POVZETEK

V tem delu predstavimo nekatere sodobne načine deljenja ključa skrivne informacije. Ključ želimo skriti tako, da ga razdelimo med več oseb in predpišemo dovoljeno sodelovanje med njimi, s katerim bodo pooblaščene skupine znale zopet sestavili skrivno informacijo. Za deljenje ključa konstruiramo varne in uporabne sheme za deljenje skrivnosti. Sheme so predstavljene z geometričnimi objekti v afinem oziroma projektivnem prostoru nad končnimi obsegi. Pri konstrukcijah izbiramo geometrične objekte, ki jih delimo članom kot zasebne dele informacije. Osredotočimo se na večnivojske in večskupinske sheme. V večnivojskih shemah imajo člani različna pooblastila po nivojih, ki so med seboj lahko odvisni ali pa neodvisni. V večskupinskih shemah pa ima vsaka skupina možnost lastne organizacije. Za lažjo implementacijo podamo zvezo med geometrično realizacijo shem za deljenje skrivnosti in teorijo grafov.

ABSTRACT

In this thesis we introduce several modern ways of sharing a secret information. We want to share this information with a group of people and prescribe admissible sets in which the secret information can be reconstructed. We can achieve that by constructing secret sharing schemes that are safe and practical. We represent our schemes with geometric objects in an afine or a projective space over a finite field. These geometric objects are used as private peace of information, which is given to the participants in the schemes. We analyze and construct mainly multilevel and concurrence schemes (which are a special case of multilevel schemes). In multilevel schemes the participants have different authorities in different levels, while in concurrence schemes every group has its own organization within. For easier implementation we establish connections between geometric realization of the schemes and graph theoretic approach.

Math. Subj. Class (2000): 05B25, 11T71, 14R10, 68R10, 94A60

Ključne besede: deljenje skrivnosti, večnivojske sheme, večskupinske sheme, končne geometrije, končni obsegi, kriptografija, skrivnost, teorija grafov

Keywords: secret sharing schemes, multilevel scheme, concurrence scheme, finite geometry, finite fields, cryptography, secret, graph theory

7. LITERATURA

[1] L.M. Batten, Combinatorics of Finite Geometries, Cambridge University Press, 1997.

[2] M.K. Bennett, Affine and Projective Geometry, New York [etc.]: John Wiley & Sons, cop. 1995

[3] P.J. Cameron, Projective and Polar Spaces, London: University of London, 1992.

[4] D.M. Cvetković, Kombinatorika, klasična i moderna, Beograd: Naučna knjiga, 1984.

[5] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, Oxford: Clarendon Press, 1979.

[6] Tomaž Košir in Bojan Magajna, Transformacije v geometriji, Društvo matematikov, fizikov in astronomov Slovenije, 1997

[7] J.H. Lint in R.M. Wilson, A Course in Combinatorics, Cambridge: Cambridge University Press, 1993.

[8] G. J. Simmons, An introduction to shared secret and/or shared control schemes and their application, v "Contemporary Cryptology, The Science of Information Integrity", G. J. Simmons, ed., IEEE Press, 1992, 441-497.

[9] G. J. Simmons, Geometric shared secret and/or shared control schemes, v "Advances in Cryptology -- CRYPTO '90", A. J. Menezes and S. A. Vanstone, eds., *Lecture Notes in Computer Science* **537** (1991), 216-241.

[10] D. R. Stinson, Criptography: Theory and Practise, CRC Press, 1995.

[11] I. Vidav, Algebra, Mladinska knjiga, 1972.