101006&DB=EPODOC&locale=en_EP&CC=CN&NR=1698306B&KC=B
http://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&at=7&locale=en_EP&FT=D&CC=US&NR=2005213765A1&KC=A1)

6. **Japan Patent JP 4432350 B2**: **M.J. Mihaljevic** and J. Abe
Data Processing Method, Program Thereof, Data Processor, and Receiver,
35 pages, March 2010.
available at
http://worldwide.espacenet.com/publicationDetails/biblio?FT=D&date=20100317&DB=&locale=en_EP&CC=JP&NR=4432350B2&KC=B2&ND=1

7. **United States Patent US 7502941 B2**: L. Michael and **M.J. Mihaljevic**
Wireless data communication method and apparatus for software download system,
March 10, 2009.
available at
http://worldwide.espacenet.com/publicationDetails/originalDocument?FT=D&date=20090310&DB=EPODOC&locale=en_EP&CC=US&NR=7502941B2&KC=B2

8. **Japan Patent JP 3918578 B2**: R. Morelos Zaragoza and **M.J. Mihaljevic**
Method and apparatus for loss correction and limited reception in streaming data, and data communication apparatus,
May 23, 2007.
available at
http://worldwide.espacenet.com/publicationDetails/biblio?FT=D&date=20070523&DB=EPODOC&locale=en_EP&CC=JP&NR=3918578B2&KC=B2

Papers in publications from the Science Citation Index (SCI) list of the Web of Science

9. **M.J. Mihaljevic**, M. Todorovic, and M. Kneževic, "An Evaluation of Power Consumption Gain and Security of Flexible Green Pool Mining in Public Blockchain Systems", *Symmetry*, 2023, vol. 15, 924. doi.org/10.3390/sym15040924

10. S. Zhang, C. Hu, L. Wang, **M.J. Mihaljevic**, S. Xu, and T. Lan, "A Malware Detection Approach Based on Deep Learning and Memory Forensics", *Symmetry*, 2023, vol. 15, 758. doi: 10.3390/sym15030758

11. **M.J. Mihaljević**, M. Knežević, D. Urošević, L. Wang, and S. Xu, "An Approach for Blockchain and Symmetric Keys Broadcast Encryption Based Access Control in IoT", *Symmetry*, 2023, vol. 15, 299. doi: 10.3390/sym15020299

12. **M.J. Mihaljevic**, L. Wang, S. Xu and M. Todorovic, "An Approach for Blockchain

Pool Mining Employing the Consensus Protocol Robust against Block Withholding and Selfish Mining Attacks", *Symmetry* 2022, 14 (8), 1711. (28 pages)

13. **M.J. Mihaljevic**, L. Wang and S. Xu,, "An Approach for Security Enhancement of Certain Encryption Schemes Employing Error Correction Coding and Simulated Synchronization Errors", *Entropy* 2022, 24(3), 406; (10 pages)

14. **M.J. Mihaljevic**, A. Radonjic, L. Wang and S. Xu,, "Security Enhanced Symmetric Key Encryption Employing an Integer Code for the Erasure Channel", *Symmetry* 2022, 14 (8), 1709. (21 pages)

15. S. Tomovic, M. Knezevic, and **M.J. Mihaljevic**, "Analysis and Correction of the Attack against the LPN-Problem Based Authentication Protocols", *Mathematics*, vol. 9, Iss. 5, (27 pages), March 2021, doi:10.3390/math9050573. https://www.mdpi.com/2227-7390/9/5/573

16. **M.J. Mihaljevic**, "A Blockchain Consensus Protocol Based on Dedicated Time-Memory-Data Trade-Off", *IEEE Access*, vol. 8, pp. 141258-141268, Avg 2020

17. M. Kneževic, S. Tomovic and **M.J. Mihaljevic**, "Man-In-The-Middle Attack against Certain Authentication Protocols Revisited: Insights into the Approach and Performances Re-Evaluation", *Electronics*, vol. 9 (8), 1296 (23 pages) Avg. 2020

18. **M.J. Mihaljevic,** "A Security Enhanced Encryption Scheme and Evaluation of Its Cryptographic Security",
Entropy , vol 21 (7), July 2019 (11 pages); https://doi.org/10.3390/e21070701 ,
https://www.mdpi.com/1099-4300/21/7/701

19. **M.J. Mihaljevic** and F. Oggier, "Security Evaluation and Design Elements for a Class of Randomized Encryptions",
IET Information Security, 12 pages, Vol. 13, no. 1, pp. 36–47, Jan. 2019,
DOI: 10.1049/iet-ifs.2017.0271,
https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2017.0271 &
https://ieeexplore.ieee.org/document/8611527

20. **M.J. Mihaljevic**, A. Kavcic and K. Matsuura, "An Encryption Technique for Provably Secure Transmission from a High Performance Computing Entity to a Tiny One",
Mathematical Problems in Engineering, Volume 2016, Article ID 7920495, 10 pages,
http://dx.doi.org/10.1155/2016/7920495 .

21. S. Tomovic, **M.J. Mihaljevic**, A. Perovic and Z. Ognjanovic, "A Protocol for Provably Secure Authentication of a Tiny Entity to a High Performance Computing One",
Mathematical Problems in Engineering, Volume 2016, Article ID 9289050, 9 pages,
http://dx.doi.org/10.1155/2016/9289050 .

22. F. Oggier and **M.J. Mihaljevic**, "An Information-Theoretic Security Evaluation of a Class of Randomized Encryption Schemes",
IEEE Transactions on Information Forensics and Security, vol. 9, no. 2, pp. 158-168,

Feb. 2014. (DOI: 10.1109/TIFS.2013.2294763).

23. **M.J. Mihaljevic**, S. Gangopadhyay, G. Paul and H. Imai, "Internal State Recovery of Keystream Generator LILI-128 Based on a Novel Weakness of the Employed Boolean Function",
Information Processing Letters, vol. 112, no. 21, pp. 805-810, November 2012.

24. **M.J. Mihaljevic**, S. Gangopadhyay, G. Paul and H. Imai, "State Recovery of Grain-v1 Employing Normality Order of the Filter Function",
IET Information Security, vol. 6, no. 2, pp. 55-64, June 2012.

25. **M.J. Mihaljevic**, S. Gangopadhyay, G. Paul and H. Imai, "Generic Cryptographic Weakness of k-normal Boolean Functions in Certain Stream Ciphers and Cryptanalysis of Grain-128",
Periodica Mathematica Hungarica, vol. 65, no. 2, pp. 205-227, Dec. 2012.

26. **M. Mihaljevic** and H. Imai, "An approach for stream ciphers design based on joint computing over random and secret data",
Computing, vol. 85, no. 1-2, pp. 153-168, June 2009. (DOI: 10.1007/s00607-009-0035-x)

27. **M. Mihaljevic**, 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.

28. M. Fossorier, **M. Mihaljevic** and H. Imai, "Modeling Block ecoding Approaches for Fast Correlation Attack",
IEEE Transactions on Information Theory, vol. 53, no. 12, pp. 4728-4737, Dec. 2007.

29. **M. Mihaljevic**, "Generic framework for secure Yuan 2000 quantum encryption protocol employing the wire-tap channel approach'",
Physical Review A, vol. 75, no. 5, pp. 052334-1-5, May 2007.

30. **M. Mihaljevic**, 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, no. 6, pp. 1248-1251, June 2007.

31. M.P.C. Fossorier, **M.J. 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.

32. **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.

33. **M. Mihaljevic**, M. Fossorier and H. Imai, " A Novel Broadcast Encryption Based on Time-Bound Cryptographic Keys",
Lecture Notes in Computer Science, vol. 3919, pp. 258-276, July 2006.

34. 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.

35. **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. 203-212, Feb. 2006.

36. **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.

37. **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.

38. **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.

39. **M. Mihaljevic**, M. Fossorier and H. Imai, "Secret-public storage trade-off for broadcast encryption key management",
Lecture Notes in Computer Science, vol. 3269, pp. 375-387, October 2004.

40. **M. Mihaljevic**, "Reconfigurable key management for broadcast encryption",
IEEE Communications Letters, vol. 8, pp. 440-442, July 2004.

41. **M. Mihaljevic**, "Key management schemes for stateless receivers based on time varying heterogeneous logical key hierarchy",
Lecture Notes in Computer Science, vol. 2894, pp. 137-154, 2003.

42. **M. Mihaljevic**, "On vulnerabilities and improvements of fast encription algorithm for multimedia FEA-M",
IEEE Trans. Cons. Electr., vol. 49, no. 4, pp. 1199-1206, Nov. 2003.

43. **M. Mihaljevic**, "Broadcast encryption schemes based on the sectioned key tree",
Lecture Notes in Computer Science, vol. 2836, pp. 158-169, Oct. 2003.

44. P. Camion, **M. Mihaljevic** and H. Imai, "Two allerts for design of certain stream ciphers: Trapped LFSR and weak resilient function over GF(q)",
Lecture Notes in Computer Science, vol. 2595, pp. 196-213, 2003.

45. L. Michael, **M. Mihaljevic**, S. Haruyama and R. Kohno, "Security issues for Software Defined Radio: Design of a Secure Download System",
IEICE Trans. Communications, vol. E85-B, pp. 2588-2600, Dec. 2002.

46. **M. Mihaljevic** and R. Kohno, "Cryptanalysis of fast encryption algorithm for multimedia FEA-M",
IEEE Communications Letters, vol. 6, pp.382-384, September 2002.

47. L. Michael, **M. Mihaljevic**, S. Haruyama and R. Kohno, "A framework for secure

download for software defined radio",
IEEE Communications Magazine, vol. 40, no. 7, pp. 88-96, July 2002.

48. **M. Mihaljevic**, M.P.C. Fossorier and H. Imai, "Fast correlation attack algorithm with the list decoding and an application",
Lecture Notes in Computer Science, vol. 2355, pp. 196-210, 2002.

49. **M. Mihaljevic** and H. Imai, "Cryptanalysis of TOYOCRYPT-HS1 Stream Cipher",
IEICE Trans. Fundamentals, vol. E85-A, pp. 66-73, Jan. 2002.

50. **M. Mihaljevic**, M.P.C. Fossorier and H. Imai, "On decoding techniques for cryptanalysis of certain encryption algorithms",
IEICE Transactions on Fundamentals, vol. E84-A, pp. 919-930, Apr. 2001.

51. **M. Mihaljevic**, M.P.C. Fossorier and H. Imai, "A low-complexity and high-performance algorithm for the fast correlation attack",
Lecture Notes in Computer Science, vol. 1978, pp.196-212, 2001.

52. **M. Mihaljevic**, M.P.C. Fossorier and H. Imai, "An algorithm for cryptanalysis of certain keystream generators suitable for high-speed software and hardware implementations",
IEICE Transactions on Fundamentals, vol. E84-A, pp. 311-318, Jan. 2001.

53. **M. Mihaljevic** and J. Golic, "A method for convergence analysis of iterative probabilistic decoding",
IEEE Transactions on Information Theory, vol. 46, pp. 2206-2211, Sept. 2000.

54. M. Fossorier, **M. Mihaljevic** and H. Imai, "Reduced complexity iterative decoding of Low Density Parity Check codes based on Belief Propagation",
IEEE Transactions on Communications, vol. 47, pp. 673-680, 1999.

55. M. Fossorier, **M. Mihaljevic** and H. Imai, "Critical noise for convergence of iterative probabilistic decoding with Belief Propagation in cryptographic applications",
Lecture Notes in Computer Science, vol. 1719, pp. 282-293, 1999.

56. **M. Mihaljevic** and H. Imai, "A family of fast keystream generators based on programmable linear cellular automata over GF(q) and time variant table",
IEICE Transactions on Fundamentals, vol. E82-A, pp. 32-39, Jan. 1999.

57. **M. Mihaljevic**, Y. Zheng and H. Imai, "A family of fast dedicated one-way hash functions based on linear cellular automata over GF(q)",
IEICE Transactions on Fundamentals, vol. E82-A, pp. 40-47, Jan. 1999.

58. **M. Mihaljevic**, Y. Zheng and H. Imai, "A cellular automaton based fast one-way hash function suitable for hardware implementation",
Lecture Notes in Computer Science, vol. 1431, pp. 217-233, 1998.

59. **M. Mihaljevic**, "An improved key stream generator based on the programmable cellular automata",
Lecture Notes in Computer Science, vol. 1334, pp. 181-191, 1997.

60. **M. Mihaljevic**, "Security examination of a cellular automata based pseudorandom bit generator using an algebraic replica approach",
Lecture Notes in Computer Science, vol. 1255, pp. 250-262, 1997.

61. **M. Mihaljevic**, "An iterative probabilistic decoding algorithm for binary linear block codes beyond the half minimum distance",
Lecture Notes in Computer Science, vol. 1255, pp. 237-249, 1997.

62. **M. Mihaljevic**, "A faster cryptanalysis of the self-shrinking generator",
Lecture Notes in Computer Science, vol. 1172, pp. 182-188, 1996.

63. **M. Mihaljevic**, "A sequence comparison approach for decoding of general binary block codes after the binary symmetric channel with synchronization errors",
Zeitschrift fur Angewandte Mathematik und Mechanik - ZAMM, vol. 76, pp. 479-481, 1996.

64. **M. Mihaljevic**, "A correlation attack on the binary sequence generators with time-varying output function",
Lecture Notes in Computer Science, vol. 917, pp. 67-79, 1995.

65. **M. Mihaljevic**, "On message protection in crypto systems modeled as the generalized wire-tap channel II",
Lecture Notes in Computer Science, vol. 829, pp. 13-24, 1994.

66. **M. Mihaljevic**, "An approach to the initial state reconstruction of a clock-controlled shift register based on a novel distance measure",
Lecture Notes in Computer Science, vol. 718, pp. 349-356, 1993.

67. **M. Mihaljevic**, J. Golic, "Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequence",
Lecture Notes in Computer Science, vol. 658, pp. 124-137, 1993. (reprinted in *Lecture Notes in Computer Science*, vol. 1440, 1999)

68. **M. Mihaljevic**, J. Golic, "A comparison of cryptanalytic principles based on iterative error-correction",
Lecture Notes in Computer Science, vol. 547, pp. 527-531, 1992. (reprinted in *Lecture Notes in Computer Science*, vol. 1440, 1999)

69. J. Golic, **M. Mihaljevic**, "A generalized correlation attack on a class of stream ciphers based on the Levenshtein distance",
Journal of Cryptology, vol. 3, pp. 201-212, 1991.

70. J. Golic, **M. Mihaljevic**, "A noisy clock-controlled shift register cryptanalysis concept based on sequence comparison approach",
Lecture Notes in Computer Science, vol. 473, pp. 487-491, 1991. (reprinted in *Lecture Notes in Computer Science*, vol. 1440, 1999)

71. **M. Mihaljevic**, J. Golic, "A fast iterative algorithm for a shift register initial state reconstruction given the noisy output sequence",
Lecture Notes in Computer Science, vol. 453, pp. 165-175, 1990.

72. J. Golic, **M. Mihaljevic**, "Minimal linear equivalent analysis of a variable memory binary sequence generator",
IEEE Transactions on Information Theory, vol. 36, pp. 190-192, Jan. 1990.

Selected Book Chapters

73. **M.J. Mihaljevic**, "Блокчејн технологија за напредне електроенергетске мреже" ("Blockchain Technology for Advanced Power Grids") u *ЕНЕРГЕТИКА И КЛИМАТСКЕ ПРОМЕНЕ* , pp. 97-119, Српска академија наука и уметности, 2023. ISBN 978-86-7025-974-4

74. V. Mikhalev, **M.J. Mihaljevic**, O. Kara and F. Armknecht, “Selected Design and Analysis Techniques of Contemporary Symmetric Encryption”, to appear in *Security of Ubiquitous Computing Systems*, Eds. G. Avoine and J. Hernandez-Castro, Springer, pp. 49-62, Springer 2021.

75. A. Mileva, V. Dimitrova, O. Kara and **M.J. Mihaljevic**, “Catalog and Illustrative Examples on Lightweight Cryptographic Primitives”, to appear in *Security of Ubiquitous Computing Systems*, Eds. G. Avoine and J. Hernandez-Castro, Springer, pp. 21-47, Springer 2021.

76. **M.J. Mihaljevic** and H. Imai, "Security Issues of Cloud Computing and a Dedicated Encryption Approach", to appear as a book chaper in *High Performance and Cloud Computing in Scientific Research and Education*, IGI Global, US, pp. 388-408, March 2014. (DOI: 10.4018/978-1-4666-5784-7, ISBN13: 9781466657847, ISBN10: 1466657847, EISBN13: 9781466657854)

77. **M.J. Mihaljevic**, "On Certain Approaches for Analysis and Design of Cryptographic Techniques for Symmetric Encryption and Key Management", in *Selected Topics of Image Processing and Cryptology*, *Zbornik Radova* , vol. 15, pp. 119-186, Mathematical Institute, Serbian Academy of Sciences and Arts, Belgrade, Dec. 2012. (ISBN: 978-86-80593-47-0, ISSN: 0351-9406)
http://elib.mi.sanu.ac.rs/files/journals/zr/23/mihaljevic2.pdf

78. **M.J. Mihaljevic**, "A Framework for Stream Ciphers Based on Pseudorandomness, Randomness and Error-Correcting Coding", in *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes*, Editors B. Preneel, S. Dodunekov, V. Rijmen and S. Nikova, Vol. 23 in the Series Information and Communication Security, pp. 117-139, IOS Press, Amsterdam, The Netherlands, June 2009. (ISSN: 1874-6268; ISBN: 978-1-60750-002-5) DOI: 10.3233/978-1-60750-002-5-117

79. **M. Mihaljevic**, "Decimation Based Correlation and Algebraic Attacks and Design of Boolean Functions", in *Boolean Functions in Cryptology and Information Security*, Editors B. Preneel and O. A. Logachev, Vol. 18 in the Series - D: Information and Communication Security, IOS Press, Amsterdam, The Netherlands, pp. 183-199, July 2008. (ISSN: 1874-6268; ISBN 978-1-58603-878-6)

80. M. Matsui and **M. Mihaljevic**, "Security Evaluation Techniques for Symmetric Cryptography", Chapter in *Information Security Handbook*, Editors H. Imai and E.

Okamoto, IEICE, Ohmusha Ltd., Tokyo, Japan, pp. 145-160, 2004.(in Japanese) (ISBN 4-274-07980-5)

Selected Papers in Proceedings of the International Conferences

81. M. Todorović, M. Knežević, D. Ševerdija, S. Jelić, and **M.J. Mihaljević**, "Implementation Framework of a Blockchain Based Infrastructure for Electricity Trading within a Microgrid", EAI CollaborateCom 2023 - 19th EAI International Conference on Collaborative Computing: Networking, Applications and Worksharing", October 4-6, 2023, Corfu Island, Greece Proceedings, 16 pages, to appear, Springer 2024.

82. S. Xu, F. Wang, L. Wang, **M.J. Mihaljevic**, S. Zhang, W. Shao and Q. Huang, "Trusted Auditing of Data Operation Behaviors in Cloud based on Blockchain and TEE", IEEE ISPA 2023, 21-24 December, 2023, Wuhan, China, Proceedings (to appear), 2023

83. M. Savic, N. Vuksa, **M.J. Mihaljevic**, "An architecture for verified medical data distribution employing blockchain technology", in *Mathematics for human flourishing in the time of COVID-19 and post COVID-19* , pp. 41-52, De Gruyter, 2023. ISBN 978-3-11-073862-9

84. A. Kavcic, **M.J. Mihaljevic**, and K. Matsuura, "Light-Weight Secrecy System Using Channels with Insertion Errors: Cryptographic Implications", *IEEE Information Theory Workshop (ITW)* 2015, Jeju Island, Korea, 11-15 Oct. 2015, *Proceedings*, pp. 257-261, 2015.

85. **M.J. Mihaljevic**, "Light-Weight and Provable Secure Cryptographic Techniques - The Key Components for Cyber Security and Efficient Smart Grid Deployment", *Global Wireless Summit (GSW)* 2013, Atlantic City, US, June 24-27, *GSW 2013 Record*, River Publishers, US, pp. 141-142. (print ISBN: 978-87-92982-51-3; cd ISBN: 978-87-92982-52-0)

86. **M.J. Mihaljevic**, and A. Kavcic, "An Approach for Reduction of the Security Overhead in Smart Grid Communication Infrastructure Employing Dedicated Encryption", *The Twelfth International Conference on Networks - ICN 2013* at *IARIA GlobNet-2013*, Jan. 27 - Feb. 1, 2013, Seville, Spain *Proceedings of ICN-2013*, pp. 46-52 (ISBN: 978-1-61208-245-5)

87. **M.J. Mihaljevic**, "An Approach for Light-Weight Encryption Employing Dedicated Coding", *Proceedings of IEEE GLOBECOM 2012*, pp. 892-898, Dec 2012. ISBN: 978-1-4673-0919-6 (and IEEE Xplore http://ieeexplore.ieee.org/xpl/conhome.jsp?punumber=1000308)

88. **M.J. Mihaljevic**, H. Imai, M. David, K. Kobara and H. Watanabe, "On Advanced Cryptographic Techniques for Information Security of Smart Grid AMI", *Proceedings of the Seventh Annual Workshop on Cyber Security and Information*

Intelligence Research - CSIIRW 2011,Oak Ridge National Laboratory, Tennessee, US, October 11-14, ACM International Conferences Series, March 2012. ISBN: 978-1-4503-0945-5; doi: 10.1145/2179298.2179371 (Article no. 64, 4 pages)

89. **M.J. Mihaljevic** and H. Imai, "An Information-Theoretic and Computational Complexity Security Analysis of a Randomized Stream Cipher Model",
4th Western European Workshop on Research in Cryptology - WEWoRC 2011, July 20-22, 2011, Weimar, Germany, Conference Record, pp. 21-25.
http://2011.weworc.org/
http://www.uni-weimar.de/cms/fileadmin/medien/medsicherheit/WEWoRC2011/files/conference_record3.pdf#page=27

90. **M.J. Mihaljevic** and H. Imai, "OEmployment of Homophonic Coding for Improvement of Certain Encryption Approaches Based on the LPN Problem",
2011 Symmetric Key Encryption Workshop - SKEW 2011, Copenhagen, Denmark, February 16-17, 2011, E-Proceedings (17 pages).
http://skew2011.mat.dtu.dk/program.html
http://skew2011.mat.dtu.dk/proceedings/Employment%20of%20Homophonic%20Coding%20for%20Improvement%20of%20Certain%20Encryption%20Approaches%20Based%20on%20the%20LPN%20Problem.pdf

91. **M.J. Mihaljevic** and H. Imai, "A Security Evaluation of Certain Stream Ciphers which Involve Randomness and Coding",
2010 Int. Symp. on Inform. Theory and its Appl. - ISITA 2010, Taichung, Taiwan, Oct. 17-20, 2010, Proceedings, pp. 789-794, IEEE, 2010.
DOI: 10.1109/ISITA.2010.5649616
(IEEE Catalog Number: CFP 10767-USB; ISBN: 078-1-4244-6014-4; Print ISBN: 978-1-4244-6016-8; ISSN: 1943-7439)
http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5649616

92. **M.J. Mihaljevic**, H. Watanabe and H. Imai, "A Low Complexity Authentication Protocol Based on Pseudorandomness, Randomness and Homophonic Coding",
2010 Int. Symp. on Inform. Theory and its Appl. - ISITA 2010, T, Taichung, Taiwan, Oct. 17-20, 2010, Proceedings, pp. 690-695, IEEE, 2010.
DOI: 10.1109/ISITA.2010.5649666
(IEEE Catalog Number: CFP 10767-USB; ISBN: 078-1-4244-6014-4; Print ISBN: 978-1-4244-6016-8; ISSN: 1943-7439)
http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5649666

93. **M.J. Mihaljevic**, S. Gangopadhyay, G. Paul and H. Imai, "A Generic Weakness of the k-normal Boolean Functions Exposed to Dedicated Algebraic Attack",
2010 Int. Symp. on Inform. Theory and its Appl. - ISITA 2010, Taichung, Taiwan, Oct. 17-20, 2010, IEEE Proceedings, pp. 911-916.
DOI: 10.1109/ISITA.2010.5649555
(IEEE Catalog Number: CFP 10767-USB; ISBN: 078-1-4244-6014-4; Print ISBN: 978-1-4244-6016-8; ISSN: 1943-7439)
http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5649555

94. M. Fossorier, **M.J. Mihaljevic** and H. Imai, "Time-Memory and Time-Memory-Data Trade-O®s for Noisy Ciphertext",

Proceedings of the ECRYPT Workshop on Tools for Cryptanalysis 2010, Francois-Xavier Standaert (Ed.), pp. 27-36, June 2010.
(Proceedings available at: http://www.ecrypt.eu.org/symlab/tools2010/tools2010-proceedings.pdf

95. **M.J. Mihaljevic**and F. Oggier, "A Wire-tap Approach to Enhance Security in Communication Systems using the Encoding-Encryption Paradigm",
2010 IEEE 17th International Conf. on Telecommunications - ICT 2010, Proceedings, pp. 484-489, April 2010., pp. 83-88
DOI: 10.1109/ICTEL.2010.5478824
(E-ISBN: 978-1-4244-5247-7 Print ISBN: 978-1-4244-5246-0)
(Proceedings available at:
http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5478824

96. **M.J. Mihaljevic** and H. Imai, "A Stream Cipher Design Based on Embedding of Random Bits",
IEEE 2008 Int. Symp. on Inform. Theory and its Appl. - ISITA2008, Auckland, New Zealand, Dec. 7-10, 2008, Proceedings, pp. 1497-1502. (ISBN: 978-1-4244-2069-8; Library of Congress: 2008900302; copyright2008 IEEE)

97. **M.J. Mihaljevic**, H. Watanabe and H. Imai, "A Cellular Automata Based HB#-like Low Complexity Authentication Technique",
IEEE 2008 Int. Symp. on Inform. Theory and its Appl. - ISITA2008, Auckland, New Zealand, Dec. 7-10, 2008, Proceedings, pp. 1355-1360. (ISBN: 978-1-4244-2069-8; Library of Congress: 2008900302; copyright2008 IEEE)

98. M. Fossorier, **M. Mihaljevic** and H. Imai, "Decimation Based Fast Correlation Attack",
2007 IEEE Int. Symp. Inform. Theory - ISIT'2007, Nice, France, June 24-29, 2007, Proceedings, pp. 456-460. (ISBN 1-4244-1429-6).

99. 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).

100. **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, Hawaii, USA, May 2005, Proceedings, pp. 183-188 (ISBN 4-902087-13-8).

101. **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.)

102. **M. Mihaljevic** and H. Imai, "Framework of a novel technique for algebraic and fast correlation attacks based on dedicated sample decimation",
The State of the Art of Stream Ciphers - SASC2004, Bruge, Belgium, October 2004,

Workshop Record, pp. 190-201.

103. **M. Mihaljevic**, M.P.C. Fossorier and H. Imai, "One-way mapping of keys and the overheads trade-off in key management schemes for broadcast encryption", *Int. Symp. Inform. Theory and its Appl. - ISITA2004*, Parma, Italy, October 2004, Proceedings, pp. 486-491.

104. **M. Mihaljevic** and H. Imai, "A method for data access control in certain storage area networks", *7th Int. Symp. on Wireless Personal Multimedia Comm. - WPMC2004*, Albano Terme, Italy, September 2004, Proceedings, pp. V3:488-491.

105. **M. Mihaljevic**, M.P.C. Fossorier and H. Imai, "An Improved Fast Correlation Attack Based on List Decoding", *IEEE Int. Symp. Inform. Theory - ISIT'2003*, Yokohama, Japan, July 2003, Proceedings, p.165.

106. **M. Mihaljevic** and R. Kohno, "On a framework for employment of cryptographic components in software defined radio", *IEEE WPMC'02 - The 5th Int. Symp. on Wireless Personal Multimedia Communications*, Honolulu, Hawaii, USA, October 2002, Proceedings, vol. II, pp. 835-839.

107. L. Michael, **M. Mihaljevic**, S. Haruyama and R. Kohno, "A proposal of architectural elements for implementing secure software download service in software defined radio", *IEEE PIMRC 2002 - The 13th IEEE Int. Symp. on Personal, Indoor and Mobile Radio Communications*, Lisbon, Portugal, September 2002, Proceedings, vol. I, pp. 442-446.

108. P. Camion, **M. Mihaljevic** and H. Imai, "Two allerts for design of certain stream ciphers: Trapped LFSR and weak resilient function over GF(q)", *Selected Areas in Cryptography - SAC2002*, St.John's, Newfoundland, Canada, August 2002, Conference Record, pp. 203-217.

109. **M. Mihaljevic** and R. Kohno, "Security issues of downloading for software reconfigurable radio systems versus usual Internet downloading", *invited talk, XXVIIth General Assembly of the International Union of Radio Science*, Maastricht, The Netherlands, Aug. 2002, Proceedings, 4 pages.

110. P. Camion, **M. Mihaljevic** and H. Imai, "On employment of LFSRs over GF(q) in certain stream ciphers", *IEEE Int. Symp. Inform. Theory - ISIT'2002*, Lausanne, Switzerland, July 2002, Proceedings, p. 210.

111. **M. Mihaljevic** and R. Kohno, "On wirelss communications privacy and security evaluation of encryption techniques", *IEEE Wireless Communications and Networking Conf. - WCNC2002*, Orlando, FL, USA, March 2002, Proceedings, pp. 865-868.

112. **M. Mihaljevic** and R. Kohno, "Cryptographic evaluation of a fast encryption for multimedia",

SONY Research Forum - SRF2001, Tokyo, Japan, Dec. 2001, Proceedings, pp. 59-64, March, 2002.

113. **M. Mihaljevic** and H. Imai, "On employment of different weigth parity-checks for the fast correlation attack",
IEEE Int. Symp. Inform. Theory - ISIT'2001, Washington, D.C., USA, June 2001, Proceedings p. 119.

114. **M. Mihaljevic**, M.P.C. Fossorier and H. Imai, "Fast correlation attack algorithm with the list decoding and an application",
Fast software Encription Workshop - FSE2001, Yokohama, Japan, April, 2001, Pre-proceedings, pp. 208-222.

115. **M. Mihaljevic**, M.P.C. Fossorier and H. Imai, "A time-memory trade-off for the fast correlation attack",
ISITA2000, Hawaii, USA, Nov. 2000, Proceedings, pp. 55-58.

116. P. Camion, **M. Mihaljevic** and H. Imai, "Vulnerability of certain keystream generators based on resilient functions",
ISITA2000, Hawaii, USA, Nov. 2000, Proceedings, pp. 70-73.

117. H. Imai, **M. Mihaljevic**, M. Isaka and M.P.C. Fossorier, "Applications of iterative decoding techniques to cryptography",
2nd Int. Symp. on Turbo Codes & Related Topics, Brest, France, Sept. 2000, *invited paper*, Proceedings, pp. 227-234.

118. **M. Mihaljevic**, M.P.C. Fossorier and H. Imai, "Novel fast correlation attack via iterative decoding of punctured simplex code",
IEEE ISIT'2000, Sorento, Italy, June 2000, Proceedings p. 214

119. **M. Mihaljevic**, M.P.C. Fossorier and H. Imai, "A low-complexity and high-performance algorithm for the fast correlation attack", Pre-proceedings,
Fast Software Encryption Workshop - FSE2000, New York, USA, April 2000,

120. **M. Mihaljevic**, M.P.C. Fossorier and H. Imai, "A novel fast correlation attack suitable for simple hardware implementation",
Proc. JW-ISC'2000, pp.1-8, Okinawa, Japan, Jan. 2000; also published as *Technical report of IEICE: ISEC99-74*, pp 1-8, Jan. 2000.

121. **M. Mihaljevic**, Y. Zheng and H. Imai, "A Fast and Secure Stream Cipher Based on Cellular Automata over GF(q)",
IEEE GLOBECOM '98, Sydney, Australia, Nov. 1998, Proceedings, pp. 3250-3255.

122. **M. Mihaljevic** and H. Imai, "Construction of Fast MAC Based Linear Cellular Automata
GF(q)",
ISITA '98 - 1998 IEEE Int. Symp. on Information Theory and Its Applications, Mexico, Mexico-City, Oct. 1998, Proceedings, pp. 40-43.

123. M. Fossorier, **M. Mihaljevic** and H. Imai, "Reduced Complexity Iterative Decoding of Low Density Parity Check Codes Based on Belief Propagation",

ISITA '98 - 1998 IEEE Int. Symp. on Information Theory and Its Applications, Mexico, Mexico-City, Oct. 1998, Proceedings, pp. 654-658.

124. **M. Mihaljevic**, Y. Zheng and H. Imai, "A Fast Cryptographic Hash Function Based on Cellular Automata over GF(q)",
in *Global IT Security*, IFIP, pp. 96-107, 1998 (Proc. 14th IFIP Int. Conf. on Information Security at 15th World Comput. Congress - IFIP/SEC '98, Vienna - Budapest, Sept. 1998).

125. **M. Mihaljevic**, "Fast Reconstruction of the Programmable Cellular Automata Initial State Using Ciphertext Only",
4th International Symposium on Communication Theory and Applications, UK, Lake district, July 1997, Proceedings, 5 pages.

126. **M. Mihaljevic**, J. Dj. Golic, "A Method for Convergence Analysis of Error-Correction Decoding",
ISITA '96 - 1996 IEEE International Symposium on Information Theory and Its Applications, Canada, Victoria, B.C., Sept. 1996, Proceedings, pp. 802-805.

127. **M. Mihaljevic** "Effective Key Size Estimation of the Self-Shrinking Generator",
ISITA '96 - 1996 IEEE International Symposium on Information Theory and Its Applications, Canada, Victoria, B.C., Sept. 1996, Proceedings, pp. 250-253.

128. **M. Mihaljevic**, "Security Examination of Certain Cellular Automata Based Key Stream Generator",
ISITA '96 - 1996 IEEE International Symposium on Information Theory and Its Applications, Canada, Victoria, B.C., Sept. 1996, Proceedings, pp. 246-249.

129. **M. Mihaljevic**, "Security Examination of a Key Stream Generator Based on Programmable Cellular Automata with ROM",
4th UK / Australian International Symposium on DSP for Communication Systems, Australia, Perth, Sept. 1996, Proceedings, pp.53-60.

130. **M. Mihaljevic**, "Novel Sequence Comparison Approaches for Binary Information Strings",
PSI'96: Perspectives of System Informatics - Andrei Ershov Second International Memorial Conference, Russia, Novosibirsk, Academgorodok, June 1996, Proceedings, pp. 273-277.

131. **M. Mihaljevic**, "Novel Tests for the Security Examination of Pseudorandom Bit Generators",
International Symposium on Information Theory and Its Applications 1994 (ISITA '94), Australia, Sydney, Nov. 1994, Proceedings, pp. 277-282.

National Journals

132. **M. Mihaljevic** "On Certain Coding Approaches for Security Evaluation and Design of Stream Ciphers",
Transaction on Advanced Research, vol. 8, no. 2, July 2012, pp. 28-34 (ISSN 1820 -

4511; http://www.internetjournals.net/)

133. **M. Mihaljevic**, Y. Watanabe and H. Imai, "Security evaluation of stream ciphers",
Computer Today, vol. 107, pp. 4-10, Jan. 2002. (in Japanese)

134. **M. Mihaljevic** and Z. Markovic, "On cryptographic approaches for security of information technologies",
Facta Universitatis, vol. 2 (10), pp. 1393-1402, Oct. 2000. (ISSN: 1820-6417)

135. **M. Mihaljevic**, D. Stijovic, B. Maric, S. Popadic i M. Ivanovic, "Koncept za uporedjivanje i uporedni pregled tri tehnike za zastitu informacionih sistema: Kerberos, SESAME i SSH",
Info-Science, br. 6, str. 8-13, decembar 1999. (ISSN: 0354-5334)

136. **M. Mihaljevic**, D. Stijovic, B. Maric, S. Popadic i M. Ivanovic, "Elektronska trgovina, elektronski novac i kriptografske tehnike: Jedan osvrt na savremene trendove",
JISA-INFO, br. 4, str. 31-34, jul-avgust 1999. (ISSN: 0354-5334)

137. **M. Mihaljevic** and H. Imai, "A message authentication approach for for information systems",
Info-Science, vol. 7, no. 1, pp. 4-7, Jan. 1999. (ISSN: 0354-5334)

138. **M. Mihaljevic** and Z. Savic, "Zastita privatnosti informacija",
Info-Science, vol. 3, no. 6, pp. 28-34, 1995.(ISSN: 0354-5334)

Selected Miscellaneous Publications

139. **M.J. Mihaljević**, "Ilustrativni napretci u tehnikama kriptologije i blokčejn tehnologije" ("Illustrative Advances in Cryptology and Blockchain Technology Techniques"),
Naučni simpozijum Nauka i male zemlje: Sinergija Dijaspore, Matice i Prijatelja Crne Gore, Zbornik radova, knjiga 162, str. 409-415, Crnogorska Akademija Nauka i Umetnosti, 2023.

140. **M.J. Mihaljević**, "Artificial Intelligence for Blockchain Technology and Vice Versa",
Keynote Talk at *The Second Serbian International Conference on Applied Artificial Inteligence (SICAAI),*
May 19-20, 2023, Kragujevac, Serbia, Book of Abstracts, p. 23, ISBN 978-86-81037-77-5

141. **M.J. Mihaljević**, "Illustrative Examples on Interactions of Artificial Intelligence and Blockchain Technology",
Keynote Talk, *2022 International High-End Technology Seminar on Artificial Inteligence*, Jinan, China, 13-15 Sept. 2022

142. M. Savić, M. Todorović, **M.J. Mihaljević** , „Softver novog blokčejn

konsenzus protokola i modifikovane Ethereum platforme“
("Software of a Novel Blockchain Consensus Protocol and a Modified Etherum Platform"),
Tehničko rešenje (referisano u [10]) (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2020.

143. M. Knežević, S. Tomović, **M.J. Mihaljević** , „Softver za evaluaciju sigurnosti klase autentikacionih protokola“
("Software for Security Evaluation of a Class of Authentication Protocols"),
Tehničko rešenje (referisano u [9] i [11]) (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2020.

144. **M.J. Mihaljevic,** "On Some Advanced Techniques for Lightweight Blockchain Technology and Certain Applications",
Invited Talk at the *International Supercomputing Industry Expo 2019*, Jinan, China, Dec. 26-28, 2019.

145. **M.J. Mihaljevic,** K. Matsuura, "On the Consensus Protocols for Public Blockchains",
Invited Talk at a Panel of *Interop Tokyo 2019* , 12-14 June 2019, Tokyo, Japan;
https://www.interop.jp/?lang=en

146. Tomović, Siniša; **M.J. Mihaljevic,**; Todorović, Milan, "Softver blokčejn sistema za upravljanje digitalnim pravima",
(Software of a Blockchain Based System for Digital Rights Management")
Tehničko rešenje (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2019.

147. Vukša, Nikolina; Savić, Milan; **M.J. Mihaljevic,**, "Softver blokčejn sistema za kontrolu porekla poljoprivrednih proizvoda"
("Software of a Blockchain Based System for Origin Control of Farmers' Products"),
Tehničko rešenje (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2019.

148. Knežević, Milica; Todorović, Milan; **M.J. Mihaljevic,**, "Softver blokčejn sistema za kontrolu integriteta podataka u oblaku"
("Software of a Blockchain Based System for Data Integrity Control in Cloud"),
Tehničko rešenje (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2019.

149. **M.J. Mihaljevic,** "On Certain Challenges of Blockchain Technology Deployment”,
Invited talk, *ETRAN (IcETRAN) 2018, 5th International Conference on Electrical, Electronic and Computing Engineering* , Palic, Serbia, June 11 - 14, 2018.
https://www.etran.rs/2018/IcETRAN/Recorded_events/ &
https://www.youtube.com/watch?v=F6IzKkokTj4

150. Todorović, Milan; **Mihaljević, Miodrag J.**; Arsić, Aleksandra, "Softver za implementaciju konsenzus protokola na bazi dokaza kapaciteta invertovanja jednosmerne funkcije korišćenjem Ethereum platforme"
("Software of the Blockchain Consensus Protocol Based on Proof of Inversion

Capacity for a Modification of Ethereum Platform"),
Tehničko rešenje (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2018

151. **Mihaljević, Miodrag J.**; Tomović, Siniša, "Metod za ostvarivanje konsenzusa na bazi dokaza kapaciteta invertovanja jednosmerne funkcije u otvorenim blokčejn sistemima"
("A Method for the Consensus Protocol Based on Proof of Inversion Capacity in Public Blockchain Systems"),
Tehničko rešenje (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2018

152. Urošević, Dragan; **Mihaljević, Miodrag J.**; Knežević, Milica, "Metod i softver za blokčejn zasnovanu kontrolu integriteta podataka u udaljenim skladištima"
("A Method and Software for Blockchain Based Data Integrity Control in Remote Strorages"),
Tehničko rešenje (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2018

153. **Mihaljević, Miodrag J.**; Arsić, Aleksandra, "Metod i softver za jednosmernu funkciju u klasi konsenzus protokola za blokčejn tehnologiju"
("A Method and Software for the One-Way Function in a Class of Blockchain Consensus Protocols"),
Tehničko rešenje (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2018

154. Korać, Vanja; Todorović, Milan; **Mihaljević, Miodrag J.**, "Metod i realizacija inicijalne zaštite bibliometrijskog sistema Ministarstva prosvete, nauke i tehnološkog razvoja"
("Method and Implementaion of the Initial Protection for the Bibliometric System of the Ministry for Education, Science and Technological Development"),
Tehničko rešenje (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2017.

155. **Mihaljević, Miodrag J.** ; Knežević, Milica ; Tomović, Siniša "Metod i softver za napredne tehnike za evaluaciju sigurnosti klase autentikacionih protokola"
("Method and Software for Advanced Security Evaluation of a Class of Authentication Protocols")
Tehničko rešenje (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2017.

156. **Mihaljević, Miodrag J.**; Arsić, Aleksandra; Jelisavčić, Vladisav, "Metod i softver za napredne tehnike za zaštitu tajnosti sa asimetričnom implementacionom složenošću"
("Method and Software for Advanced Security Evaluation of a Class of Authentication Protocols")
Tehničko rešenje (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2017.

157. **Mihaljević, Miodrag J.**; Knežević, Milica; Tomović, Siniša, "Metod i softver za napredne tehnike za autentikaciju u domenu Cloud i Big Data"

("Method and Software for Advanced Security Evaluation of a Class of Authentication Protocols"),
Tehničko rešenje (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2016.

158. **Mihaljević, Miodrag J.**; Knežević, Milica; Jelisavčić, Vladisav; Zdravković, Aleksandra, "Metod i softer za napredne tehnike za zaštitu tajnosti/privatnosti u domenu IoT i M2M"
("Method and Software for Advanced Techniques for Security/Privacy Protection in IoT and M2M Domains"),
Tehničko rešenje (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2016.

159. **Mihaljević, Miodrag J.**; Arsić, Aleksandra ; Tomović, Siniša ; Perović, Aleksandar; Ognjanović, Zoran "Metod i softver za napredne tehnike za autentikaciju u domenu IoT i M2M"
("Method and Software for Advanced Techniques for Authentication in IoT and M2M Domains"),
Tehničko rešenje (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2016.

160. **Mihaljević, Miodrag J.**; Ognjanović, Zoran; Šegan-Radonjić, Marija; Vujošević, Sandra, "Metod za prilagođeno upravljanje privatnošću informacija kroz implementaciju principa iz familije standarda ISO 29100"
("Customized Method for Privacy Management Employing Recommendation from ISO 29100 Standards"),
Tehničko rešenje (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2016.

161. **Mihaljević, Miodrag J.**; Korać, Vanja; Todorović, Milan; Marinković, Bojan, "Kastomizovani metod i softfer za federativno upravljanje identitetima FIM (Federated Identity Management)"
("Customized Method and Software for Federated Identity Management (FIM)"),
Tehničko rešenje (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2016.

162. Korać, Vanja; Jelisavčić, Vladisav; **Mihaljević, Miodrag J.**; Todorović, Milan; Davidovac, Zoran, "Metod i softver za zaštitu sistema sa digitalizovanim dokumentima o spoljnoj politici Kraljevine Srbije 1903-1914"
("Method and Software for Information Security of the System with Digtal Documents on Foreign Affairs of Kingdom Serbia, 1903-1914"),
Tehničko rešenje (Technical Report),
Mathematical Institute, The Serbian Academy of Sciences and Arts, Belgrade, 2016.

163. **M. Mihaljevic** , M. Todorovic, P. Maksimovic, S. Roksandic, M. Milojevic-Jevric, B. Marinkovic, "Evaluacija podataka o ostvarivanju napredne informacione bezbednosti u Cloud Computing (A Comprehensive Overview of Colud Computing Security Issues)",
Studija - Evaluacija, MI-SANU, Beograd, Dec. 2013

164. **M. Mihaljevic**, S. Roksandic, M. Laban, B. Marinkovic, "Evaluacija podataka

o ostvarivanju napredne informacione bezbednosti za M2M (masina-masina) komunikacije u okviru IoT (Internet of Things) (A Comprehensive Overview of Machine-to-Machine Secure Communications over IoT)",
Studija - Evaluacija, MI-SANU, Beograd, Dec. 2013

165. H. Imai and **M.J. Mihaljevic**, "Cryptography Policy of Japan and CRYPTREC" *Invited talk, BalkanCrypt 2013*, Sofia, Bulgaria, 07-08 Nov., 2013.
http://balkancrypt.uist.edu.mk/docs/imai_mihaljevic_policy.pdf
http://balkancrypt.uist.edu.mk/abstracts.html

166. **M.J. Mihaljevic** and H. Imai, "Towards Lightweight Cryptographic Primitives Employing Coding Theory", *Invited talk, BalkanCrypt 2013*, Sofia, Bulgaria, 07-08 Nov., 2013.
http://balkancrypt.uist.edu.mk/docs/mihaljevic_imai_lightweight.pdf
http://balkancrypt.uist.edu.mk/abstracts.html

167. **M.J. Mihaljevic**, (one of the co-authors), *Specification of algorithms for static reconfiguration of Ad-Hoc network, for security and authentication and multimedia services*.
Technical Report, EU FP6 Project No. 026548, ADHOCSYS, Deliverable D11, 237 pages, Feb. 2007.

168. **M.J. Mihaljevic**, (one of the co-authors), *Software implementation, partial prototype*.
Technical report, EU FP6 Project No. 026548, ADHOCSYS, Deliverable D13, 75 pages, Feb. 2007.

169. **M. Mihaljevic**, *Report on Security Evaluation of RC4 Stream Cipher*.
Peer Reviewed Technical Report, *CRYPTREC*, Information-technology Promotion Agency (IPA), Japan, Tokyo, 51 pages, Sept. 2002.

170. **M. Mihaljevic**, *Report on Security Evaluation of MUGI Stream Cipher*.
Peer Reviewed Technical Report, *CRYPTREC*, Information-technology Promotion Agency (IPA), Japan, Tokyo, 47 pages, Sept. 2002.

171. **M. Mihaljevic**, *Report on Security Evaluation of PANAMA Stream Cipher*.
Peer Reviewed Technical Report, *CRYPTREC*, Information-technology Promotion Agency (IPA), Japan, Tokyo, 36 pages, Dec. 2001.

172. **M.J. Mihaljevic**, Z. Markovic and T. Davidovic, "Security Evaluation of Certain Advanced Cryptographic Techniques for GSM network at Division for Mobile Telephony of Telecom Serbia", ("Tehnicki izvestaj o evaluaciji kriptografske sigurnosti odredjenih kriptografskih tehnika od perspektivnog interesa za GSM mrezu Mobilne telefonije, Telekoma Srbije"),
Technical Report, Mathematical Institute, Serbian Academy of Sciences and Arts, Belgrade, 73 pages, May 2008.

173. **M. Mihaljevic**,"A standardized framework for information security of the E-Register" (Prikaz opsteg standardizovanog okvira za ostvarivanje informaticke bezbednosti Elektronskog Registra u njegovom integralnom okruzenju - Projekat razvoja i implementacije savremenog eletronskog registra u Republickoj direkciji za

imovinu),
Technical Report, Mathematical Institute, Serbian Academy of Sciences and Arts, Belgrade, 55 pages, Dec. 2008.

174. **M. Mihaljevic**,"An overview on security evaluation of certain cryptographic primitives" (Evaluacija sigurnosti odredjenih kriptografskih resenja - Projekat razvoja i implementacije savremenog eletronskog registra u Republickoj direkciji za imovinu),
Technical Report, Mathematical Institute, Serbian Academy of Sciences and Arts, Belgrade, 33 pages, Dec. 2008.

175. **M. Mihaljevic**, "A comparison of certain RSA and Entrust PKI systems: Elements of the methodology for comparison of PKI systems" ("Elaborat o uporednoj tehnickoj analizi odredjenih PKI resenja RSA i Entrust: Metodolololoski elementi za evaluaciju i poredjenje PKI sistema"),
Technical Report, Centralna Banka Crne Gore, Podgorica, 34 pages, Dec. 2008.

176. **M.J. Mihaljevic**, Z. Markovic and Z. Ognjanovic, "Security Evaluation of the Cryptographic Techniques in GSM network for the Data Services at Division for Mobile Telephony of Telecom Serbia", ("Tehnicki izvestaj o evaluaciji kriptografske sigurnosti tehnika za zastitu negovornih servisa Mobilne telefonije, Telekoma Srbije"),
Technical Report, Mathematical Institute, Serbian Academy of Sciences and Arts, Belgrade, 60 pages, Dec. 2007.

177. **M.J. Mihaljevic**, Z. Markovic, Z. Perisic and M. Markovic, *Frameworks and Particular Elements for Business Continuity and Disaster Recovery of IT system in IT Infrastructure Management Department, IT Division, Telecom Serbia* (Metodoloska osnova, genericki elementi i odredjena pravila za upravljanje kontinuitetom IT poslovanja i oporavkom sistema u Sektoru za upravljanje IT platformama, Direkcije za IT, Telekoma Srbija).
Collection of Technical Reports, Volumes I - VIII, Mathematical Institute, Serbian Academy of Sciences and Arts, Belgrade, in total more than 300 pages, Nov. 2007.

178. **M.J. Mihaljevic**, Z. Markovic and Z. Ognjanovic, "Security Evaluation of the Cryptographic Techniques in GSM network for the Speach Service at Division for Mobile Telephony of Telecom Serbia", (``Tehnicki izvestaj o evaluaciji kriptografske sigurnosti tehnika za zastitu govornog servisa Mobilne telefonije, Telekoma Srbije"),
Technical Report, Mathematical Institute, Serbian Academy of Sciences and Arts, Belgrade, 59 pages + Appendix, Sept. 2007.

179. **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.

180. **M. Mihaljevic**, M.P.C. Fossorier, M. Isaka and H. Imai, "Evaluation of certain stream ciphers via message-passing decoding techniques",
2000 Workshop on Information-Based Induction Sciences (IBIS2000), Izu, Japan, July 17-18, 2000, Proceedings, 6 pages.

181. **M.J. Mihaljevic** and H. Imai, "Privacy Preserving Light-Weight

Authentication Based on a Variant of Niederreiter Public-Key Encryption",
Symp. on Crypology and Information Security - SCIS 2014, Kagoshima, Japan, 21-24 January 2014, Proceedings, paper no. 2B4-3, 6 pages.

182. R. Hosoya, T. Kitagawa, **M.Mihaljevic**, K. Kobara and H. Imai, "An Authentication Protocol Based on a Variant of Niederreiter Public-Key Encryption",
Symp. on Crypology and Information Security - SCIS 2014, Kagoshima, Japan, 21-24 January 2014, Proceedings, paper no. 3F3-2, 6 pages.

183. K. Yanagishima, T. Kitagawa,**M.Mihaljevic** and H. Imai, "On computational complexity required to completely identify the key from the CPA results",
Symp. on Crypology and Information Security - SCIS 2014, Kagoshima, Japan, 21-24 January 2014, Proceedings, paper no. 2A4-4, 6 pages.

184. **M. Mihaljevic** and G. Hanaoka, "A Framework for Provably Secure and Light-Weight Stream Cipher Like Encryption Based on the LPN Problem and Dedicated Coding",
The 2013 Symposium on Cryptography and Information Security - SCIS2013, Kyoto, Japan, January 22-25, 2013, CD-ROM Proceedings, paper #2B4-3, 7 pages.

185. **M. Mihaljevic** and G. Hanaoka, "A Framework for Light-Weight Authentication Based on the LPN Problem and Random Selection",
The 2013 Symposium on Cryptography and Information Security - SCIS2013, Kyoto, Japan, January 22-25, 2013, CD-ROM Proceedings, paper #2D3-2, 6 pages.

186. **M. Mihaljevic** and H. Imai, "Improved fast correlation attack based on highly restricted search minimum distance decoding",
The 2001 Symposium on Cryptography and Information Security - SCIS2001, Oiso, Japan, January 23-26, 2001, Proceedings, pp. 283-288.

187. **M. Mihaljevic** and H. Imai, "Improved decimation attack based on matrix characterization of LFSR",
The 2001 Symposium on Cryptography and Information Security - SCIS2001, Oiso, Japan, January 23-26, 2001, Proceedings, pp. 289-291.

188. **M. Mihaljevic** and H. Imai, "Effective secret key size of TOYOCRYPT-HS1 stream cipher",
The 2001 Symposium on Cryptography and Information Security - SCIS2001, Oiso, Japan, January 23-26, 2001, Proceedings, pp. 665-667.

189. **M. Mihaljevic**, "Zastita podataka na Internetu",
Internet i savremeno poslovanje, Beograd, str. 281-300, 1998.

190. **M. Mihaljevic**, J. Golic, "A Parity-Check Weight Distribution for Maximum-Length Sequences",
Second International Conference on Finite Fields, SAD, Las Vegas, Aug. 1993, Abstracts p. 35.

191. J. Golic and **M. Mihaljevic**, "On a binary sequence generator",
EUROCRYPT '89, Belgium, Houthalen, Apr. 1989, Ext. Abstracts pp. 59.1-59.6.