Povzetek

Proučevali bomo simetrične šifre, natančneje tokovne šifre, ter njihovo varnost. Podali bomo njihovo klasifikacijo. Temu sledijo opisi osnovnih kriptografskih lastnosti toka ključev. Podrobneje sta predstavljena dva generatorja toka ključev, linearni povratni pomični register (LFSR) in urno-kontroliran pomični register (CCSR). Glavni poudarek je na napadu z vložitvami na CCSR in analizi varnosti.

Ključne besede: kriptografija, kriptoanaliza, tokovni tajnopisi, LFSR, CCSR, napad z vložitvami, vložitvena verjetnost.

Abstract

We study symmetric cryptology, in particulary stream ciphers. We clasify stream ciphers, describe basic properties of keystream generators. Detailed descriptions of linear feedback shift register (LFSR) and clock controlled shift register (CCSR) are given. Our focus are constrained embedding attack and cryptoanalysis of CCSR.

Key words: cryptology, cryptanalysis, stream ciphers, LFSR, CCSR, embedding attack, embedding probability.

Math. Subj. Class. (2000): 03D80, 11T06, 11T71, 68P25, 60C05, 11B83, 11B85

Literatura

[1] E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill Book Company, 1968.

[2] T. Beth, F.C. Piper, *The stop-and-go generator*, Advances in cryptology: Proc. EUROCRYPT '84, *Lecture Notes in Computer Science*, **209** (1985), str.88-92.

[3] W. G. Chambers, *Clock-controlled shift registers in binary sequence generators*, IEE Proceedings E., **135** (1988), str.17-24.

[4] W. G. Chambers, D. Gollman, *Lock-in effect in cascades of clock-controlled shift registers*, Advances in Cryptology, EUROCRYPT '87, *Lecture Notes in Computer Science*, **330** (1988), str.331-342.

[5] T. W. Cusick, C. Ding, A. Renvall, *Stream ciphers and number theory*, Elsevier Science B.V., Amsterdam, 1998.

[6] D. W. Davies, *The Siemens and Halske T52e cipher machine*, Cryptologia, **10** (1986), str.289-307.

[7] C. Ding, *The Differential Cryptanalysis and Design of Natural Stream Ciphers*, Fast software encryption, *Lecture Notes in Computer Science*, **809** (1994), str.101-115.

[8] C. Ding, G. Xiao, W. Shan, *The Stability Theory of Stream Ciphers*, Lecture Notes in Computer Science **561**1991

[9] J. Dj. Golić, *Constrained embedding probability for two binary strings*, SIAM Journal on Discrete Mathematics, **9/3** (1996), str.360-364.

[10] J. Dj. Golić, L. O'Connor, *A Cryptanalysis of Clock-Controlled Shift Registers with Multiple Steps*, Cryptography: policy and algorithms (Brisbane, 1995) *Lecture Notes in Computer Science*, **1029** (1996), str.174-185.

[11] J. Dj. Golić, L. O'Connor, *Embedding and probabilistic Correlation Attacks on Clock-controlled Shift Registers*, Advances in Cryptology-EUROCRYPT '94, *Lecture Notes in Computer Science*, **950** (1995), str.230-243.

[12] J. Dj. Golić, M. J. Mihaljević, *A generalized correlation attack on a class of stream ciphers based on the Levensthein distance*, Journal of Cryptology, **3(3)** (1991), str.201-212.

[13] J. Dj. Golić, *On the Linear Complexity of Functions of Periodic GF(q) Sequences*, IEEE Transactions on Information Theory, **35** (1989), str.69-75.

[14] J. Dj. Golić, M. J. Mihaljević, *A fast iterative algorithm for shift register initial state reconstruction given the noisy output sequences*, Advances in Cryptology - AUSCRYPT '90, *Lectur Notes in Computer Science*, **453** (1990), str.165-175.

[15] D. GOLLMAN, W. G. CHAMBERS, *Clock controlled shift register: a review*, IEEE Journal on Selected Areas in Communications, **7(4)** (1989), str.525-533.

[16] D. GOLLMAN, *Linear recursions of cascaded sequences*, Contributions to General Algebra 3, Proceedings of the Vienna Conference June 1984. Verlag Holder-Pichler-Tempsky, Wien 1985

[17] G. R. GRIMMETT, D. R. STIRZAKER, *Probability and Random Processes*, 2.nd ed., Clarendon Press, Oxford, 1992.

[18] C. G. GÜNTHER, *Alternating step generators controlled by de Bruijn sequences*, Proceedings of EUROCRYPT '87, *Lecture Notes in Computer Science*, **309** (1988), str.5-14.

[19] J. E. HOPCROFT, J.D.ULLMAN, *Introduction to automata, theory, languages and computation*, Addison-Wesley Publishnig, 1979.

[20] A. JURIŠIĆ, A. MENEZES, *Eliptic Curves and Cryptography*, Dr. Dobb's Journal, **264** (1997), str.26-36.

[21] R. LIDL, H.NIEDERREITER, *Introduction to finite fields and their applications*, Cambridge University Press, 1986.

[22] J. C. LAGARIAS, *Pseudorandom number generators in cryptography and number theory*, Cryptography and Computational Number Theory; *Proceeding of Symposia in Applied Mathematics*, **42** (1990), str.115-143.

[23] J. L. MASSEY, *Shift-Register Synthesis and BCH Decoding*, IEEE Transactions on Information Theory, **IT-15, No.1** (1969), str.122-127.

[24] A. J. MENEZES, P. C. VAN OORSCHOT, S. A. VANSTONE, *Handbook of Applied Cryptography*, CRC Press LLC, 1997.

[25] F. ROBERTS, *Applied Combinatorics*, Englewood Cliffs, NJ: Prentice Hall, 1984.

[26] W.RUDIN, *Functional Analysis*, McGraw-Hill,1991.

[27] R. A. RUEPPEL, *Analysis and Design of Stream Ciphers*, Heidelberg: Springer-verlag, 1986.

[28] T. SIEGENTHALER, *Decrypting a Class of Stream Ciphers Using Ciphertext Only*, IEEE Transactions on Computers, **c-34** (1985), str.81-85.

[29] D. R. STINSON, *Cryptography: Theory and Practice*, CRC Press, 1995.

[30] D. WELSH, *Codes and Cryptography*, Okford Science Publications, 1988.

[31] M. V. ŽIVKOVIĆ, *An algorithm for the initial state reconstruction of the clock-controlled shift register*, IEEE Transactions on Information Theory, **37/6** (1991), str.1488-1490.

[32] http://csrc.nist.gov/encryption/aes/round2/r2report.pdf