Povzetek

Diplomsko delo obravnava dokaze brez razkritja znanja. Taki dokazi imajo nenavadno lastnost: prepričujejo nas le o veljavnosti trditve in pri tem o njej ne razkrijejo nobenih informacij oziroma znanja. Cilj diplomskega dela je predstaviti postopek konstrukcije sistema z dokazom brez razkritja znanja za poljuben jezik iz razreda *NP*. Ta postopek izvršimo s pomočjo sheme zaobvezanih bitov, pri čemer uporabimo poljuben generator naključnih števil.

Math. Subj. Class. (2000): 68Q05, 68Q15, 94A60.

Ključne besede: računalništvo, kriptografija, dokazi brez razkritja znanja, sistemi z interaktivnim dokazom, časovna zahtevnost algoritmov.

Key words: computer science, cryptography, zero-knowledge proofs, interactive proof systems, complexity classes.

Literatura

[1] O. Goldreich, *Foundations of cryptography*, rokopis, **http://theory.lcs.mit.edu/~oded/frag.html**, 1995.

[2] D. R. Stinson, *Cryptography: theory and practice*, Boca Raton: CRC, 1995.

[3] A. Menezes, *Handbook of applied cryptography*, CRC Press, 1996.

[4] J. van Leeuwen, *Handbook of theoretical computer science Vol. A, Algorithms and complexity,* MIT Press, cop. 1990.

[5] M. Petkovšek, *NP-polni problemi,* diplomsko delo, Ljubljana,1978.

[6] R. Jamnik, *Verjetnostni račun*, DMFA RS, Ljubljana, 1987.

[7] J. Nešetřil, *Mathematics of Ramsey theory*, Berlin [etc.] : Springer, 1990

[8] O. Goldreich, S.Micali, A. Wigderson; *How to prove all NP statements in zero-knowledge and a methodology of Cryptographic Protocol Design*, CRYPTO 86 Proceedings, Springer-Verlag, Berlin Heidelberg, 1986.

[9] A. Fiat, A. Shamir, *How to prove yourself: Practical solutins to identification and signature problem*, CRYPTO 86 Proceedings, Springer-Verlag, Berlin Heidelberg,1986.

[10] D, Chaum, *Demonstrating that a public predicate can be satisfied without revealing any information about how*, CRYPTO 86 Proceedings, Springer-Verlag, Berlin Heidelberg, 1986.

[11] N. Koblitz, *A course in number theory and cryptography*, Springer-Verlag, 1987.

[12] G. Brassard, *Zero-knowledge simulation of Boolean circuits,* CRYPTO 86 Proceedings, Springer-Verlag, 1986.

[13] G. Brassard, *Modern cryptology,* Springer-Verlag, Berlin Heidelberg, 1998.

[14] H. A. Aronsson, Zero-knowledge protocols and small systems, **http://www.tml.hut.fi/Opinnot/Tik-110.501/1995/zeroknowledge.html,** 1995.

[15] A. Jurišić, *Dokazi brez razkritja znanja* (tečaj iz kriptografije), **http://valjhun.fmf.uni-lj.si/~ajurisic,** 1999.

[16] S. Goldwasser, S Micali, C. Rackoff, *The knowledge complexity of interactive proof systems,* SIAM J. on comput., Vol. 18, No.1, 1989, str. 186 – 205.