Journal of Universal Computer Science, vol. 15, no. 14 (2009), 2881-2893
submitted: 28/8/07 accepted: 27/7/09, appeared: 1/8/09

Ideal Homogeneous Access Structures Constructed from Graphs

Javier Herranz
(Dept. Matemàtica Aplicada IV
Universitat Politècnica de Catalunya
C. Jordi Girona, 1-3, Mòdul C3, 08034 Barcelona, Spain
jherranz@ma4.upc.edu)

Abstract: Starting from a new relation between graphs and secret sharing schemes introduced by Xiao, Liu and Zhang, we show a method to construct more general ideal homogeneous access structures. The method has some advantages: it efficiently gives an ideal homogeneous access structure for the desired rank, and some conditions can be imposed (such as forbidden or necessary subsets of players), even if the exact composition of the resulting access structure cannot be fully controlled. The number of homogeneous access structures that can be constructed in this way is quite limited; for example, we show that (t, ℓ)-threshold access structures can be constructed from a graph only when $t = 1$, $t = \ell - 1$ or $t = \ell$.

Key Words: cryptography, ideal secret sharing, graph connectivity
Category: E.3, G.2

1 Introduction: Secret Sharing Schemes

Distributed public key cryptography deals with scenarios where a cryptographic secret task (signing or decrypting) is performed by a collective of users -persons, machines, devices, in general we refer to them as *players*- instead of an individual user. In this way, the systems win in security and reliability.

An important point in these schemes is to determine which subsets of players are authorized to perform the secret task. A usual strategy to design distributed cryptographic schemes is to use a *secret sharing scheme* to distribute shares of the secret key of a known individual cryptographic scheme.

Secret sharing schemes were introduced independently in 1979, by Shamir [Shamir 1979] and Blakley [Blakley 1979]. Let $\mathcal{P} = \{P_1, \ldots, P_\ell\}$ be a set of ℓ players. In this set of players, a family of authorized or qualified subsets $\Gamma \subset 2^{\mathcal{P}}$ must be defined. This family is called the *access structure* of the scheme, and it must be *monotone increasing*; that is, if $A_1 \in \Gamma$ and $A_1 \subset A_2 \subset \mathcal{P}$, then $A_2 \in \Gamma$. Because of this property, an access structure is determined by its basis $\Gamma_0 = \{A \in \Gamma \mid A - \{P_i\} \notin \Gamma, \text{ for all } P_i \in A\}$.

If all the subsets in the basis Γ_0 of an access structure Γ have the same cardinality r, then we say that Γ is an *homogeneous* access structure with *rank* r. These kind of access structures have been studied, e.g., in [Padró and Sáez 2002], for the general case. For the particular case $r = 2$, these structures can be represented by graphs (see [Blundo et al. 1995], for example).

Given a monotone increasing access structure Γ and a secret to be shared, the idea behind a secret sharing scheme is that each player of the set $\mathcal{P}$ receives from a trusted authority (the *dealer*, usually denoted by D) a share of the secret. A secret sharing scheme is said to be *perfect* if the two following conditions hold:

(i) from the shares of any authorized subset, in Γ, the secret can be recovered;

(ii) from the shares of a non-authorized subset, not in Γ, no information about the secret is obtained.

The parameter that measures the efficiency of a secret sharing scheme is the *information rate*, which is the quotient between the length of the secret (in bits) and the maximum length of the shares distributed to the players. The information rate of a perfect secret sharing scheme is at most 1; when this is the case, i.e. when the length of all the shares is the same as the length of the shared secret, we say that the secret sharing scheme (and also the realized access structure) is *ideal*.

Shamir proposed in [Shamir 1979] a *threshold* scheme, where subsets that can recover the secret are those with at least t members (t is the threshold), or in other words, the access structure is $\Gamma = \{A \subset \mathcal{P} : |A| \geq t\}$ (such structures are called (t, ℓ)-threshold access structures, where ℓ is the total number of players and $1 \leq t \leq \ell$). The scheme is ideal and is based on polynomial interpolation.

A more general family of ideal secret sharing schemes are *vector space secret sharing schemes*, introduced by Brickell in [Brickell 1989]. An access structure Γ is realizable by such a scheme, over a finite field $\mathcal{K}$, if there exist a positive integer d and a map $\psi : \mathcal{P} \cup \{D\} \longrightarrow \mathcal{K}^d$ such that $A \in \Gamma$ if and only if $\psi(D) \in \langle \psi(P_i) \rangle_{P_i \in A}$, where $\langle \cdot \rangle$ denotes the linear subspace generated by the indicated vectors. In this case, we say that Γ is a *vector space access structure*. If the dealer wants to distribute a secret value $s \in \mathcal{K}$ according to such an access structure, he takes a random vector $\boldsymbol{\omega} \in \mathcal{K}^d$, such that $\boldsymbol{\omega} \cdot \psi(D) = s$, where $\cdot$ denotes the inner product of two vectors. The share of a participant $P_i \in \mathcal{P}$ is $s_i = \boldsymbol{\omega} \cdot \psi(P_i) \in \mathcal{K}$. Let A be an authorized subset, $A \in \Gamma$; then, by definition, $\psi(D) = \sum_{P_i \in A} \lambda_i^A \psi(P_i)$, for some values $\lambda_i^A \in \mathcal{K}$. In order to recover the secret from their shares, the players of A compute

$$\sum_{P_i \in A} \lambda_i^A s_i \ = \ \sum_{P_i \in A} \lambda_i^A \boldsymbol{\omega} \cdot \psi(P_i) \ = \ \boldsymbol{\omega} \cdot \sum_{P_i \in A} \lambda_i^A \psi(P_i) \ = \ \boldsymbol{\omega} \cdot \psi(D) \ = \ s \ .$$

Such secret sharing schemes are ideal: all the shares and the secret belong to the same finite field $\mathcal{K}$, so they all have the same length.

Vector space secret sharing schemes can also be generalized. Simmons, Jackson and Martin [Simmons et al. 1991] introduced *linear secret sharing schemes*, that can be seen as vector space ones in which each player can be associated with more than one vector, leading therefore to non-ideal schemes. They proved that any access structure can be realized by a linear secret sharing scheme. In general, the construction that they proposed results in an inefficient secret sharing scheme, with a very low information rate.

As we have already said, secret sharing schemes are used as primitives in the design of other cryptographic protocols: distributed encryption schemes [Canetti and Goldwasser 1999, Fouque et al. 2001], distributed signature schemes [Herranz and Sáez 2006], attribute-based encryption [Waters 2008], etc. In all these protocols, efficiency of the inherent secret sharing techniques (in particular, the length of the shares) is very important. For this reason, it is desirable to consider ideal access structures, for example those which can be realized by a vector space secret sharing scheme. In some situations, this efficiency property may be even more important than the exact composition of the access structure itself. This observation motivates the results that we provide in this paper.

Our contribution. Following the ideas introduced in [Xiao et al. 2007], we propose a method to construct ideal homogeneous access structures and secret sharing schemes realizing them, starting from graphs. In [Section 2] we review the construction introduced in [Xiao et al. 2007] of ideal access structures based on the connectivity of graphs. In [Section 3], we extend this construction in order to obtain a larger number of ideal access structures and secret sharing schemes. We enumerate in [Section 4] some situations from real life where these constructions can be useful. As a negative result, we prove that (t, ℓ)-threshold access structures can be obtained through our constructions only for the cases $t = 1$, $t = \ell - 1$ or $t = \ell$. Then, we argue in [Section 5] that it is impossible to obtain similar results when working with hypergraphs instead of graphs, and we explain in [Section 6] the relation between the results of this paper and matroids. Conclusions and some open problems are given in [Section 7].

2 Graphs and Access Structures

The relation between (non-directed) graphs and access structures has been considered in many works. The traditional scenario [Blundo et al. 1995] was the following: given a graph $G(V, E)$ with set of vertices V and set of edges E, the set of players $\mathcal{P}$ was defined as the set of vertices E, and then a pair of players was authorized to recover the secret if and only if there existed an edge between the two corresponding vertices. In this way, the resulting access structures were homogeneous with rank 2.

In [Xiao et al. 2007], Xiao, Liu and Zhang propose a different relation between graphs and access structures. Now the players will be represented as edges of the graph, not as vertices. They consider complete graphs $G(V, E) = K_m$, where there are m vertices and all the possible edges; that is, $V = \{v_1, v_2, \ldots, v_m\}$ and $E = \{v_i v_j \mid 1 \leq i < j \leq m\}$. Each player of the secret sharing scheme is associated to an edge of the complete graph K_m. Therefore, the set of players $\mathcal{P} = \{P_{ij}\}_{1 \leq i < j \leq m}$, where player P_{ij} is represented by the edge $v_i v_j$, has cardinality $\ell = \binom{m}{2}$. Given a subset of players $A \subset \mathcal{P}$, we denote as E_A the set of edges associated to players in A, and we denote as $G(V, E_A)$ the graph obtained by considering only the edges in E_A.

The access structure is then defined as

$$\Gamma_G = \{A \subset \mathcal{P} \mid G(V, E_A) \text{ is a connected graph}\}.$$

With this definition, it is easy to see that the basis Γ_0 of Γ corresponds exactly to the set of spanning trees of the graph $G(V, E)$. Since all the spanning trees contain $m - 1$ edges, then we conclude that Γ is an homogeneous access structure with rank $r = m - 1$.

In [Xiao et al. 2007], the authors propose a vector space secret sharing scheme realizing such access structures Γ_{K_m}. Let $\mathcal{K}$ be a finite field with enough elements (more than m), and let us consider a basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_{m-1}\}$ of the vector space $\mathcal{K}^{m-1}$. The vertex v_1 of the graph is associated with the vector $\mathbf{w} = \mathbf{0}$; then, for $i = 2, \ldots, m$, vertex v_i is associated with the vector $\mathbf{w}_i = \sum_{j=1}^{i-1} \mathbf{v}_j$.

Finally, if player P_{ij} is the player corresponding to the edge $v_i v_j$, then the vector assigned to this player is $\psi(P_{ij}) = \mathbf{w}_i - \mathbf{w}_j$. It is proved in [Xiao et al. 2007] (Theorem 1) that one can then find a vector $\psi(D) \in \mathcal{K}^{m-1}$ such that the vector space secret sharing scheme defined by the assignment of vectors $\psi : \mathcal{P} \cup \{D\} \to \mathcal{K}^{m-1}$ realizes the access structure Γ_{K_m}.

3 Constructing More Access Structures

The construction proposed in [Xiao et al. 2007] is very nice and shows a different approach to the connections between graphs and ideal secret sharing schemes. However, it has the limitation that only few access structures can be constructed in this way. In this section we generalize the given construction by relaxing this limitation, in order to obtain more ideal homogeneous access structures.

The inherent principles in our generalizations are quite simple: the idea is to consider *minors* of the access structure Γ_{K_m} (the 'minor' terminology has been taken from [Martí-Farré and Padró 2007]). Given an access structure $\Gamma \subset 2^{\mathcal{P}}$ and a subset of players $B \subset \mathcal{P}$, we can considered the following two access structures on the set $\mathcal{P} - B$:

$$\Gamma \backslash B = \{A \subset \mathcal{P} - B \ : \ A \in \Gamma\},$$

$$\Gamma / B = \{A \subset \mathcal{P} - B \ : \ A \cup B \in \Gamma\}$$

Lemma 1. *If $\Gamma \subset 2^{\mathcal{P}}$ is an ideal access structure and $B \subset \mathcal{P}$, then both $\Gamma \backslash B$ and Γ / B are ideal access structures.*

Proof. Given an ideal secret sharing scheme Σ realizing Γ, let us concentrate on the shares for the players in B. If the dealer keeps these shares private and runs Σ on the players in $\mathcal{P} - B$, then the access structure $\Gamma \backslash B$ is ideally realized.

Alternatively, if the dealer publishes, along with the public parameters of Σ (for example, the inherent finite field $\mathcal{K}$), the shares of the players in B, then the access structure Γ / B is ideally realized. $\square$

In the rest of this section, we show that these two transformations, when applied to Γ_{K_m}, can overcome some of the limitations of the construction described in the previous section.

The most evident restriction in [Xiao et al. 2007] is the fact that only complete graphs K_m are considered. This is because the main objective of that paper is to construct multiparty computation protocols in the resulting access structures, and a necessary condition for doing this is $\mathcal{Q}^2$. An access structure Γ defined on a set of players $\mathcal{P}$ is $\mathcal{Q}^2$ if $B_1 \cup B_2 \neq \mathcal{P}$, for any pair of subsets $B_1, B_2 \notin \Gamma$. It is easy to see that access structures constructed from complete graphs K_m are $\mathcal{Q}^2$.

If only complete graphs K_m are considered, then the number ℓ of players in the access structure must be of the form $\ell = \binom{m}{2}$. That is, the resulting access structures are quite inflexible: a unique structure for $\ell = 6$ players with rank $r = m - 1 = 3$, a unique structure for $\ell = 10$ players with rank $r = m - 1 = 4$, a unique access structure for $\ell = 15$ players with rank $r = m - 1 = 5$, and so on.

A first and obvious step to generalize the construction consists in considering non-complete graphs $G(V, E)$. If the graph has $m = |V|$ vertices, then the number of players (or edges) must be at least $m - 1$, to ensure the existence of some spanning tree and to ensure therefore that $\Gamma \neq \emptyset$. The graph $G(V, E)$ is a subgraph of K_m, if $|V| = m$, that has been obtained by removing from K_m some subset E_B of edges. If B denotes the subset of players, in Γ_{K_m}, associated to this subset of edges E_B, then it is easy to see that $\Gamma_{G(V,E)} = \Gamma_{K_m} \backslash B$ and so $\Gamma_{G(V,E)}$ is also ideal (by Lemma 1). In this way, we will obtain more ideal access structures of rank $r = m - 1$, where the number of players ℓ is still restricted to $m - 1 \leq \ell \leq \binom{m}{2}$, or in other words:

$$r \leq \ell \leq \binom{r+1}{2}.$$

This means, for example, that we cannot obtain with this method an ideal access structure with rank $r = 4$ for a set of $\ell = 11$ players or more.

Now we explain how to give one more step to overcome this limitation and obtain more access structures. The idea is to consider fixed edges in the graph, which represent artificial players. We start from a graph $G'(V, E')$ with $m = |V|$ vertices and a fixed acyclic set E' of $e < m - 1$ edges. Therefore, the number of connected components in this graph $G'(V, E')$ is $c = m - e > 1$. After that, we can add new edges to the graph, representing the real players, until we obtain a graph $G(V, E)$, where $E' \subset E$. If we denote as $\mathcal{P}$ the players corresponding to the access structure $\Gamma_{G(V,E)}$ and as $B \subset \mathcal{P}$ the players corresponding to the subset of edges E', then the access structure on the set of players $\mathcal{P} - B$ is naturally defined as

$$\Gamma' = \{A \subset \mathcal{P} - B \mid G(V, E_A \cup E') \text{ is a connected graph}\},$$

and one can easily check that $\Gamma' = \Gamma_{G(V,E)}/B$. Therefore, this access structure will also be ideal, according to Lemma 1.

Connecting the graph $G'(V, E')$ means connecting c connected components; therefore, the resulting access structure is homogeneous with rank $r = c - 1$. Obviously, the added edges in $E - E'$ must not connect two vertices which are in the same connected component of $G'(V, E')$, because the corresponding players would be irrelevant in the access structure Γ.

In general, given a set of ℓ players and a desired rank $r \in \{1, \ldots, \ell\}$, we are always able to obtain with this method an ideal access structure which is homogeneous with rank r. For this, it suffices to start from a graph $G'(V, E')$ with $c = r+1$ connected components $G'_i(V_i, E'_i)$, where $|V_i| = m_i$ for $i = 1, \ldots, c$. The necessary condition is that we can add later the ℓ edges of the real players to the initial graph, connecting different components. This will be ensured if

$$\sum_{1 \le i < j \le c} m_i m_j \;\ge\; \ell.$$

For example, taking into account that $c = r+1$, we can achieve this by imposing $|V_i| = \tilde{m}$ for all $i = 1, \ldots, c$, such that

$$\frac{r(r+1)}{2}\,\tilde{m}^2 \;\ge\; \ell.$$

An Example. With our method, we can now construct an homogeneous access structure with rank $r = 4$ for a set $\mathcal{P}$ of $\ell = 12$ players. For example, by considering an initial graph $G'(V, E')$ with $m = 7$ vertices and $e = 2$ edges. Figure 1 shows the initial graph $G'(V, E')$ and the final graph $G(V, E)$, where dotted lines represent the initial (fixed) edges in E', and full lines represent the added edges $E - E'$ corresponding to the players in $\mathcal{P} = \{P_1, \ldots, P_{12}\}$. Some subsets of 4 players which are authorized are $\{P_1, P_2, P_3, P_4\}$ or $\{P_2, P_5, P_6, P_{12}\}$, for example, whereas some subsets of 4 players which are not authorized are $\{P_1, P_2, P_3, P_6\}$, $\{P_2, P_5, P_7, P_{10}\}$ and, in general, any subset of 4 players whose associated edges, plus the two edges in E', form some cycle in $G(V, E)$.

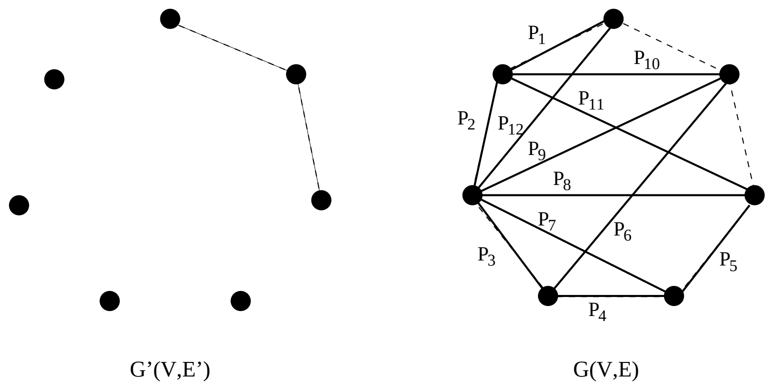

Figure 1: An example of the new construction

4 Possible Uses of the New Construction

The main objection that can be made to the construction presented in the previous section is that one cannot control the exact access structures which result from the construction. That is, we will know the number of players and the rank of the access structure, and we can impose some partial conditions, but we cannot pretend to construct with this method a specific access structure given *a priori*, in general.

On the other hand, the construction can be useful in some scenarios (including distributed signature / decryption schemes), where someone wants to efficiently implement a distributed protocol for some access structure with some properties, but where the exact composition of the access structure is not very relevant. Let us show some examples.

4.1 Forbidden Subsets

Assume the head of a company wants to quickly distribute the signing power of the company among its ℓ members, in such a way that r players are needed to compute valid signatures. The head wants to impose some conditions: he does not mind if some particular subsets of r players are not able to compute signatures; in fact, there are some particular subsets, say $B_1, \ldots, B_d$, each one containing r players, which should be unable to compute signatures, because the head suspects they do not contain any reliable member, for example. A solution is to apply our construction based on graphs to obtain an access structure of rank r for the set of ℓ players, imposing that the edges of the subset B_i form at least one cycle, for all $i = 1, \ldots, d$. Note that the question of forbidden subsets

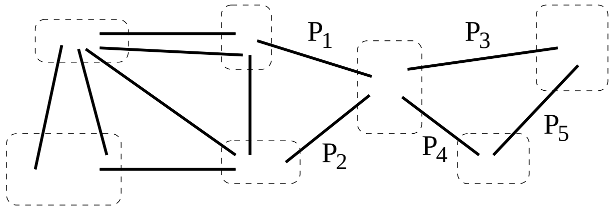

Figure 2: (a) P_1 or P_2 are necessary, and two out of $\{P_3, P_4, P_5\}$ are necessary

was easier in the standard scenario of graph-based access structures where users are vertices and edges represent authorized pairs (see [Sun and Shieh 1996], for example).

4.2 Necessary Players or Subsets

Assume now that one wants to obtain an access structure of rank r for ℓ players, such that some players must be necessarily involved in order to form an authorized subset. Again, if we can afford the fact that some subsets of r players will not be authorized, then we can use our construction to quickly and efficiently obtain an ideal secret sharing scheme satisfying the above-mentioned necessity requirements.

For example, figure 2 shows a situation where the minimal authorized subsets will contain 6 players, such that the presence of either P_1 or P_2 is necessary, and also the presence of at least two players of the set $\{P_3, P_4, P_5\}$ is required. Dotted figures represent the connected components of the initial graph $G'(V, E')$, while full lines represent the edges of the real players.

4.3 Can Threshold Access Structures Be Constructed from Graphs?

One could think that this method to construct ideal secret sharing schemes could be used to theoretically characterize ideal access structures of rank r, i.e. to obtain a result such as: *an access structure of rank r is ideal if and only if it can be constructed from a graph by using the methods explained above.*

This very optimistic goal is ruled out at once, since even the most simple ideal homogeneous access structures, which are (t, ℓ)-threshold ones, can be constructed from a graph only when $t = 1$, $t = \ell - 1$ or $t = \ell$.

The case $t = 1$ can be obtained by considering an initial graph $G'(V, E')$ with two connected components $G'_1(V_1, E'_1)$ and $G'_2(V_2, E'_2)$, and then by adding the edges of the ℓ real players, each connecting a vertex in V_1 with a vertex in V_2.

The case $t = \ell$ can be easily obtained by considering as initial graph $G'(V, E')$ a set of $m = \ell + 1$ isolated vertices, that is $E' = \emptyset$. The final graph $G(V, E)$ is just some spanning tree for V, formed by $\ell + 1$ vertices and $t = \ell$ edges.

To obtain the case $t = \ell - 1$, we start from the initial graph $G'(V, E')$ formed by $m = \ell$ isolated vertices. We add ℓ edges for the players to form the cycle C_ℓ (of length ℓ) as the final graph $G(V, E)$. Any subset of $t = \ell - 1$ edges is a path of length $t = \ell - 1$, and so a spanning tree of $G(V, E)$, as desired.

For the rest of cases, we prove the following impossibility result.

Proposition 2. *A (t, ℓ)-threshold access structure cannot be obtained from our graph-based construction, if $1 < t < \ell - 1$.*

Proof. Let us assume the contrary. Since the resulting access structure would be of rank t, the initial graph $G'(V, E')$ should have $t + 1$ connected components $G'_i(V_i, E'_i)$, for $i = 1, \dots, t + 1$. We can imagine $G'(V, E')$ therefore as a graph with $t + 1$ isolated big-vertices, one for each $G'_i(V_i, E'_i)$. Now we should place in this graph the edges corresponding to the real players $\mathcal{P} = \{P_1, \dots, P_\ell\}$.

We consider the first t players. Since they form an authorized subset, their edges must form a spanning tree. We must still add $\ell - t \geq 2$ edges. When we add the edge for the player P_{t+1}, a cycle appears; there are two possibilities.

(i) The degree of each big-vertex $G'_i(V_i, E'_i)$ is at least 2. Since there are $t + 1$ big-vertices and $t + 1$ edges at this moment, the only possibility is that the big-vertices form a cycle C_{t+1} (that is, the degree of all the big-vertices is 2). Now we must still add at least one more edge for player P_{t+2}, because $t + 2 \leq \ell$. Once this edge is added, two of the big-vertices will have now degree 3. However, since the number of big-vertices is $t + 1 \geq 3$, there is at least one big-vertex $G'_j(V_j, E'_j)$ which still has degree 2; we can denote as P_{j_1} and P_{j_2} the players associated with the two edges inciding $G'_j(V_j, E'_j)$. If we consider the set $A = \{P_1, \dots, P_{t+2}\} - \{P_{j_1}, P_{j_2}\}$ of t players, it should be authorized, but the graph $G(V, E_A)$ is not connected because the big-vertex $G'_j(V_j, E'_j)$ remains isolated in $G(V, E_A)$. This gives us a contradiction.

(ii) The degree of some big-vertex $G'_j(V_j, E'_j)$ is 1 (corresponding to the edge of some player P_j), when we have already added $t + 1$ edges for the first $t + 1$ real players. Then the subset $B = \{P_1, \dots, P_{t+1}\} - \{P_j\}$ has t players, but it is not authorized because the big-vertex $G'_j(V_j, E'_j)$ is isolated, and so the resulting graph $G(V, E_B)$ is not connected. Again, a contradiction. $\square$

5 On Possible Extensions to Hypergraphs

Since the conclusion of the previous section is that the access structures $\Gamma_{G(V,E)}$ are far from covering all the spectrum of ideal homogeneous access structures, one could think of possible ways to further extend the ideas in this paper, in order to obtain even more ideal structures. A possible idea is to consider hypergraphs instead of graphs.

A *hypergraph* $HG(V,E)$ is defined by a set of vertices $V = \{v_1, \dots, v_n\}$ and a set of *hyperedges* $E \subset 2^V$. A hyperedge $e = \{v_{i_1}, \dots, v_{i_k}\} \subset V$ is therefore a subset of vertices. If all the hyperedges have the same cardinality k, then the hypergraph is called k-uniform. Graphs are 2-uniform hypergraphs. A hypergraph $HG(V,E)$ is connected if, for every subset of vertices $X \subset V$, there exists a hyperedge $e \in E$ such that both $e \cap X \neq \emptyset$ and $e \cap (V - X) \neq \emptyset$.

A generalization of the techniques in this paper to the case of hypergraphs would lead to access structures $\Gamma_{HG(V,E)}$ defined on a set $\mathcal{P}$ of $\ell = |E|$ players, where each player $i \in \mathcal{P}$ is associated to a hyperedge $e_i \in E$. Again, given a subset $E_A \subset E$ of hyperedges, for some $A \subset \mathcal{P}$, one can consider the sub-hypergraph $HG(V, E_A)$ which contains only the hyperedges in E_A. The access structure would be

$$\Gamma_{HG(V,E)} = \{A \subset \mathcal{P} \ : \ HG(V, E_A) \text{ is a connected hypergraph}\}.$$

This definition leads to a very large number of access structures. The next step would be to find an ideal secret sharing scheme realizing them. Unfortunately, the following result shows that there is no hope to find any construction of ideal secret sharing schemes realizing $\Gamma_{HG(V,E)}$ which works in general, for all hypergraphs $HG(V,E)$.

Proposition 3. *There exist hypergraphs $HG(V,E)$ which lead to non-ideal access structures $\Gamma_{HG(V,E)}$.*

Proof. Let us consider the 3-uniform hypergraph $HG(V,E)$ defined on a set V of $n = 5$ vertices, containing the following $\ell = 4$ hyperedges: $E = \{\{v_1, v_2, v_5\}, \{v_3, v_4, v_5\}, \{v_1, v_2, v_3\}, \{v_1, v_4, v_5\}\}$.

The resulting access structure, defined on a set $\mathcal{P} = \{1, 2, 3, 4\}$ of players (one for each hyperedge, in the given order) is $\Gamma_{HG(V,E)} = \{\{1,2\}, \{2,3\}, \{3,4\}\}$. It is well-known (see [Blundo et al. 1995], for example) that this access structure is non-ideal, for any finite field. $\square$

Therefore, an attempt to generalize the results in [Xiao et al. 2007] and in this paper to hypergraphs already fails in the first following step of 3-uniform hypergraphs. Of course, this does not mean that other generalizations may not exist; maybe some particular families of hypergraphs (not containing 3-regular ones!) lead to access structures for which it is always possible to construct ideal secret sharing schemes.

6 Secret Sharing and Matroids

There is a strong relation between ideal secret sharing and matroids, as it was shown in [Brickell and Davenport 1991]. For every vector space secret sharing scheme realizing an access structure Γ defined on a set $\mathcal{P}$ of players, there exits a *representable* matroid M with ground set $\mathcal{P} \cup \{D\}$, where $D \notin \mathcal{P}$ is a special point of the matroid M, such that $A \subset \mathcal{P}$ is minimal authorized if and only if $A \cup \{D\}$ is a maximally dependent subset (circuit) of M. Reciprocally, given a matroid $M = (\mathcal{Q}, \mathcal{I})$ with $n = |\mathcal{Q}|$ points and family of independent sets $\mathcal{I} \subset 2^{\mathcal{Q}}$, which is representable over a finite field $\mathcal{K}$, we can obtain n vector space access structures (over $\mathcal{K}$), one for each point $p \in \mathcal{Q}$:

$$\Gamma_p = \{A \subset \mathcal{Q} - \{p\} \ : \ A \in \mathcal{I} \text{ and } A \cup \{p\} \notin \mathcal{I}\}.$$

It is possible to construct matroids by starting from a graph; this leads to *graphic* matroids (see [Oxley 1992], for example): given a graph $G(V,E)$, the ground set of the graphic matroid $M(G)$ is the set of edges E, whereas the independent sets of $M(G)$ are the acyclic subsets of edges. It is a well-known result that graphic matroids are representable over any finite field.

At first glance, graphic matroids are very related to the access structures $\Gamma_{G(V,E)}$ considered in this paper. This fact, along with the fact that all graphic matroids are representable over any finite field, could lead to the conclusion that the vector space secret sharing schemes realizing $\Gamma_{G(V,E)}$ that we have discussed in this work are nothing new or surprising. But this is not true at all; given a graph $G(V,E)$, it is possible that the access structure $\Gamma_{G(V,E)}$ does not come from any graphic matroid. In other words, there does not exist any graph $G'(V',E')$ such that the graphic matroid $M(G') = (\mathcal{Q}, \mathcal{I})$ leads, by fixing a point in $\mathcal{Q}$, to the access structure $\Gamma_{G(V,E)}$.

Proposition 4. *There exist homogeneous ideal access structures $\Gamma_{G(V,E)}$ that do not come from any graphic matroid $M(G')$, for any graph $G'(V',E')$.*

Proof. Let us consider the access structure Γ_{K_4} obtained from the complete graph K_4. There are six participants, $\mathcal{P} = \{1,2,3,4,5,6\}$, one for each edge of the graph, and the access structure is

$$(\Gamma_{K_4})_0 = \{ \ \{1,2,3\}, \{1,2,4\}, \{1,2,6\}, \{2,3,4\}, \{2,3,5\},$$

$$\{2,4,5\}, \{2,4,6\}, \{3,4,6\}, \{3,5,6\}, \{4,5,6\} \ \}.$$

Now assume that Γ_{K_4} comes from a graphic matroid $M(G')$, for some graph $G'(V',E')$. Since $M(G')$ is graphic, it is representable over any finite field, in particular over $\mathcal{K} = \mathbb{Z}_2$. Using the relation between matroids and access structures, we conclude that Γ_{K_4} must be realizable by a vector space secret sharing scheme over $\mathcal{K} = \mathbb{Z}_2 = \{0,1\}$, as well.

Let $\psi : \mathcal{P} \cup \{D\} \rightarrow (\mathbb{Z}_2)^d$ be the map realizing Γ_{K_4} over $\mathbb{Z}_2$. Since $\{1,2,3\} \in (\Gamma_{K_4})_0$, $\{1,2,4\} \in (\Gamma_{K_4})_0$ and we work over $\mathbb{Z}_2$, we must have $\psi(D) = \psi(1) + \psi(2) + \psi(3)$ on the one hand, and $\psi(D) = \psi(1) + \psi(2) + \psi(4)$ on the other hand, which implies $\psi(3) = \psi(4)$. Analogously, $\{2,3,4\} \in (\Gamma_{K_4})_0$, so $\psi(D) = \psi(2) + \psi(3) + \psi(4)$. Combining this last equality and the equality $\psi(3) = \psi(4)$, we conclude that $\psi(D) = \psi(2)$, which means that the player 2 could always recover the secret, i.e. $\{2\} \in \Gamma_{K_4}$, a contradiction.

Therefore, Γ_{K_4} cannot come from a graphic matroid $M(G')$. □

The conclusion of this section is that, despite the similarities between $\Gamma_{G(V,E)}$ and graphic matroids, the constructions of ideal secret sharing schemes realizing $\Gamma_{G(V,E)}$ proposed in [Xiao et al. 2007] and in this paper are interesting and original on their own.

7 Conclusion

We have generalized in this work the method introduced in [Xiao et al. 2007] to construct, from graphs, a larger number of ideal homogeneous access structures. Even if one cannot fully control the exact composition of the resulting access structures, one can impose some conditions, like fixing some necessary players or non-authorized subsets of players.

On the other hand, it is quite clear that the proposed method cannot be thought as a tool to characterize ideal homogeneous access structures. In particular, we prove that even (t, ℓ)-threshold access structures cannot be constructed from a graph, when $1 < t < \ell - 1$. Therefore, the problem of characterizing which homogeneous access structures of rank r are ideal is still open (see [Padró and Sáez 2002] for some related results).

References

[Blakley 1979] Blakley, G.R.: "Safeguarding cryptographic keys"; Proc. National Computer Conference, American Federation of Information, Processing Societies Proceedings 48 (1979), 313–317.

[Blundo et al. 1995] Blundo, C., De Santis, A., Stinson D., Vaccaro, U.: "Graph decompositions and secret sharing schemes"; J. Cryptology, 8 (1995), 39–64.

[Brickell 1989] Brickell, E.F.: "Some ideal secret sharing schemes"; J. Combinatorial Mathematics and Combinatorial Computing, 9 (1989), 105–113.

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

[Canetti and Goldwasser 1999] Canetti, R., Goldwasser, S.: "An efficient threshold public key cryptosystem secure against adaptive chosen ciphertext attack"; Proceedings of Eurocrypt'99, Lecture Notes in Computer Science 1592, Springer-Verlag (1999), 90–106.

[Fouque et al. 2001] Fouque, P.A., Poupard, G., Stern, J.: "Sharing decryption in the context of voting or lotteries"; Proceedings of Financial Cryptography 2000, Lecture Notes in Computer Science 1962, Springer-Verlag (2001), 90–104.

[Herranz and Sáez 2006] Herranz, J., Sáez, G.: "Distributed ring signatures from general dual access structures"; Designs, Codes and Cryptography, 40, 1 (2006), 103–120.

[Martí-Farré and Padró 2007] Martí-Farré, J., Padró, C.: "On secret sharing schemes, matroids and polymatroids"; Proceedings of Theory of Cryptography Conference 2007, Lecture Notes in Computer Science 4392, Springer-Verlag (2007), 273–290.

[Oxley 1992] Oxley, J.G.: "Matroid theory"; Oxford Science Publications; The Clarendon Press, Oxford University Press, New York (1992).

[Padró and Sáez 2002] Padró, C., Sáez, G.: "Lower bounds on the information rate of secret sharing schemes with homogeneous access structure"; Information Processing Letters, 83 (2002), 345–351.

[Shamir 1979] Shamir, A.: "How to share a secret"; Communications of the ACM, 22 (1979), 612–613.

[Simmons et al. 1991] Simmons, G.J., Jackson, W., Martin, K.: "The geometry of secret sharing schemes"; Bulletin of the ICA, 1 (1991), 71–88.

[Sun and Shieh 1996] Sun, H.M., Shieh, S.P.: "An efficient construction of perfect secret sharing schemes for graph-based structures"; Computers & Mathematics with Applications, 31, 7 (1996), 129–135.

[Xiao et al. 2007] Xiao, L., Liu, M., Zhang, Z.: "Multiplicative linear secret sharing schemes based on connectivity of graphs"; IEEE Transactions on Information Theory, 53, 11 (2007), 3973–3978.

[Waters 2008] Waters, B.: "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization"; ePrint report 2008/290, available at `http://eprint.iacr.org/2008/290` (2008).