Secret sharing schemes – solved and unsolved problems

László Csirmaz, Central European University, Budapest

The talk surveys the present status of secret sharing schemes: How did it emerge, where and how is/can be used in other branches of cryptography. It has computational vs information theoretical approach as well perfect vs ramp schemes. We will focus mainly on the information theoretical perfect case. On the positive side, the existence of perfect secret sharing scheme for every possible access structure is known. The main unsolved problem of the field is the efficiency: all known constructions give exponentially large shares (in the number of participants), while only linear lower bounds are known. Thus search for tight bounds in special cases is the subject of several ongoing research, see [2, 3, 4, 6, 7, 8, 10, 11, 13, 14, 16].

The problems are closely connected to open problems in Information Theory [5, 9, 15], Matroid representation [1, 12]. We enlist recent results, and indicate why solving the general case seems to be extremely difficult.

We shall pay special attention to systems defined on graphs. A folklore theorem says that the information ratio for a graph is either 1, or is at least 3/2. (By [12] this result extends to quite general structures.) Determining which real numbers can occur as information ratio for graphs is unsolved. All known results are covered by the following theorem.

Theorem. a) *For each integer $k \geq 1$ there is a graph with information ratio $2-1/k$.* b) *For each integer $k \geq 2$ there is a graph with information ratio $k/2$.*

Thus the *spectrum* of information ratio of graphs is not discrete: 2 is a limit point. We shall discuss several conjectures concering this spectrum, methods to attack them, and the difficulty to solving them.

Conjecture. a) *There is no limit point below 2.* b) *All values below 2 are of the form $2-1/k$.* c) *Each integer is a limit point.* d) *There is an irrational point in the spectrum.*

References

[1] A. Beimel, N. Livne: On matriods and non-ideal secret sharing, In: Proc. of the third Theory of Cryptography Conference, Lecture Notes in Computer Science, Vol 3876(2006) pp. 482–501

[2] C. Blundo, A. De Santis, D. R. Stinson, U. Vaccaro: Graph Decomposition and Secret Sharing Schemes *Journal of Cryptology*, Vol 8(1995) pp. 39–64.

[3] C. Blundo, A. De Santis, R. D. Simone, U. Vaccaro: Tight Bounds on the Information Rate of Secret Sharing Schemes *Designs, Codes and Cryptography*, Vol 11(1997) pp. 107–110

[4] R. M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro: On the size of shares of secret sharing schemes *Journal of Cryptology*, vol 6(1993), pp. 157–168

[5] B. Chor, E. Kushilevitz: Secret sharing over infinite domains *Journal of Cryptology*, Vol 6(1993) pp. 87–96

[6] L. Csirmaz: The size of a share must be large *Journal of Cryptology*, vol 10(1997) pp. 223–231

[7] L. Csirmaz: Secret sharing on the d-dimensional cube, IACR eprint `http://eprint.iacr.org/2005/177`

[8] L. Csirmaz, G. Tardos: Exact information rate of trees, *manuscript*

[9] I. Csiszár and J. Körner: *Information Theory. Coding Theorems for Discrete Memoryless Systems*, Academic Press, New York, 1981.

[10] M. van Dijk: On the information rate of perfect secret sharing schemes *Designs, Codes and Cryptography*, Vol 12(1997) pp. 143–169

[11] M. van Dijk, T. Kevenaar, G. J. Schrijen, P. Tuyls: Improved constructions of secret sharing schemes by applying (λ,ω)-decompositions Inf. Processing Letters, vol 99(2006) pp. 154–157

[12] O. Ferràs, J. Martì-Farré, C. Padró: Ideal Multipartite Secret Sharing Schemes Preprint (2006) `http://www-ma4.upc.edu/ cpadro/papers/mltprtt.pdd`

[13] W. Jakson, K. M. Martin: Perfect secret sharing schemes on five participants, *Designs, Codes and Cryptography*, Vol 9(1996) pp. 233-250

[14] J. Martì-Farré, C. Padró: Secret sharing schemes with three or four minimal qualified subsets *Designs, Codes and Cryptography*, Vol 34(2005) pp. 17–34

[15] F. Matus: Matroid representations by partitions, *Discrete Mathematics*, vol 203(1999) pp. 169–194

[16] D. R. Stinson: Decomposition construction for secret sharing schemes, *IEEE Trans. Inform. Theory* Vol 40(1994) pp. 118-125.