CONGRESO DE JÓVENES INVESTIGADORES
Real Sociedad Matemática Española
Universidad de Murcia, del 7 al 11 de Septiembre de 2015

On the Information Ratio of Non-Perfect Secret Sharing Schemes

Oriol Farràs[1], **Torben Hansen**[2], **Tarik Kaced**[3], **Carles Padró**[4]

A secret sharing scheme is a method to protect a secret value by distributing it into shares among a set of players in order to prevent both the disclosure and the loss of the secret. Secret sharing schemes were independently introduced by Shamir [7] and Blakley [1] in 1979, and soon became a very important primitive in cryptography with many different applications, such as secure multiparty computation and distributed cryptography. These applications require efficient schemes. In particular, shares of a secret value should be small. A common measure of the efficiency of a secret sharing scheme is the information ratio, the ratio between the maximum length of the shares and the length of the secret.

A secret sharing scheme is non-perfect if some subsets of players that cannot recover the secret value have partial information about it. The first non-perfect schemes were introduced by Blakley and Meadows [3], and the main purpose was to improve the efficiency of the schemes by relaxing the security requirements. In a perfect scheme, the information ration is always greater or equal to one, but in a non-perfect scheme it can be smaller.

This work is dedicated to the search of bounds on the information ratio of non-perfect secret sharing schemes and the construction of efficient linear non-perfect secret sharing schemes. To this end, we extend the known connections between matroids, polymatroids and perfect secret sharing schemes [2, 4] to the non-perfect case. Previous results in this line of work were presented in [6, 5].

Referencias

[1] G. R. Blakley: Safeguarding cryptographic keys. *AFIPS Conference Proceedings.*, **48** (1979) 313–317.

[2] E. F. Brickell, D. M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology*, **4** (1991) 123–134.

[3] G. R. Blakley, C. Meadows: Security of Ramp Schemes. *Advances in Cryptology, Crypto'84. Lecture Notes in Comput. Sci.* **196** (1985) 242–268.

[4] L. Csirmaz. The size of a share must be large. *J. Cryptology*, **10** (1997) 223–231.

[5] O. Farràs, T. Hansen, T. Kaced, C. Padró: Optimal Non-Perfect Uniform Secret Sharing Schemes. *Advances in Cryptology, CRYPTO 2014. Lecture Notes in Comput. Sci.* **8617** (2014) 217–234.

[6] O. Farràs, C. Padró: Extending Brickell–Davenport theorem to non-perfect secret sharing schemes. *Des. Codes Cryptogr.*, **74(2)** (2015) 495–510.

[7] A. Shamir: How to share a secret. *Commun. of the ACM*, **22** (1979) pp. 612–613.

[1]Universitat Rovira i Virgili
oriol.farras@urv.cat

[2]Aarhus University
torben.brandt.hansen@post.au.dk

[3]Université de Paris-Est
tarik.kaced@ens-lyon.org

[4]Universitat Politècnica de Catalunya
cpadro@ma4.upc.edu.