Ideal Secret Sharing Schemes for Useful Multipartite Access Structures

Oriol Farràs[1] and Carles Padró[2]

[1] Universitat Rovira i Virgili, Tarragona, Catalonia
[2] Nanyang Technological University, Singapore

Abstract. This paper is a survey of the main results and open problems in a line of work that was initiated shortly after secret sharing was introduced. Namely, the construction of ideal linear secret sharing schemes for access structures that are natural generalizations of the threshold ones and have interesting properties for the applications. Some of them have hierarchical properties, while other ones are suitable for situations requiring the agreement of several parties. These access structures are multipartite, that is, the participants are distributed into several parts and all participants in the same part play an equivalent role in the structure. This line of work has received an impulse from a recently discovered connection between ideal multipartite secret sharing schemes and integer polymatroids.

Keywords: Secret sharing, Ideal secret sharing schemes, Multipartite secret sharing, Hierarchical secret sharing, Integer polymatroids.

1 Introduction

Since its introduction in 1979 by Shamir [45] and Blakley [11], many different applications of secret sharing to several areas of Cryptology have appeared. In most applications, only threshold secret sharing schemes, as the ones in those seminal papers, are used. In addition, the homomorphic properties of Shamir's [45] threshold scheme make it suitable to be used in one of the main applications of secret sharing: secure multiparty computation [9,17,19]. Nevertheless, secret sharing for general (non-threshold) access structures has received a lot of attention. Two lines of research can be identified in the works on this topic.

The first one is the optimization of secret sharing schemes for general access structures. Most of the works on this line focus on two open problems. Namely, minimizing the length of the shares in relation to the length of the secret and the characterization of the access structures admitting an *ideal* secret sharing scheme, that is, a scheme in which all shares have the same length as the secret. These appeared to be extremely difficult open problems, with connections to several areas of Mathematics. Among the main results in this line of work we find the relation between ideal secret sharing and matroids discovered by Brickell and Davenport [15] and some subsequent findings about this connection [1,35,37,44,47], the proof that linear secret sharing schemes are not enough

Y.M. Chee et al. (Eds.): IWCC 2011, LNCS 6639, pp. 99–108, 2011.

to minimize the ratio between the length of the shares and the length of the secret [2,6,26], and the use of different combinatorial and information theoretical techniques [13,16,20,32,49] and, in particular, non-Shannon information inequalities [3,4] to find upper and lower bounds on the length of the shares.

The second line of research is more oriented towards the applications of secret sharing. It deals with constructions of ideal secret sharing schemes for *multipartite* access structures, in which the participants are distributed into several parts according to their role. These access structures are among the most natural generalizations of the threshold ones, and they are suitable for situations involving several parties as, for instance, hierarchical organizations. This was initiated by Kothari [34], Simmons [46], and Brickell [14], and it has been continued by several other authors [7,29,41,50,51].

This paper is a survey of the main results on that second line of research, with a special emphasis on the consequences of the recent introduction of integer polymatroids as a tool for the analysis and design of ideal multipartite secret sharing schemes [22].

2 Shamir's Threshold Secret Sharing Scheme

Since complete and detailed descriptions of Shamir's [45] threshold secret sharing scheme can be found in many texts (for instance in [48]), we only summarize here its main properties.

Shamir's scheme works for every (t, n)-*threshold access structure*, in which the qualified subsets are those having at least t out of n participants. The secret value is taken from a finite field with at least $n + 1$ elements. Since each share is taken from the same finite field as the secret, Shamir's scheme is ideal. In addition, it is *linear*, because both the generation of the shares and the secret reconstruction can be performed by computing values of some linear transformations. This implies homomorphic properties for Shamir's secret sharing scheme. Specifically, a linear combination of shares for different secrets result in shares for the corresponding linear combination of the secrets. Moreover, if the ratio between the number n of participants and the threshold t is large enough, Shamir's scheme has also homomorphic properties in relation to the multiplication in the finite field. Because of these multiplicative properties, it can be applied to the construction of secure multiparty computation protocols [9,17,19].

3 First Generalizations of Threshold Secret Sharing

The first secret sharing schemes for non-threshold access structures were introduced already in the seminal paper by Shamir [45], by modifying his threshold scheme to adapt it to situations in which some participants are more powerful than others. Specifically, every participant receives a certain number of shares from a threshold scheme. This scheme has a *weighted threshold access structure*, in which every participant has a weight and the qualified sets are those whose

weight sum attains the threshold. Since some shares are larger than the secret, this secret sharing scheme is not ideal.

Ito, Saito and Nishizeki [31] and Benaloh and Leichter [8] proved that there exists a secret sharing scheme for every access structure. Nevertheless, the size of the shares in those schemes grows exponentially with the number of participants. Actually, it is not possible to find an ideal scheme for every access structure [8], and in some cases the shares must be much larger than the secret [20]. Actually, the optimization of secret sharing schemes for general access structures has appeared to be an extremely difficult problem, and not much is known about it. Anyway, it seems clear that we cannot expect to find an efficient secret sharing scheme for every given access structure.

Nevertheless, this does not imply that efficient and useful secret sharing schemes only exist for threshold access structures. Actually, several constructions of ideal linear secret sharing schemes for access structures with interesting applications have been proposed.

Bloom [12] and Karnin, Greene and Hellman [33] presented alternative descriptions of Shamir's [45] and Blakley's [11] threshold schemes in terms of Linear Algebra. By generalizing the ideas in [12,33], Kothari [34] introduced the first ideal hierarchical secret sharing schemes.

Simmons [46] introduced two families of multipartite access structures, the so-called multilevel and compartmented access structures. The first ones are suitable for hierarchical organizations, while the second ones can be used in situations requiring the agreement of several parties. By generalizing the geometrical threshold scheme by Blakley [11], Simmons constructed ideal secret sharing schemes for some multilevel and compartmented access structures, and he conjectured that this was possible for all of them.

In a *multilevel access structure*, the participants are divided into m hierarchical levels and, for some given integers $0 < t_1 < \cdots < t_m$, a subset is qualified if and only if it has at least t_i participants in the first i levels for some $i = 1, \ldots, m$. A *compartmented access structure* is determined as well by some positive integers t and $t_1, \ldots, t_m$ with $t \geq \sum_{i=1}^{m} t_i$. The participants are divided into m compartments, and a subset is qualified if and only if it has at least t participants and, for every $i = 1, \ldots, m$, at least t_i participants in the i-th compartment.

4 Brickell's Ideal Secret Sharing Schemes

Simmons' [46] conjecture about the existence of ideal secret sharing schemes for the multilevel and the compartmented access structures was proved by Brickell [14]. This was done by introducing a new method, based on linear algebra, to construct ideal secret sharing schemes. This method has appeared to be very powerful and it has been used in most of the subsequent constructions of ideal secret sharing schemes. In addition, it provides a sufficient condition for an access structure to be *ideal*, that is, to admit an ideal scheme. This result was the first step in the discovery by Brickell and Davenport [15] of the connection between ideal secret sharing schemes and matroids.

We present the method by Brickell [14] to construct ideal secret sharing schemes as described by Massey [36] in terms of linear codes. Let C be an $[n+1, k]$-linear code over a finite field $\mathbb{K}$ and let M be a generator matrix of C, that is, a $k \times (n+1)$ matrix over $\mathbb{K}$ whose rows span C. Such a code defines an ideal secret sharing scheme on a set $P = \{p_1, \ldots, p_n\}$ of participants. Specifically, every random choice of a codeword $(s_0, s_1, \ldots, s_n) \in C$ corresponds to a distribution of shares for the secret value $s_0 \in \mathbb{K}$, in which $s_i \in \mathbb{K}$ is the share of the participant p_i. Such an ideal scheme is called a $\mathbb{K}$-*vector space secret sharing scheme* and its access structure is called a $\mathbb{K}$-*vector space access structure*.

It is easy to check that a set $A \subseteq P$ is in the access structure Γ of this scheme if and only if the column of M with index 0 is a linear combination of the columns whose indices correspond to the players in A. Therefore, if $Q = P \cup \{p_0\}$ and $\mathcal{M}$ is the representable matroid with ground set Q and rank function r that is defined by the columns of the matrix M, then

$$\Gamma = \Gamma_{p_0}(\mathcal{M}) = \{A \subseteq P \,:\, r(A \cup \{p_0\}) = r(A)\}.$$

That is, Γ is the *port of the matroid* $\mathcal{M}$ *at the point* p_0. Consequently, a sufficient condition for an access structure to be ideal is obtained. Namely, the ports of representable matroids are ideal access structures. Actually, they coincide with the vector space access structures. As a consequence the results by Brickell and Davenport [15], this sufficient condition is not very far from being necessary. Specifically, they proved that every ideal access structure is a matroid port. The reader is addressed to [35] for more information about matroid ports and their connection to ideal secret sharing.

By considering Reed-Solomon codes, one can check that Shamir's threshold scheme is a particular case of vector space secret sharing scheme. Like Shamir's threshold scheme, vector space secret sharing schemes are linear. Because of that, the algorithms to compute the shares and to recover the secret value are very efficient. In addition, linearity implies homomorphic properties of those schemes that are very useful for certain applications.

Brickell [14] proved that all multilevel and compartmented access structures are ideal. Specifically, he proved that, similarly to threshold access structures, every structure in one of those families admits a vector space secret sharing scheme over every large enough field. Even though the proof is constructive, it is still an open problem to determine how efficiently these schemes can be constructed.

One of the unsolved questions is to find out the minimum size of the fields over which there exist vector space secret sharing schemes for a given multilevel or compartmented access structure. This is an open problem as well for threshold access structures, equivalent to the main conjecture on maximum distance separable codes. Nevertheless, it is known that this minimum size of the field is linear on the number of participants for threshold structures, while the asymptotic behavior of this parameter is unknown for multilevel and compartmented access structures.

The computation time to construct a vector space secret sharing scheme for a multilevel or compartmented access structure is another open question. By

following the construction proposed by Brickell [14], a large number of determinants, which grows exponentially with the number of participants, have to be computed. An alternative method that avoids the necessity of computing this large number of determinants is proposed in the same work, but this construction is inefficient because it requires an extremely large field.

5 Constructing and Characterizing

The general method proposed by Brickell [14] is used in all subsequent constructions of ideal secret sharing schemes for multipartite access structures. Some of these works propose constructions for new families of multipartite access structures, while other papers deal with the aforementioned open problems about the efficiency of the constructions. In addition, the characterization of ideal multipartite access structures has attracted some attention as well. We describe some of these results in the following.

Tassa [50] considered a family of hierarchical access structures that are very similar to the multilevel ones. Specifically, given integers $0 < t_1 < \cdots < t_m$, a subset is qualified if and only if, for every $i = 1, \ldots, m$, it has at least t_i participants in the first i levels. Actually, these access structures are dual to the multilevel ones and, because of that, they admit as well vector space secret sharing schemes. The construction proposed by Tassa can be seen as a variant of Shamir's threshold scheme. As in Shamir's scheme, a random polynomial is used to determine the shares, but some of the shares are the values on some given points of the derivatives of certain orders instead of the values of the polynomial itself. The order of the derivative depends on the hierarchical level of the participant. Therefore, the secret value is reconstructed by using Birkhoff interpolation instead of Lagrange interpolation. Belenkiy [7] showed how to use Birkhoff interpolation to construct schemes for the multilevel access structures.

These constructions have the same efficiency problems as the ones by Brickell [14] for the multilevel and compartmented access structures. Nevertheless, Tassa proposes a probabilistic method that has a high practical interest. Specifically, one can estimate the probability of obtaining a matrix defining a secret sharing scheme with the required access structure when some of the parameters are chosen at random. This probability grows with the size of the field and it can be arbitrarily close to one.

Another construction of ideal multipartite secret sharing schemes is presented in [51]. In this case, polynomials on two variables are used. This construction is applied to the compartmented access structures and a variant of them and also to the family of hierarchical access structures considered in [50]. Constructions for other families of multipartite access structures are given in [29,41].

Other works deal with the characterization of the ideal access structures in some families of multipartite access structures. A complete characterization of the bipartite access structures that admit an ideal secret sharing scheme was presented by Padró and Sáez [42]. In particular, they characterized the ideal weighted threshold access structures with two weights. Other partial results

about the characterization of ideal weighted threshold access structures were given in [39], and this problem was completely solved by Beimel, Tassa, and Weinreb [5]. Partial results about the characterization of the ideal tripartite access structures were given in [18,29].

A common feature of all ideal access structures appearing in the works that have been surveyed in this section is that they admit vector space secret sharing schemes over every large enough field. In addition, the aforementioned open problems about the efficiency of the constructions of ideal schemes for multilevel and compartmented access structures appear as well for all those families.

In particular, determining the minimum size of the fields over which those structures admit a vector space secret sharing scheme has appeared to be extremely difficult. This problem is studied by Beutelspacher and Wettl [10] and by Giuletti and Vincenti [27] for particular cases of multilevel access structures. They present upper and lower bounds on the minimum size of the field for several multilevel access structures with two and three levels.

6 A New Tool: Integer Polymatroids

Integer polymatroids have been applied for the first time in [22] as a mathematical tool to study ideal multipartite secret sharing schemes. Specifically, this combinatorial object is used in that work to present a necessary condition and a sufficient condition for a multipartite access structure to be ideal. These results provide a general framework to analyze the previous constructions and characterizations, and also the existing open problems. We briefly describe them in the following, together with several important consequences that have been derived from them.

In the same way as matroids abstract some properties related to linear dependencies in collections of vectors in a vector space, integer polymatroids abstract similar properties in collections of subspaces of a vector space. Integer polymatroids have been thoroughly studied by researchers in combinatorial optimization, and the main results can be found in the books [25,40,43]. A concise presentation of the basic facts about integer polymatroids was given by Herzog and Hibi [30], who applied this combinatorial object to commutative algebra.

Brickell and Davenport [15] proved that every ideal secret sharing scheme with access structure Γ on a set P of participants defines a matroid $\mathcal{M}$ with ground set $Q = P \cup \{p_0\}$, such that Γ is the port of the matroid $\mathcal{M}$ at the point p_0. If the access structure Γ is m-partite, then the matroid $\mathcal{M}$ is $(m+1)$-partite. This is due to the fact that the symmetry properties of Γ are transported to the matroid $\mathcal{M}$, where one part consisting only of the point p_0 has to be added. Every $(m+1)$-partite matroid defines in a natural way an integer polymatroid on a ground set with $m+1$ elements. This implies the connection between ideal multipartite secret sharing schemes and integer polymatroids that is presented in [22]. In particular, a necessary condition for a multipartite access structure to be ideal is obtained.

In a similar way as some matroids can be represented by families of vectors, some integer polymatroids can be represented by families of vector subspaces.

One of the main results in [22] relates the representability of multipartite matroids and integer polymatroids. Specifically, a multipartite matroid is representable if and only if its associated integer polymatroid is representable. This provides a sufficient condition for a multipartite access structure to admit a vector space secret sharing scheme.

These general results about ideal multipartite access structures are applied in [22] to find a characterization of the ideal tripartite access structures. In addition, those results were used as well to find a characterization of the ideal hierarchical access structures [24]. As a consequence, a new proof for the characterization of the ideal weighted threshold access structures in [5] is obtained. It is proved in [24] that the ideal hierarchical access structures coincide with the hierarchical matroid ports and, moreover, that every hierarchical matroid port admits a vector space secret sharing scheme over every large enough field. The family of the tripartite access structures has the same properties.

As a consequence of the results in [22], if an integer polymatroid is representable over every large enough field, the same applies to the multipartite matroids that are associated to it. Therefore, every family of such integer polymatroids provides a family of multipartite access structures that admit vector space secret sharing schemes over every large enough field.

By analyzing the families of ideal multipartite access structures that have appeared in the literature under the light of the results in [22], we see that all of them are related to families of quite simple integer polymatroids. Of course, they are representable over every large enough field. For instance, the ideal bipartite and tripartite access structures, and also the compartmented ones, are obtained from integer polymatroids satisfying the strong exchange property [21]. On the other hand, all ideal hierarchical access structures are associated to Boolean polymatroids, which are very simple integer polymatroids that can be represented over every field (see [38] for more information). In particular, this applies to the multilevel access structures and to the ideal weighted threshold access structures.

7 Open Problems and Directions for Future Work

Unfortunately, the results in [22] do not solve the open problems related to the efficiency of the constructions of ideal secret sharing schemes for the multipartite access structures in those families. Nevertheless, those problems can be restated now in a clearer way. Specifically, as a consequence of [22, Theorem 6.1 (full version)], one should determine how efficiently a representation of a multipartite matroid can be obtained from a representation of its associated integer polymatroid. The proof of this theorem is constructive, but of course it does not provide the most efficient way to do that and, in addition, the given upper bound on the required size of the field is not tight.

Another direction for future work is to find new families of ideal multipartite access structures with similar properties as the ones analyzed in this paper. Namely, they should admit vector space secret sharing schemes over every large

enough finite field, and they should have additional properties that make them useful for the applications of secret sharing. By analogy to the previous families, it seems that one should analyze other families of simple integer polymatroids as, for instance, boolean polymatroids (only some of them define the ideal hierarchical access structures) or uniform integer polymatroids (see [23] for the definition).

Finally, characterizing the ideal access structures in other families of multipartite access structures is worth considering as well. For instance, one could try to characterize the ideal quadripartite access structures. Differently to the bipartite and tripartite cases, there exist quadripartite matroid ports that are not ideal. Namely, the access structures related to the Vamos Matroid. The results in [28] about the representability of integer polymatroids on four points can be very useful to obtain this characterization.

Acknowledgments and Disclaimer

The first author's work was partly funded by the Spanish Government through project CONSOLIDER INGENIO 2010 CSD2007-00004 "ARES", and by the Government of Catalonia through grant 2009 SGR 1135. The first author is with the UNESCO Chair in Data Privacy, but the views expressed in this paper are his own and do not commit UNESCO. The second author's work was supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

References

1. Beimel, A., Chor, B.: Universally ideal secret-sharing schemes. IEEE Trans. Inform. Theory 40, 786–794 (1994)
2. Beimel, A., Ishai, Y.: On the power of nonlinear secret sharing schemes. SIAM J. Discrete Math. 19, 258–280 (2005)
3. Beimel, A., Livne, N., Padró, C.: Matroids Can Be Far from Ideal Secret Sharing. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 194–212. Springer, Heidelberg (2008)
4. Beimel, A., Orlov, I.: Secret Sharing and Non-Shannon Information Inequalities. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 539–557. Springer, Heidelberg (2009)
5. Beimel, A., Tassa, T., Weinreb, E.: Characterizing Ideal Weighted Threshold Secret Sharing. SIAM J. Discrete Math. 22, 360–397 (2008)
6. Beimel, A., Weinreb, E.: Separating the power of monotone span programs over different fields. SIAM J. Comput. 34, 1196–1215 (2005)
7. Belenkiy, M.: Disjunctive Multi-Level Secret Sharing. Cryptology ePrint Archive, Report 2008/018, `http://eprint.iacr.org/2008/018`
8. Benaloh, J.C., Leichter, J.: Generalized secret sharing and monotone functions. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 27–35. Springer, Heidelberg (1990)

9. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: Proc. ACM STOC 1988, pp. 1–10 (1988)
10. Beutelspacher, A., Wettl, F.: On 2-level secret sharing. Des. Codes Cryptogr. 3, 127–134 (1993)
11. Blakley, G.R.: Safeguarding cryptographic keys. In: AFIPS Conference Proceedings, vol. 48, pp. 313–317 (1979)
12. Bloom, J.R.: Threshold Schemes and Error Correcting Codes. Am. Math. Soc. 2, 230 (1981)
13. Blundo, C., De Santis, A., De Simone, R., Vaccaro, U.: Tight bounds on the information rate of secret sharing schemes. Des. Codes Cryptogr. 11, 107–122 (1997)
14. Brickell, E.F.: Some ideal secret sharing schemes. J. Combin. Math. and Combin. Comput. 9, 105–113 (1989)
15. Brickell, E.F., Davenport, D.M.: On the classification of ideal secret sharing schemes. J. Cryptology 4, 123–134 (1991)
16. Capocelli, R.M., De Santis, A., Gargano, L., Vaccaro, U.: On the size of shares of secret sharing schemes. J. Cryptology 6, 157–168 (1993)
17. Chaum, D., Crépeau, C., Damgård, I.: Multi-party unconditionally secure protocols. In: Proc. ACM STOC 1988, pp. 11–19 (1988)
18. Collins, M.J.: A Note on Ideal Tripartite Access Structures. Cryptology ePrint Archive, Report 2002/193, `http://eprint.iacr.org/2002/193`
19. Cramer, R., Damgård, I.B., Maurer, U.M.: General Secure Multi-party Computation from any Linear Secret-Sharing Scheme. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 316–334. Springer, Heidelberg (2000)
20. Csirmaz, L.: The size of a share must be large. J. Cryptology 10, 223–231 (1997)
21. Farràs, O.: Multipartite Secret Sharing Schemes. PhD Thesis, Universitat Politècnica de Catalunya (2010)
22. Farràs, O., Martí-Farré, J., Padró, C.: Ideal Multipartite Secret Sharing Schemes. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 448–465. Springer, Heidelberg (2007); The full version of this paper is available at the Cryptology ePrint Archive, Report 2006/292, `http://eprint.iacr.org/2006/292`
23. Farràs, O., Metcalf-Burton, J.R., Padró, C., Vázquez, L.: On the Optimization of Bipartite Secret Sharing Schemes. In: Kurosawa, K. (ed.) ICITS 2009. LNCS, vol. 5973, pp. 93–109. Springer, Heidelberg (2010)
24. Farràs, O., Padró, C.: Ideal hierarchical secret sharing schemes. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 219–236. Springer, Heidelberg (2010); The full version of this paper is available at the Cryptology ePrint Archive, Report 2009/141 (2010), `http://eprint.iacr.org/2009/141`
25. Fujishige, S.: Submodular Functions and Optimization. Annals of Discrete Mathematics, vol. 47. North-Holland Elsevier, Amsterdam (1991)
26. Gál, A.: A characterization of span program size and improved lower bounds for monotone span programs. In: Proceedings of 30th ACM Symposium on the Theory of Computing, STOC 1998, pp. 429–437 (1998)
27. Giuletti, M., Vincenti, R.: Three-level secret sharing schemes from the twisted cubic. Discrete Mathematics 310, 3236–3240 (2010)
28. Hammer, D., Romashchenko, A.E., Shen, A., Vereshchagin, N.K.: Inequalities for Shannon Entropy and Kolmogorov Complexity. J. Comput. Syst. Sci. 60, 442–464 (2000)
29. Herranz, J., Sáez, G.: New Results on Multipartite Access Structures. IEEE Proceedings on Information Security 153, 153–162 (2006)

30. Herzog, J., Hibi, T.: Discrete polymatroids. J. Algebraic Combin. 16, 239–268 (2002)
31. Ito, M., Saito, A., Nishizeki, T.: Secret sharing scheme realizing any access structure. In: Proc. IEEE Globecom 1987, pp. 99–102 (1987)
32. Jackson, W.-A., Martin, K.M.: Perfect secret sharing schemes on five participants. Des. Codes Cryptogr. 9, 267–286 (1996)
33. Karnin, E.D., Greene, J.W., Hellman, M.E.: On secret sharing systems. IEEE Trans. Inform. Theory 29, 35–41 (1983)
34. Kothari, S.C.: Generalized Linear Threshold Scheme. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 231–241. Springer, Heidelberg (1985)
35. Martí-Farré, J., Padró, C.: On Secret Sharing Schemes, Matroids and Polymatroids. J. Math. Cryptol. 4, 95–120 (2010)
36. Massey, J.L.: Minimal codewords and secret sharing. In: Proceedings of the 6-th Joint Swedish-Russian Workshop on Information Theory, Molle, Sweden, pp. 269–279 (August 1993)
37. Matúš, F.: Matroid representations by partitions. Discrete Math. 203, 169–194 (1999)
38. Matúš, F.: Excluded minors of Boolean polymatroids. Discrete Math. 253, 317–321 (2001)
39. Morillo, P., Padró, C., Sáez, G., Villar, J.L.: Weighted Threshold Secret Sharing Schemes. Inf. Process. Lett. 70, 211–216 (1999)
40. Murota, K.: Discrete convex analysis. SIAM Monographs on Discrete Mathematics and Applications. SIAM, Philadelphia (2003)
41. Ng, S.-L.: Ideal secret sharing schemes with multipartite access structures. IEEE Proc.-Commun. 153, 165–168 (2006)
42. Padró, C., Sáez, G.: Secret sharing schemes with bipartite access structure. IEEE Trans. Inform. Theory 46, 2596–2604 (2000)
43. Schrijver, A.: Combinatorial optimization. Polyhedra and efficiency. Springer, Berlin (2003)
44. Seymour, P.D.: On secret-sharing matroids. J. Combin. Theory Ser. B 56, 69–73 (1992)
45. Shamir, A.: How to share a secret. Commun. of the ACM 22, 612–613 (1979)
46. Simmons, G.J.: How to (Really) Share a Secret. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 390–448. Springer, Heidelberg (1990)
47. Simonis, J., Ashikhmin, A.: Almost affine codes. Des. Codes Cryptogr. 14, 179–197 (1998)
48. Stinson, D.R.: An explication of secret sharing schemes. Des. Codes Cryptogr. 2, 357–390 (1992)
49. Stinson, D.R.: Decomposition constructions for secret-sharing schemes. IEEE Transactions on Information Theory 40, 118–125 (1994)
50. Tassa, T.: Hierarchical Threshold Secret Sharing. J. Cryptology 20, 237–264 (2007)
51. Tassa, T., Dyn, N.: Multipartite Secret Sharing by Bivariate Interpolation. J. Cryptology 22, 227–258 (2009)