Povzetek

V diplomskem delu bomo najprej predstavili Shamirjevo stopenjsko shemo ter uvedli potrebno terminologijo. Sledila bo posplošitev dotične sheme, nato pa bomo razvili še splošen matematičen model sheme za deljenje skrivnosti. Sledil bo razdelek o informacijski zmogljivosti, v katerem bomo tehtali, katere sheme so dobre in katere ne ter zakaj, ter razmislili, koliko in kako lahko sheme izboljšamo. Sledili bodo nekateri drugi primeri konstrukcij shem za deljenje skrivnosti, nato pa se bomo posvetili še matroidom ter njihovi povezavi z idealnimi shemami za deljenje skrivnosti. V zadnjem poglavju bomo za vsak primer konstrukcije sheme za deljenje skrivnosti naredili še konkreten zgled.

Abstract

In this paper we are going to introduce the Shamir threshold scheme as well as the needed terminology. Followed by the generalization of the present scheme we will develop a general mathematical model of the secret sharing scheme. We shall continue with the section devoted to the information rate where we will be considering the quality and usefulness of different schemes as well as the options for their improvement. After we present some other examples of secret sharing scheme constructions we will devote a chapter to matroids and their connections to the ideal secret sharing schemes. In the last chapter we will perform a concrete example for every case of secret sharing scheme construction.

Math. Subj. Class. (2000): 94A62

Ključne besede: sheme za deljenje skrivnosti, strukture dostopa, informacijska zmogljivost, entropija, idealne sheme, matroidi.

Keywords: secret sharing schemes, access structures, information rate, entropy, ideal schemes, matroids.

Literatura

[1] J. Benaloh, J. Leichter, *Generalized Secret Sharing and Monotone Functions*, Lecture Notes in Computer Science, Springer-Verlag, Berlin, New York (403), 1990, 27-35.

[2] E. F. Brickell, D. M. Davenport, *On the Classification of Ideal Secret Sharing Schemes*, Journal of Cryptology (4), 1991, 123-134.

[3] R. Jamnik, *Elementi teorije informacije*, DMFA (1987), Ljubljana.

[4] J. Kozak, *Numerična analiza*, DMFA (2008), Ljubljana.

[5] T. Košir, B. Magajna, *Transformacije v geometriji*, DMFA (1997), Ljubljana.

[6] K. M. Martin, *Discrete Structures in the Theory of Secret Sharing*, Ph.D. thesis, University of London, 1991.

[7] M. Mlakar, *Jensenova neenakost* (online), citirano 30. 8. 2011, dostopno na naslovu www2.arnes.si/˜mmlaka10/Clanki/Jensen.pdf.

[8] A. Shamir, *How to Share a Secret*, Commun. of the ACM (22), 1979, 612-613.

[9] D. R. Stinson, *An Explication of Secret Sharing Schemes*, Designs, Codes and Cryptography (2), 1998, 357-390.

[10] D. R. Stinson, *Cryptography: Theory and Practice*, CRC-Press (1995), Boca Raton.

[11] D. J. A. Welsh, *Matroid Theory*, Academic Press (1976), London.