PUBLICATIONS

Jovan Dj. Golić

August 2006

Papers in Refereed International Journals and Book Series


Lecture Notes in Computer Science is both a book series and a journal (ISSN 0302-9743), which is included in the ISI Master Journal List, Institute for Scientific Information, Philadelphia, USA.


38. R. Menicocci and J. Dž. Golić, "Edit probability correlation attack on the bilateral
stop/go generator," Cryptography and Coding - Cirencester '99, Lecture Notes in Com-


40. J. Dž. Golić, "Iterative probabilistic decoding and parity checks with memory," Elec-

41. J. Dž. Golić, A. Clark, and E. Dawson, "Inversion attack and branching," selected
among three best papers from ACISP '99, Australian Computer Journal, vol. 31(2),

42. J. Dž. 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.,


44. R. Menicocci and J. Dž. Golić, "Correlation attacks on up/down and stop/go cas-

45. J. Dž. Golić, A. Clark, and E. Dawson, "Inversion attack and branching," Information
Security and Privacy - Wollongong '99, Lecture Notes in Computer Science, vol. 1587,

46. J. Dž. Golić, "Stream cipher encryption of random access files," Information Process-

47. J. Dž. Golić, "Comment on 'Relations between error probability and entropy'," IEEE


49. J. Dž. Golić and R. Menicocci, "Correlation attacks on up/down cascades," Informa-

50. L. Simpson, J. Dž. Golić, and E. Dawson, "A probabilistic correlation attack on the
shrinking generator," Information Security and Privacy - Brisbane '98, Lecture Notes


Papers in Refereed Yugoslav Journals


Papers in International/National Conference Proceedings


**Papers in Yugoslav Conference Proceedings**


Books


Theses


International/National Conference Presentations


