PUBLICATIONS

Jovan Dj. Golić

December 1999

Papers in Refereed International Journals and Book Series

1. J. Dj. Golić, "Cryptanalysis of three mutually clock-controlled stop/go shift registers," *IEEE Trans. Inform. Theory*, to appear.

2. M. Mihaljević and J. Dj. Golić, "A method for convergence analysis of iterative probabilistic decoding," *IEEE Trans. Inform. Theory*, to appear.

3. R. Menicocci and J. Dj. Golić, "Edit probability correlation attack on the bilateral stop/go generator," Cryptography and Coding - Cirencester '98, *Lecture Notes in Computer Science*, Springer-Verlag, to appear.

4. J. Dj. Golić, M. Salmasizadeh, and E. Dawson, "Fast correlation attacks on the summation generator," *Journal of Cryptology*, to appear.

5. H. Gustafson, E. Dawson, J. Dj. Golić, and A. Pettitt, "Methods for testing subblock patterns," *Statistics and Computing*, to appear.

6. J. Dj. Golić, "Linear models for a time-variant permutation generator," *IEEE Trans. Inform. Theory*, vol. IT-45, pp. 2374-2382, Nov. 1999.

7. J. Dj. Golić, "Iterative probabilistic decoding and parity checks with memory," *Electronics Letters*, vol. 35(20), pp. 1721-1723, Sept. 1999.

8. J. Dj. Golić, A. Clark, and E. Dawson, " Inversion attack and branching," selected among three best papers from ACISP '99, *Australian Computer Journal*, vol. 31(2), pp. 44-53, May 1999.

9. J. Dj. Golić and R. Menicocci, "Edit probability correlation attack on the alternating step generator," Sequences and their Applications - SETA '98, *Discrete Mathematics and Theoretical Computer Science*, C. Ding, T. Helleseth, and H. Niederreiter eds., Springer-Verlag, pp. 213-227, 1999.

10. L. Simpson, J. Dj. Golić, M. Salmasizadeh, and E. Dawson, "A fast correlation attack on multiplexer generators," *Information Processing Letters*, vol. 70, pp. 89-93, 1999.

11. R. Menicocci and J. Dj. Golić, "Correlation attacks on up/down and stop/go cascades," *IEEE Trans. Inform. Theory*, vol. IT-45, pp. 486-498, Mar. 1999.

12. J. Dj. Golić, A. Clark, and E. Dawson, " Inversion attack and branching," Information Security and Privacy - Wollongong '99, *Lecture Notes in Computer Science*, vol. 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry eds., Springer-Verlag, pp. 88-102, 1999.

13. J. Dj. Golić, "Stream cipher encryption of random access files," *Information Processing Letters*, vol. 69, pp. 145-148, 1999.

14. J. Dj. Golić, "Comment on 'Relations between error probability and entropy'," *IEEE Trans. Inform. Theory*, vol. IT-45, p. 372, Jan. 1999.

15. J. Dj. Golić, "Periods of interleaved and nonuniformly decimated sequences," *IEEE Trans. Inform. Theory*, vol. IT-44, pp. 1257-1260, July 1998.

16. J. Dj. Golić and R. Menicocci, " Correlation attacks on up/down cascades," Information Security and Privacy - Brisbane '98, *Lecture Notes in Computer Science*, vol. 1438, C. Boyd and E. Dawson, eds., Springer-Verlag, pp. 123-134, 1998.

17. L. Simpson, J. Dj. Golić, and E. Dawson, " A probabilistic correlation attack on the shrinking generator," Information Security and Privacy - Brisbane '98, *Lecture Notes in Computer Science*, vol. 1438, C. Boyd and E. Dawson, eds., Springer-Verlag, pp. 147-158, 1998.

18. J. Dj. Golić, "On matroid characterization of ideal secret sharing schemes," *Journal of Cryptology*, vol. 11(2), pp. 75-86, 1998.

19. J. Dj. Golić, " Random correlation matrices," *Australasian Journal of Combinatorics*, vol. 17, pp. 147-156, Mar. 1998.

20. J. Dj. Golić, M. Salmasizadeh, L. Simpson, and E. Dawson, "Fast correlation attacks on nonlinear filter generators," *Information Processing Letters*, vol. 64, pp. 37-42, 1997.

21. H. Gustafson, E. Dawson, and J. Dj. Golić, "Automated statistical methods for measuring the strength of block ciphers," *Statistics and Computing*, vol. 7, pp. 125-135, 1997.

22. J. Dj. Golić and R. Menicocci, "Edit distance correlation attack on the alternating step generator," Advances in Cryptology - CRYPTO '97, *Lecture Notes in Computer Science*, vol. 1294, B. Kaliski ed., Springer-Verlag, pp. 499-512, 1997.

23. M. Salmasizadeh, L. Simpson, J. Dj. Golić, and E. Dawson, " Fast correlation attacks and multiple linear approximations," Information Security and Privacy - Nepean '97, *Lecture Notes in Computer Science*, vol. 1270, V. Varadharadjan, J. Pieprzyk, and Yi Mu eds., Springer-Verlag, pp. 228-239, 1997.

24. J. Dj. Golić, "Linear statistical weakness of alleged RC4 keystream generator," Advances in Cryptology - EUROCRYPT '97, *Lecture Notes in Computer Science*, vol. 1233, W. Fumy ed., Springer-Verlag, pp. 226-238, 1997.

25. J. Dj. Golić, "Cryptanalysis of alleged A5 stream cipher," Advances in Cryptology - EUROCRYPT '97, *Lecture Notes in Computer Science*, vol. 1233, W. Fumy ed., Springer-Verlag, pp. 239-255, 1997.

26. J. Dj. Golić, "Edit distance correlation attacks on clock-controlled combiners with memory," Information Security and Privacy - Wollongong '96, *Lecture Notes in Computer Science*, vol. 1172, J. Pieprzyk and J. Seberry eds., Springer-Verlag, pp. 169-181, 1996.

27. J. Dj. Golić, "On period of multiplexed sequences," Information Security and Privacy - Wollongong '96, *Lecture Notes in Computer Science*, vol. 1172, J. Pieprzyk and J. Seberry eds., Springer-Verlag, pp. 158-168, 1996.

28. J. Dj. Golić, "Conditional correlation attack on combiners with memory," *Electronics Letters*, vol. 32(24), pp. 2193-2195, Nov. 1996.

29. J. Dj. Golić, "Computation of low-weight parity-check polynomials," *Electronics Letters*, vol. 32(21), pp. 1981-1982, Oct. 1996.

30. J. Dj. Golić, "Constrained embedding probability for two binary strings," *SIAM Journal on Discrete Mathematics*, vol. 9(3), pp. 360-364, 1996.

31. J. Dj. Golić and S. Petrović, "Correlation attacks on clock-controlled shift registers in keystream generators," *IEEE Trans. Comput.*, vol. C-45, pp. 482-486, Apr. 1996.

32. J. Dj. Golić, "Fast low order approximation of cryptographic functions," Advances in Cryptology - EUROCRYPT '96, *Lecture Notes in Computer Science*, vol. 1070, U. Maurer ed., Springer-Verlag, pp. 268-282, 1996.

33. J. Dj. Golić, "Correlation properties of a general binary combiner with memory," *Journal of Cryptology*, vol. 9(2), pp. 111-126, 1996.

34. J. Dj. Golić, "Linear models for keystream generators," *IEEE Trans. Comput.*, vol. C-45, pp. 41-49, Jan. 1996.

35. J. Dj. Golić, "On the security of nonlinear filter generators," Fast Software Encryption - Cambridge '96, *Lecture Notes in Computer Science*, vol. 1039, D. Gollmann ed., Springer-Verlag, pp. 173-188, 1996.

36. A. Clark, J. Dj. Golić, and E. Dawson, "A comparison of fast correlation attacks," Fast Software Encryption - Cambridge '96, *Lecture Notes in Computer Science*, vol. 1039, D. Gollmann ed., Springer-Verlag, pp. 145-157, 1996.

37. J. Dj. Golić, "A note on nonuniform decimation of periodic sequences," Cryptography: Policy and Algorithms - Brisbane '95, *Lecture Notes in Computer Science*, vol. 1029, E. Dawson and J. Golić eds., Springer-Verlag, pp. 125-131, 1996.

38. J. Dj. Golić and L. O'Connor, "A cryptanalysis of clock-controlled shift registers with multiple steps," Cryptography: Policy and Algorithms - Brisbane '95, *Lecture Notes in Computer Science*, vol. 1029, E. Dawson and J. Golić eds., Springer-Verlag, pp. 174-185, 1996.

39. J. Dj. Golić, M. Salmasizadeh, A. Clark, A. Khodkar, and E. Dawson, "Discrete optimisation and fast correlation attacks," Cryptography: Policy and Algorithms - Brisbane '95, *Lecture Notes in Computer Science*, vol. 1029, E. Dawson and J. Golić eds., Springer-Verlag, pp. 186-200, 1996.

40. H. Gustafson, E. Dawson, and J. Dj. Golić, "Randomness measures related to subset occurrence," Cryptography: Policy and Algorithms - Brisbane '95, *Lecture Notes in Computer Science*, vol. 1029, E. Dawson and J. Golić eds., Springer-Verlag, pp. 132-143, 1996.

41. J. Dj. Golić, "On decimation of linear recurring sequences," *The Fibonacci Quarterly*, vol. 33, pp. 407-411, Nov. 1995.

42. J. Dj. Golić and S. Petrović, "Constrained many-to-one string editing with memory," *Information Sciences*, vol. 86, pp. 61-76, Sept. 1995.

43. J. Dj. Golić, "Towards fast correlation attacks on irregularly clocked shift registers," Advances in Cryptology - EUROCRYPT '95, *Lecture Notes in Computer Science*, vol. 921, L. C. Guillou and J.-J. Quisquater eds., Springer-Verlag, pp. 248-262, 1995.

44. J. Dj. Golić and L. O'Connor, "Embedding and probabilistic correlation attacks on clock-controlled shift registers," Advances in Cryptology - EUROCRYPT '94, *Lecture Notes in Computer Science*, vol. 950, A. De Santis ed., Springer-Verlag, pp. 230-243, 1995.

45. J. Dj. Golić, "Linear cryptanalysis of stream ciphers," Fast Software Encryption - Leuven '94, *Lecture Notes in Computer Science*, vol. 1008, B. Preneel ed., Springer-Verlag, pp. 154-169, 1995.

46. J. Dj. Golić, "Intrinsic statistical weakness of keystream generators," Advances in Cryptology - ASIACRYPT '94, *Lecture Notes in Computer Science*, vol. 917, J. Pieprzyk and R. Safavi-Naini eds., Springer-Verlag, pp. 91-103, 1995.

47. L. O'Connor and J. Dj. Golić, " A unified Markov approach to differential and linear cryptanalysis," Advances in Cryptology - ASIACRYPT '94, *Lecture Notes in Computer Science*, vol. 917, J. Pieprzyk and R. Safavi-Naini eds., Springer-Verlag, pp. 387-397, 1995.

48. J. Dj. Golić, "On the security of shift register based keystream generators," Fast Software Encryption - Cambridge '93, *Lecture Notes in Computer Science*, vol. 809, R. Anderson ed., Springer-Verlag, pp. 90-100, 1994.

49. S. Petrović and J. Dj. Golić, "String editing under a combination of constraints," *Information Sciences*, vol. 74, pp. 151-163, Oct. 1993.

50. J. Dj. Golić, "Correlation via linear sequential circuit approximation of combiners with memory," Advances in Cryptology - EUROCRYPT '92, *Lecture Notes in Computer Science*, vol. 658, R. A. Rueppel ed., Springer-Verlag, pp. 113-123, 1993.

51. M. Mihaljević and J. Dj. Golić, "Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequence," Advances in Cryptology - EUROCRYPT '92, *Lecture Notes in Computer Science*, vol. 658, R. A. Rueppel ed., Springer-Verlag, pp. 124-137, 1993.

52. J. Dj. Golić and S. Petrović, "A generalized correlation attack with a probabilistic constrained edit distance," Advances in Cryptology - EUROCRYPT '92, *Lecture Notes in Computer Science*, vol. 658, R. A. Rueppel ed., Springer-Verlag, pp. 472-476, 1993.

53. J. Dj. Golić and M. Mihaljević, "A generalized correlation attack on a class of stream ciphers based on the Levenshtein distance," *Journal of Cryptology*, vol. 3(3), pp. 201-212, 1991.

54. J. Dj. Golić, "The number of output sequences of a binary sequence generator," Advances in Cryptology - EUROCRYPT '91, *Lecture Notes in Computer Science*, vol. 547, D. V. Davies ed., Springer-Verlag, pp. 160-167, 1991.

55. M. Mihaljević and J. Dj. Golić, "A comparison of cryptanalytic principles based on iterative error-correction," Advances in Cryptology - EUROCRYPT '91, *Lecture Notes in Computer Science*, vol. 547, D. V. Davies ed., Springer-Verlag, pp. 527-531, 1991.

56. J. Dj. Golić and M. Mihaljević, "A noisy clock-controlled shift register cryptanalysis concept based on sequence comparison approach," Advances in Cryptology - EUROCRYPT '90, *Lecture Notes in Computer Science*, vol. 473, I. B. Damgard ed., Springer-Verlag, pp. 487-491, 1991.

57. M. Mihaljević and J. Dj. Golić, "A fast iterative algorithm for a shift register initial state reconstruction given the noisy output sequence," Advances in Cryptology - AUSCRYPT '90, *Lecture Notes in Computer Science*, vol. 453, J. Seberry and J. Pieprzyk eds., Springer-Verlag, pp. 165-175, 1990.

58. J. Dj. Golić and M. Mihaljević, "Minimal linear equivalent analysis of a variable-memory binary sequence generator," *IEEE Trans. Inform. Theory*, vol. IT-36, pp. 190-192, Jan. 1990.

59. J. Dj. Golić, "On the linear complexity of functions of periodic GF(q) sequences," *IEEE Trans. Inform. Theory*, vol. IT-35, pp. 69-75, Jan. 1989.

60. J. Dj. Golić and M. Živković, "On the linear complexity of nonuniformly decimated PN-sequences," *IEEE Trans. Inform. Theory*, vol. IT-34, pp. 1077-1079, Sept. 1988.

61. J. Dj. Golić and M. Obradović, "A lower bound on the redundancy of D-ary Huffman codes," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 910-911, Nov. 1987. See also "Correction to 'A lower bound on the redundancy of D-ary Huffman codes'," *IEEE Trans. Inform. Theory*, vol. IT-36, pp. 443, Mar. 1990.

62. J. Dj. Golić, "On the relationship between the separability measures and the Bayes probability of error," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 694-701, Sept. 1987.

63. J. Dj. Golić, "On the relationship between the information measures and the Bayes probability of error," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 681-693, Sept. 1987.

64. J. Dj. Golić, "On the relationship between the efficiency measures of multicategory information systems," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 531-538, July 1987.

Papers in Refereed Yugoslav Journals

1. J. Dj. Golić, "Recent advances in stream cipher cryptanalysis," *Publications de l'Institut Mathematique*, vol. 64/78, pp. 183-204, 1998.

2. J. Dj. Golić, "Period of certain pseudorandom sequences," *Univ. Beograd Publ. Elektrotehn. Fak. Ser. Mat.*, vol. 9, pp. 61-70, 1998.

Papers in International/National Conference Proceedings

1. J. Dj. Golić, "Some combinatorial aspects of stream cipher analysis," invited talk, *Abstracts of 23. Australasian Conference on Combinatorial Mathematics and Combinatorial Computing*, Brisbane, Australia, p. 27, 1998.

2. L. Simpson, E. Dawson, J. Dj. Golić, and M. Salmasizadeh, "Fast correlation attacks on the multiplexer generator," *Abstracts of 1998 IEEE International Symposium on Information Theory*, MIT, Cambridge, USA, p. 270, 1998.

3. J. Dj. Golić, "Universal stream ciphers," *Cryptography, Dagstuhl-Seminar-Report*, vol. 190, by invitation, Dagstuhl, Germany, p. 5, 1997.

4. M. Salmasizadeh, J. Dj. Golić, E. Dawson, and L. Simpson, "A systematic procedure for applying fast correlation attacks to combiners with memory," *Proceedings of Workshop on Selected Areas of Cryptography SAC '97*, Ottawa, Canada, pp. 102-115, 1997.

5. J. Dj. Golić, M. Salmasizadeh, E. Dawson, and A. Khodkar, "Cryptanalysis of the summation generator with three input LFSRs," *Proceedings of 1996 IEEE International Symposium on Information Theory and Its Applications*, Victoria, B.C., Canada, pp. 802-805, 1996.

6. M. Mihaljević and J. Dj. Golić, " A method for convergence analysis of iterative error-correction decoding," *Proceedings of 1996 IEEE International Symposium on Information Theory and Its Applications*, Victoria, B.C., Canada, pp. 343-346, 1996.

7. J. Dj. Golić and L. O'Connor, "A combinatorial pattern matching problem with applications to cryptography," *Proceedings of the 19. Australasian Computer Science Conference*, Melbourne, Australia, pp. 473-478, 1996.

8. J. Dj. Golić, "Noiseless coding for multiple channels," *Proceedings of 1994 International Symposium on Information Theory and Its Applications*, Sydney, Australia, pp. 787-792, 1994.

9. J. Dj. Golić, "On parallel generation of linear recurring sequences," *Proceedings of 1994 International Symposium on Information Theory and Its Applications*, Sydney, Australia, pp. 1023-1026, 1994.

10. J. Dj. Golić, M. Salmasizadeh, and E. Dawson, "Autocorrelation weakness of multiplexed sequences," *Proceedings of 1994 International Symposium on Information Theory and Its Applications*, Sydney, Australia, pp. 983-987, 1994.

11. J. Dj. Golić, "On the period of interleaved and decimated sequences," *Abstracts of the 2. International Conference on Finite Fields: Theory, Applications, and Algorithms*, Las Vegas, USA, p. 18, 1993.

12. M. Mihaljević and J. Dj. Golić, "A parity-check weight distribution for maximum-length sequences," *Abstracts of the 2. International Conference on Finite Fields: Theory, Applications, and Algorithms*, Las Vegas, USA, p. 35, 1993.

13. J. Dj. Golić and S. Petrović, "Constrained edit distance for a memoryless function of strings," invited introductory paper, *Proceedings of the 2. Spanish Conference on Cryptology*, Madrid, Spain, pp. 1-23, 1992.

14. J. Dj. Golić and M. Mihaljević, "On a binary sequence generator," *Extended abstracts of EUROCRYPT '89*, Houthalen, Belgium, pp. 59.1-59.6, 1989.

15. J. Dj. Golić, "Chernoff measures, information measures, and probability of error," *Proceedings of the 22. Conference on Information Sciences and Systems*, Princeton, USA, pp. 368-371, 1988.

16. J. Dj. Golić, "On two-channel source coding," *Proceedings of the 22. Conference on Information Sciences and Systems*, Princeton, USA, pp. 386-388, 1988.

17. J. Dj. Golić, "Uncertainty and similarity measures in pattern recognition," *Proceedings of the 26. Allerton Conference on Communication, Control, and Computing*, vol. II, Urbana-Champaign, USA, pp. 639-646, 1988.

Papers in Yugoslav Conference Proceedings

1. J. Dj. Golić, "Universal use of stream ciphers," *Proceedings of the 5. Yugoslav Symposium TELFOR*, Beograd, Yugoslavia, pp. 247-252, 1997.

2. V. Delić, V. Milošević, and J. Dj. Golić, "Band scrambling based on the filter bank theory," *Proceedings of the 38. Yugoslav Conference ETRAN*, Niš, Yugoslavia, pp. II.113-II.114, 1994.

3. V. Delić, V. Milošević, and J. Dj. Golić, "Realization of conventional speech scramblers by sample block transformations," *Proceedings of the 1. Yugoslav Symposium TELFOR*, Beograd, Yugoslavia, pp. 509-514, 1993.

4. J. Dj. Golić, "A lower bound on the capacity of a class of channels with deletion synchronization errors," *Proceedings of the 37. Yugoslav Conference ETAN*, Beograd, Yugoslavia, pp. IV.3-IV.8, 1993.

5. S. Petrović and J. Dj. Golić, "Probabilistic edit-distance for a memoryless function of discrete sequences," *Proceedings of the 37. Yugoslav Conference ETAN*, Beograd, Yugoslavia, pp. XIII.15-XIII.20, 1993.

6. S. Petrović and J. Dj. Golić, "Probabilistic edit-distance for a function of discrete sequences with memory," *Proceedings of the 20. Yugoslav Conference SYM-OP-IS*, Beograd, Yugoslavia, pp. 463-466, 1993.

7. J. Dj. Golić, "A lower bound on the capacity of a binary channel with synchronization errors," *Proceedings of the 36. Yugoslav Conference ETAN*, Kopaonik, Yugoslavia, pp. V.167-V.174, 1992.

8. S. Petrović and J. Dj. Golić, "A new probabilistic constrained edit-distance measure between discrete sequences," *Proceedings of the 36. Yugoslav Conference ETAN*, Kopaonik, Yugoslavia, pp. V.161-V.166, 1992.

9. M. Mihaljević and J. Dj. Golić, "On the residual error-rate of the algorithm for iterative error-correction in a class of binary sequences," *Proceedings of the 36. Yugoslav Conference ETAN*, Kopaonik, Yugoslavia, pp. III.–IV.265-III.–IV. 272, 1992.

10. J. Dj. Golić, "Fuzzy neural networks," *Proceedings of the 35. Yugoslav Conference ETAN*, Ohrid, Yugoslavia, pp. III.231-III.238, 1991.

11. M. Mihaljević and J. Dj. Golić, "A convergence analysis of an algorithm for the iterative error-correction in a class of binary sequences," *Proceedings of the 35. Yugoslav Conference ETAN*, Ohrid, Yugoslavia, pp. III.337-III.344, 1991.

12. S. Petrović and J. Dj. Golić, "Probabilistic edit-distance determination for statistically dependent edit-operations," *Proceedings of the 18. Yugoslav Conference SYM-OP-IS*, Herceg Novi, Yugoslavia, pp. 246-248, 1991.

13. J. Dj. Golić, "A binary sequence generator with variable permutation," *Proceedings of the 33. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 40-43, 1991.

14. J. Dj. Golić, "Period of a binary sequence generator with variable permutation," *Proceedings of the 33. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 44-47, 1991.

15. M. Mihaljević and J. Dj. Golić, "Analysis of a decoding approach based on iterative error-correction," *Proceedings of the 33. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 25-28, 1991.

16. M. Mihaljević and J. Dj. Golić, "A comparison of decoding algorithms based on iterative error-correction," *Proceedings of the 15. Yugoslav Conference on Information Technologies*, Sarajevo-Jahorina, Yugoslavia, pp. 250–1-250–8, 1991.

17. J. Dj. Golić and M. Mihaljević, "A dynamic programming algorithm for block codes decoding for specific communication channels," *Proceedings of the 17. Yugoslav Conference SYM-OP-IS*, Dubrovnik-Kupari, Yugoslavia, pp. 231-233, 1990.

18. S. Petrović and J. Dj. Golić, "An algorithm for the determination of a distance measure between discrete sequences," *Proceedings of the 17. Yugoslav Conference SYM-OP-IS*, Dubrovnik-Kupari, Yugoslavia, pp. 239-242, 1990.

19. J. Dj. Golić, "A number of output sequences of a variable-memory nonlinear generator," *Proceedings of the 24. Yugoslav Conference YUTEL*, Ljubljana, Yugoslavia, pp. SP/5–1-SP/5–4, 1990.

20. J. Dj. Golić, "A number of output sequences of a nonlinear generator with a multiplexer," *Proceedings of the 32. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 515-518, 1990.

21. J. Dj. Golić, "Linear complexity of uniformly decimated periodic finite field sequences," *Proceedings of the 32. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 519-522, 1990.

22. J. Dj. Golić, "Period of a variable-memory binary sequence generator," *Proceedings of the 32. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 523-526, 1990.

23. J. Dj. Golić, "On estimation of misclassification probability in pattern recognition," *Proceedings of the 34. Yugoslav Conference ETAN*, Zagreb, Yugoslavia, pp. IX.191-IX.198, 1990.

24. V. Nedeljković and J. Dj. Golić, "BPSA 2 - A new multilayer neural networks training algorithm," *Proceedings of the 34. Yugoslav Conference ETAN*, Zagreb, Yugoslavia, pp. IX.175-IX.182, 1990.

25. J. Dj. Golić, "Neural network training algorithms based on the nearest neighbour classification rules," *Proceedings of the 14. Yugoslav Conference on Information Technologies*, Sarajevo-Jahorina, Yugoslavia, pp. 154–1-154–8, 1990.

26. J. Dj. Golić and V. Nedeljković, "Neural networks training procedures for pattern recognition in the nonseparable case," *Proceedings of the Yugoslav Conference: Implementations and Applications of Artificial Intelligence*, Dubrovnik, Yugoslavia, pp. 161-169, 1989.

27. V. Nedeljković and J. Dj. Golić, "Simulated annealing for the RHW neural networks," *Proceedings of the Yugoslav Conference: Implementations and Applications of Artificial Intelligence*, Dubrovnik, Yugoslavia, pp. 145-154, 1989.

28. V. Nedeljković and J. Dj. Golić, "Simulated annealing training algorithms for the RHW neural networks," *Proceedings of the Yugoslav Conference: Implementations and Applications of Artificial Intelligence*, Dubrovnik, Yugoslavia, pp. 155-160, 1989.

29. J. Dj. Golić and Lj. Buturović, "Complexity and accuracy of neural network decoding," *Proceedings of the 16. Yugoslav Conference SYM-OP-IS*, Dubrovnik-Kupari, Yugoslavia, pp. 95-98, 1989.

30. J. Dj. Golić and M. Mihaljević, "Some new approaches to neural network decoding," *Proceedings of the 16. Yugoslav Conference SYM-OP-IS*, Dubrovnik-Kupari, Yugoslavia, pp. 99-102, 1989.

31. M. Mihaljević and J. Dj. Golić, "Analysis of a decoding procedure based on preclassification and neural networks," *Proceedings of the 16. Yugoslav Conference SYM-OP-IS*, Dubrovnik-Kupari, Yugoslavia, pp. 115-118, 1989.

32. V. Nedeljković, J. Dj. Golić, and M. Milosavljević, "Neural networks training by stochastic optimization algorithms," *Proceedings of the 16. Yugoslav Conference SYM-OP-IS*, Dubrovnik-Kupari, Yugoslavia, pp. 121-124, 1989.

33. J. Dj. Golić and M. Mihaljević, "Correlation characteristics of a binary sequence generator for spread-spectrum applications," *Proceedings of the 23. Yugoslav Conference YUTEL*, Ljubljana, Yugoslavia, pp. D/7–1-D/7–3, 1989.

34. J. Dj. Golić, "On the period of interleaved binary sequences," *Proceedings of the 31. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 592-595, 1989.

35. J. Dj. Golić, "On the period of nonuniformly decimated binary sequences," *Proceedings of the 31. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 518-521, 1989.

36. M. Mihaljević and J. Dj. Golić, "On a characteristic of the McEliece's public-key system," *Proceedings of the 31. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 522-525, 1989.

37. J. Dj. Golić and Lj. Buturović, "Neural networks in decoding," *Proceedings of the 33. Yugoslav Conference ETAN*, Novi Sad, Yugoslavia, pp. III.189-III.194, 1989.

38. M. Mihaljević and J. Dj. Golić, "Decoding of a general binary block code based on preclassification and neural networks," *Proceedings of the 33. Yugoslav Conference ETAN*, Novi Sad, Yugoslavia, pp. IV.229-IV.236, 1989.

39. M. Mihaljević and J. Dj. Golić, "A neural network approach to text error correction," *Proceedings of the 5. Yugoslav Conference on Applied Linguistics*, Ljubljana, Yugoslavia, pp. 90-96, 1989.

40. J. Dj. Golić, "Uncertainty measures and probability of error in pattern recognition," *Proceedings of the 13. Yugoslav Conference on Information Technologies*, Sarajevo-Jahorina, Yugoslavia, pp. 294–1-294–8, 1989.

41. J. Dj. Golić and M. Obradović, "On the redundancy of D-ary Huffman codes," *Proceedings of the 21. Yugoslav Conference YUTEL*, Ljubljana, Yugoslavia, pp. D/12–1-D/12–3, 1987.

42. J. Dj. Golić and M. Živković, "On the linear complexity probability distribution of nonuniformly clocked linear feedback shift registers," *Proceedings of the 29. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 462-465, 1987.

43. J. Dj. Golić, "Minimal linear equivalent analysis of the product of periodic sequences with irreducible generating polynomials," *Proceedings of the 29. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 458-461, 1987.

44. J. Dj. Golić, "Minimal linear equivalent analysis of switching functions of periodic binary sequences," *Proceedings of the 29. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 450-453, 1987.

45. J. Dj. Golić, "The relationship between the information measures and the Bayes probability of error," *Proceedings of the 29. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 446-449, 1987.

46. M. Mihaljević and J. Dj. Golić, "A symmetry characteristic of the generalized discrete prolate spheroidal sequences transform," *Proceedings of the 29. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 295-298, 1987.

47. J. Dj. Golić and M. Mihaljević, "Minimal linear equivalence analysis of a binary sequence generator," *Proceedings of the 31. Yugoslav Conference ETAN*, Bled, Yugoslavia, pp. IV.405-IV.412, 1987.

48. J. Dj. Golić, "The relationship between the concave efficiency measures of multicategory information systems and the Bayes probability of error," *Proceedings of the 11. Yugoslav Conference on Information Technologies*, Sarajevo-Jahorina, Yugoslavia, pp. 205–1-205–8, 1987.

49. M. Mihaljević and J. Dj. Golić, "Equivocation of an illegitimate user in a class of private digital communication systems," *Proceedings of the 20. Yugoslav Conference YUTEL*, Ljubljana, Yugoslavia, pp. C/8–1-C/8–4, 1986.

50. M. Milosavljević and J. Dj. Golić, "An algorithm for isolated words edge detection based on the posterior detection of abrupt signal changes," *Proceedings of the 28. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 353-356, 1986.

51. J. Dj. Golić and M. Mihaljević, "Minimal linear equivalent analysis of a sum of periodic sequences," *Proceedings of the 28. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 442-444, 1986.

52. J. Dj. Golić and M. Milosavljević, "Minimal linear equivalent a product of periodic sequences," *Proceedings of the 28. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 445-448, 1986.

53. J. Dj. Golić, "Some sufficient conditions for the convex relationship between the efficiency measures of multicategory information systems," *Proceedings of the 30. Yugoslav Conference ETAN*, Herceg Novi, Yugoslavia, pp. IV.81-IV.86, 1986.

54. J. Dj. Golić, "On the convex relationship between the efficiency measures of multicategory information systems," *Proceedings of the 10. Yugoslav Conference on Information Technologies*, Sarajevo-Jahorina, Yugoslavia, pp. 263–1-263–7, 1986.

55. J. Dj. Golić, "A similarity measure between the monotonicly related efficiency measures of multicategory information systems," *Proceedings of the 3. Yugoslav Conference ROJP*, Bled, Yugoslavia, pp. 139-144, 1985.

56. M. Mihaljević and J. Dj. Golić, "An application of discrete prolate spheroidal sequences to subphoneme speech recognition," *Proceedings of the 3. Yugoslav Conference ROJP*, Bled, Yugoslavia, pp. 521-530, 1985.

57. J. Dj. Golić and M. Mihaljević, "Minimal linear equivalent analysis of a special class of binary finite state machines," *Proceedings of the 27. Yugoslav Conference ETAN in MARINE*, Zadar, Yugoslavia, pp. 561-565, 1985.

58. J. Dj. Golić, "A similarity measure between the efficiency measures of multicategory information systems," *Proceedings of the 29. Yugoslav Conference ETAN*, Niš, Yugoslavia, pp. VIII.67-VIII.74, 1985.

59. J. Dj. Golić, "A contribution to gradient image edge detection procedures," *Proceedings of the 24. Yugoslav Conference ETAN*, Priština, Yugoslavia, 1980.

Books

1. E. Dawson and J. Golić eds., *Cryptography: Policy and Algorithms. Lecture Notes in Computer Science.* Berlin: Springer-Verlag, 1996.

2. M. Obradović, D. Lazić, J. Golić, M. Milosavljević, and V. Šenk, *Error-Correction Codes and Statistical Pattern Recognition.* Beograd: VINC, 1989 (in Serbian).

Theses

1. J. Dj. Golić, "On the relationship between the efficiency measures of multicategory information systems," Ph.D. dissertation, Faculty of Electrical Engineering, University of Belgrade, Yugoslavia, 1985 (in Serbian).

2. J. Dj. Golić, "Information theory methods in analysis and synthesis of linear recurring sequences," M.Sc. thesis, Faculty of Electrical Engineering, University of Belgrade, Yugoslavia, 1981 (in Serbian).

3. J. Dj. Golić, "Image edge detection and linking," B.E.E. thesis, Faculty of Electrical Engineering, University of Belgrade, Yugoslavia, 1979 (in Serbian).

International/National Conference Presentations

1. J. Dj. Golić and R. Menicocci, "Edit probability correlation attack on the alternating step generator," presented at the poster session of *EUROCRYPT '98*, Espoo, Finland, June 1998.

2. J. Dj. Golić, "Inversion attack on filter generators," presented at the rump session of *EUROCRYPT '97*, Konstanz, Germany, May 1997.

3. H. Gustafson, E. Dawson, J. Dj. Golić, and A. Pettitt, "Methods for testing sub-block patterns," presented at the *The 22. Australasian Conference on Combinatorial Mathematics and Combinatorial Computation*, Sydney, Australia, July 1996.

4. H. Gustafson, E. Dawson, and J. Dj. Golić, "Repetition test for stream ciphers," presented at the rump session of *EUROCRYPT '95*, Saint-Malo, France, May 1995.

5. H. Gustafson, E. Dawson, and J. Dj. Golić, "Testing for dependencies in block ciphers," presented at the rump session of *ASIACRYPT '94*, Wollongong, Australia, Nov. 1994.

6. J. Dj. Golić, "Access structure characterization of ideal secret sharing schemes," presented at the rump session of *EUROCRYPT '94*, Perugia, Italy, May 1994.

7. J. Dj. Golić, "On information-theoretic secrecy criteria for cipher systems," presented at *Monte-Verita Seminar: Future Directions in Cryptography*, Ascona, Switzerland, Oct. 1989.

8. J. Dj. Golić, "On multi-channel source coding," presented at *The 4. Cornell Summer Workshop on Systems, Control, and Communications*, Cornell University, USA, Aug. 1988.