Hypergraph Decomposition and Secret Sharing

Giovanni Di Crescenzo[1] and Clemente Galdi[2⋆]

[1] Telcordia Technologies Inc.,
445 South Street, Morristown, New Jersey, 07960, USA.
giovanni@research.telcordia.com
[2] Research Academic Computer Technology Institute and
Department of Computer Engineering and Informatics
University of Patras, 26500, Rio, Greece
clegal@ceid.upatras.gr

Abstract. In this paper we investigate the construction of efficient secret sharing schemes by using a technique called *hypergraph decomposition*, extending in a non-trivial way the previously studied graph decomposition technique. A major advantage advantage of hypergraph decomposition is that it applies to *any* access structure, rather than only structures representable as graphs. As a consequence we obtain secret sharing schemes for several classes of access structures with improved efficiency over previous results. We also obtain an elementary characterization of the ideal access structures among the hyperstars, which is of independent interest.

Keywords: Cryptography, Secret Sharing, Algorithms, Hypergraph Decomposition.

1 Introduction

A secret sharing scheme is a pair of efficient algorithms: a distribution algorithm and a reconstruction algorithm, run by a dealer and some parties. The distribution algorithm is executed by a dealer who, given a secret, computes some shares of it and gives them to the parties. The reconstruction algorithm is executed by a qualified subset of parties who, by putting together their own shares, can therefore reconstruct the secret. A secret sharing scheme satisfies the additional property that any non-qualified subset of participants does not obtain any information about the secret. The set of qualified subsets of parties is also called "access structure". The notion of secret sharing was introduced by Blackley [2] and Shamir [11], who considered the important case in which the access structure contains all subsets of size at least k, for some integer k.

Since their introduction, secret sharing schemes have been widely employed in the construction of more elaborated cryptographic primitives and several types

⋆ Work done while visiting Telcordia Technologies. The visit of the author to Telcordia Technologies has been partially supported by DIMACS under grant NSF CCR 99-06105. The work of the second author is partially supported by the European Union under IST FET Project CRESCCO, and RTN Project ARACNE.

T. Ibaraki, N. Katoh, and H. Ono (Eds.): ISAAC 2003, LNCS 2906, pp. 645–654, 2003.

of cryptographic protocols. Being so often employed, central research questions in this area are both the construction of efficient secret sharing schemes for several classes of access structures, and finding bounds on the possible efficiency that any such scheme can achieve for a certain access structure. The efficiency measures studied in the literature, and the ones that we will also consider in this paper, are related to the size of the largest distributed share (typically called "information rate", for its analogy with a so-called coding theory notion), or the sum of the distributed shares (typically called "average information rate"). The importance of these parameters is clear since they are directly related to the storage complexity, the communication complexity and the amount of secret information of the scheme. In the construction of efficient sharing schemes and in the search of bounds on such efficiency, the literature has paid special attention to the so-called "ideal" access structures; namely, access structures for which there exists a secret sharing scheme where the share distributed to each participant has the same size as the secret. (Note that this is well-known to be the best efficiency that one can achieve.) Further studied topics along these lines are: The classification of all access structures according to whether they are ideal or not, and the investigation of the efficiency of non-ideal access structures using ideal ones, using elegant techniques such as "graph decomposition".

In this paper we elaborate along this research direction by studying a non-trivial extension of the graph decomposition technique, which we call "hypergraph decomposition"; by applying this technique so to obtain secret sharing schemes that are dramatically more efficient than what previously known; and by finding novel and elementary characterization of ideal access structures within a large class of them.

Previous results. Secret sharing schemes have been proposed, for instance, in [11,2] for threshold structures, in [13] for all graph-based access structures, in [1] for all monotone circuits, in [12] for homogeneous access structures, rank requirements, in [10] for all access structures. Lower bounds on the size of shares for all secret sharing schemes have been proposed, for instance, in [7,3,4] for certain graph-based access structures, and in [14,9,15] for other classes of access structures. A characterization of ideal access structures in terms of weighted matroids has been presented in [6]. The *graph decomposition* technique [13,5] consists of decomposing a graph into smaller graphs whose union covers the original graph and representing ideal access structure. (We note that graphs can be associated only to access structures including all subsets containing some subsets of size 2.) This technique has been firstly extended in [14,12] for general access structures, where the author describes lower bounds for the information rate and average information rate for general access structure.

Our results. Following this line of research, in this paper we present the *hypergraph decomposition* technique, of decomposing an hypergraph into smaller hypergraphs whose union covers the original hypergraph and representing ideal access structures. A secret sharing scheme for the original hypergraph can then be obtained by composing the schemes for the smaller ones. Applying this technique requires (a) finding small hypergraphs which represent the access structure

and (b) finding the optimal decomposition of the input hypergraph into such smaller ones. As for (a), we consider simple structures such as hyperstars, and find a new and elementary condition that characterizes whether a given hyperstar is ideal or not. (This condition being more elementary than the condition in [6] that however characterizes all ideal access structures.) We prove (b) to be an NP-complete problem for general hypergraphs, but we note that it can be solved efficiently for special types of hypergraphs. We then move on to study special classes of access structures to which the hypergraph decomposition technique can be efficiently applied. Specifically, we study hyperpaths, hypercycles, hyperstars and hypertrees (all generalizing their graph-based counterpart) and obtain efficient secret sharing schemes for these structures. More specifically, for these classes of access structures, we give upper and lower bounds on the average information rate that improve on the previous known schemes. We further present optimal secret sharing schemes for hyperpaths and hypercycles.

Due to space constraints, several proofs are omitted from this extended abstract.

2 Definitions and Preliminaries

In this section we review some basic definitions and notations that will be used through the paper. Suppose $\mathcal{P}$ be a set of participants. We denote by $\mathcal{A}$ the set of subsets of parties which we desire to be able to reconstruct the secret, thus $\mathcal{A} \subseteq 2^{\mathcal{P}}$. Each set in $\mathcal{A}$ is said to be an *authorized set* while each set not in $\mathcal{A}$ is called a *forbidden set*. We define the family of *minimal sets* as $\delta^- A = \{A \in \mathcal{A} : \forall A' \in \mathcal{A} \setminus \{A\}, A' \not\subset A\}$. The set $\mathcal{A}$ is called the *access structure* and $\delta^- \mathcal{A}$ is said to be its *basis*. We will deal only with access structures that are *monotone*, i.e., they satisfy the following property: If $B \in \mathcal{A}$ and $B \subseteq C \subseteq \mathcal{P}$ then $C \in \mathcal{A}$. Thus, in order to describe an access structure it is sufficient to describe its basis.

Let $\mathcal{S}$ be a set of size q containing all the possible secrets to be shared. For every participant $P \in \mathcal{P}$ let us denote by $\mathcal{S}_P$ a the set containing all the possible information given to P by a secret sharing scheme. The elements in $\mathcal{S}_P$ are called shares. As done in the literature, we will denote by P both the party in the access structure and the random variable describing shares assigned to him. Similarly, we will denote by S both the secret to be shared and the random variable associated to it. Suppose a *dealer* $D \notin \mathcal{P}$ wants to share a secret $s \in S$ among the participants in $\mathcal{P}$. For each party in $P \in \mathcal{P}$ he selects one element in S_P and gives it to P. Using Shannon's entropy function (see [8] for a complete covering), we say a secret sharing scheme to be *perfect* if the following conditions hold:

1 $H(S|A) = 0, \forall A \in \mathcal{A}$ (Any set $A \in \mathcal{A}$ of participants who pool their shares together can recover the secret s).
2 $H(S|A) = H(S), \forall A \notin \mathcal{A}$ (Any set $A \notin \mathcal{A}$ of participants who pool their share together obtain no information on s.)

We will use two values for measuring the efficiency of a secret sharing schemes, the *information rate* ρ and the *average information rate* $\widetilde{\rho}$ defined as follows:

$$\rho = \frac{\log q}{\log \max\{|\mathcal{S}_P| : P \in \mathcal{P}\}} \qquad \widetilde{\rho} = \frac{|\mathcal{P}| \log q}{\sum_{P \in \mathcal{P}} \log |\mathcal{S}_P|}$$

It is easy to see that in any perfect secret sharing scheme, $q \leq \max\{|\mathcal{S}_P| : P \in \mathcal{P}\}$ and thus $\rho \leq 1$. A secret sharing scheme in which $\rho = 1$ is said to be *ideal*. An access structure having an ideal secret sharing scheme is also called ideal. Notice that as the (maximum) amount of information distributed to the parties increases, the information rate decreases. Thus the closer the information rate is to one, the more efficient the secret sharing scheme is.

The information rate considers only the "maximum size" among the share distributed to the parties. Sometimes it could be more preferable to consider the average size of the shares distributed by the secret sharing scheme. Since, in any perfect secret sharing scheme, for any $P \in \mathcal{P}$, $q \leq |\mathcal{S}_P|$ it is immediate that $\widetilde{\rho} \leq 1$. Moreover it is not hard to see that $\widetilde{\rho} \geq \rho$.

A *hypergraph* H is a pair (V, E) where V is a non-empty set of vertices and $E = \{E_1, \ldots, E_m\} \subseteq 2^V$ is a set of hyperedges. The hypergraph is said to be *connected* if for any two vertices $u, v \in V$ there exists a hyperpath from u to v in H. More formally there exists a sequence $E_{i_1}, \ldots, E_{i_s}$ such that $u \in E_{i_1}$, $E_{i_j} \cap E_{i_{j+1}} \neq \emptyset$ for each $j = 1, \ldots, s-1$, and $v \in E_{i_s}$.

Each access structure, $\mathcal{A} \subseteq 2^{\mathcal{P}}$, can be represented as a hypergraph $H = (\mathcal{P}, \mathcal{A})$ by letting each party being a vertex and each authorized set being represented as an hyperedge in the hypergraph.

Let $H = (V, E)$ be a hypergraph and let $W \subseteq V$. We say that the sub-hypergraph $H' = (V', E')$ is *S-induced* by W iff $E' = \{e \in E | e \cap W \neq \emptyset\}$ and $V' = \cup_{e \in E'} e$. For any subset $W \subseteq \mathcal{P}$, the sub-hypergraph S-induced by W represents a minimal sub-access structure containing all the vertices in W and, at the same time, all hyperedges that have non-empty intersection with W. (We note that the definition of S-induced subhypergraph does *not* reduce to the classical definition of *induced* subhypergraph.)

Let I be a set of hyperedges. We say that the *region* determined by the hyperedges in I is the set of vertices that belong to all the hyperedges in I and does not belong to any other hyperedge in the hypergraph. More formally: $R = \texttt{Region}(I) = (\cap_{E_i \in I} E_i) \setminus \cup_{E_i \in (E \setminus I)} E_i$. Moreover we say that R is an i-region if $|I| = i$. We also define the $\texttt{Remove}(H, R)$ to be hypergraph $H' = (V', E')$ where $V' = V \setminus R$ and $E' = \{E'_i = E_i \cap V' \neq \emptyset$ for any $E_i \in E\}$.

It is important to notice that $\texttt{Remove}(H, R)$ is no longer a substructure of H. Indeed some forbidden sets for H could be authorized sets for $\texttt{Remove}(H, R)$. It is immediate that the following holds:

Theorem 1. *Let $H = (V, E)$ be a hypergraph, $W \subseteq V$ and let H_W be the sub-hypergraph S-induced by W. Then $\rho(H) \leq \rho(H_W)$.*

We will extensively use some classes of hypergraphs that we are going to define formally. These hypergraphs are a natural generalization of graphs like

stars, paths and cycles. More precisely, a hypergraph $H = (V, E)$ is said to be a *hyperstar* if $A = \bigcap_{E_i \in E} E_i \neq \emptyset$. We will call A the *center* of the hyperstar. Notice that this definition is more general than the one of *sunflower* or *delta-system*, where it is required the egdes must have *pairwise* the same intersection. In our case, we simply require that the intersection of *all* the edges of the hypergraph must be non-empty. The hypergraph H is said to be a *hyperpath*, (resp. a *hypercycle*) if there exists an permutation $\pi : \{0, \ldots, m-1\} \to \{0, \ldots, m-1\}$ such that for any i, $E_{\pi(i)} \cap E_{\pi(i+1)} \neq \emptyset$ and $E_{\pi(i)} \cap E_{\pi(j)} = \emptyset$ if $j \notin \{i-1, i, i+1\}$ and $2 \leq i \leq m-1$, (resp., $j \notin \{i-1 \bmod m, i, i+1 \bmod m\}$ and $0 \leq i \leq m-1$). We will denote by P_m the hyperpath with m hyperedges and by C_m the hypercycle with m hyperedges.

3 Hypergraph Decomposition

In this section we describe the technique of hypergraph decomposition, a generalization of the graph decomposition technique studied in [5,13]. Given an access structure $\mathcal{A}$, we can construct a secret sharing for it as follows. We first represent $\mathcal{A}$ as an hypergraph H. Then we decompose the hypergraph in smaller sub-hypergraphs $H_1, \ldots, H_k$ for which efficient (and possibly ideal) secret sharing schemes are known and such that all the edges in H belong to at least one of the H_i. Thus each participant will receive a certain number of shares by means of each sub-structure H_i. The secret sharing for H is thus obtained as a "union" of the secret sharing of all the H_i's. Indeed since all the hyperedges in H are covered by the decomposition, each authorized set will be able to reconstruct the secret. On the other hand, the security of the secret sharing scheme for H is guaranteed by the security of the secret sharing schemes for the H_i's and by the fact that these schemes are independent. Notice that the performance of the secret sharing scheme not only depends on the performance of the decomposition of $\mathcal{A}$, but also on "how" the sub-structures combine together.

We now define formally a hypergraph decomposition:

Definition 1 (Hypergraph Decomposition). *Let $H = (V, E)$ be a hypergraph and let $\Delta = \{H_1, \ldots, H_k\}$, where $H_i = (V_i, E_i)$, with $E_i \subseteq E$ and $V_i = \cup_{e \in E_i} e$, be a set of sub-hypergraphs of H. The sequence Δ is said to be a decomposition of H if and only if each hyperedge in H belongs to at least one H_i. The decomposition is said to be ideal if the access structure represented each H_i is ideal. A decomposition $\Delta = \{H_1, \ldots, H_k\}$ of H is said to be a hyperstar decomposition of H if all the subhypergraphs H_i are hyperstars.*

Basic results (omitted here) about hypergraph decomposition include generalizations of two Theorems in [5]. Our first theorem allows to evaluate the information rate and the average information rate that can be achieved by a secret sharing scheme for an access structure $\mathcal{A}$ having a decomposition of the hypergraph representing $\mathcal{A}$. Our second theorem states that, having a number of distinct decompositions of a hypergraph, it is possible to construct secret sharing schemes that improve the average information rate w.r.t. the algorithm that use a single hypergraph decomposition.

In order to apply the hypergraph decomposition construction to a certain class of access structures, we have to solve the following two main problems.

- Define classes of ideal hypergraph-based access structures for which it is possible to construct in polynomial time an ideal secret sharing scheme.
- Represent the class of access structures given as a class of hypergraphs and find in polynomial time the optimal decomposition of these hypergraphs using only the ideal structures previously defined.

4 Hyperstars

In this section we give a complete characterization of the hyperstars having an ideal secret sharing scheme. We will show that it is possible in polynomial time to decide whether a given hyperstar represents an ideal access structure on not. This gives a new (and more elementary than [6]) characterization of ideal structures within this specific class of structures. We further give an algorithm that, on input an access structure $\mathcal{A}$ representable as an ideal hyperstar, realizes an ideal secret sharing scheme for it.

Theorem 2. *Let $H = (V, E)$ be a hyperstar with $E = (E_1, \ldots, E_m)$ and let $B_0, \ldots B_p$ be the set of all regions in H. Denote by $I_j \subseteq E$ the set of hyperedges determining B_j. There exists an ideal secret sharing scheme for H if and only if for each pair of sets I_{j_1} and I_{j_2} it holds that either $I_{j_1} \cap I_{j_2} = \emptyset$ or $I_{j_1} \subseteq I_{j_2}$ (or $I_{j_2} \subseteq I_{j_1}$).*

The key idea of the characterization is the fact that if a hyperstar H contains a non-ideal sub-hypergraph, than H itself cannot be ideal. On the other hand we need an algorithm that, given an ideal hyperstar, distributes to each party a share of the same size of the secret. We start by giving the condition under which a hyperstar is not ideal (in fact, we prove a stronger statement by quantifying the blowup on the size of the shares).

Lemma 1. *Let $H = (V, E)$ be a hyperstar with $|V| = n$, $E = (E_1, \ldots, E_m)$ and let $B_1, \ldots, B_p$ be the set of all regions in H. Denote by $I_j \subseteq E$ the set of hyperedges determining B_j. If there exist two non-empty sets I_{j_1} and I_{j_2} such that $I_{j_1} \cap I_{j_2} \neq \emptyset$, $I_{j_1} \setminus I_{j_2} \neq \emptyset$ and $I_{j_2} \setminus I_{j_1} \neq \emptyset$, then there exist two parties P_i and P_j such that $H(P_i) + H(P_j) \geq 3H(S)$.*

In the following lemma we show that if the condition of the previous lemma does not hold, then there exists an ideal secret sharing scheme for hypergraph H.

Lemma 2. *Let $H = (V, E)$ be a hyperstar with $|V| = n$, $E = (E_1, \ldots, E_m)$ and let $B_0, \ldots B_p$ be the set of all regions in H with B_0 being the center of H. Denote by $I_j \subseteq E$ the set of hyperedges determining B_j. If for each pair of sets I_{j_1} and I_{j_2} it holds that either $I_{j_1} \cap I_{j_2} = \emptyset$ or $I_{j_1} \subseteq I_{j_2}$ (or $I_{j_2} \subseteq I_{j_1}$), then $\texttt{Remove}(H, B_0)$ is the union of disjoint ideal hyperstars.*

This Lemma immediately suggests an algorithm that allows to construct an ideal secret sharing scheme for an ideal hyperstar. Roughly speaking, given an ideal hyperstar H, the algorithm applies a `Remove` operation on the center B_0 of H obtaining a set of disjoint (ideal) hyperstars. We write s as $s_1 \oplus s_2$ (the $\oplus$ operation being over GF(2)), and share s_1 among the parties in the center using a $(|B_0|, |B_0|)$-threshold scheme, and s_2 among the remaining parties of H. Since the hypergraph graph obtained is the union of a set of disjoint ideal hyperstars, we can recursively apply the same algorithm to each of these hyperstars by using s_2 as a secret. However, there are two algorithmic problems to be solved in order to realize this algorithm. The first one is how to efficiently partition the parties into disjoint regions. Notice that this problem can be easily solved in polynomial time. A second problem is how to verify that a given hyperstar is ideal. But, given the decomposition in regions of the hyperstar, this problem can be easily solved in polynomial time.

5 Average Information Rate

In this section we will give upper bounds on the average information rate for general access structures. By extending the proofs in [5], we can prove the problem of finding the optimal hyperstar decomposition to be NP-Hard. Moreover we can prove that it is possible to compute in polynomial-time, optimal secret sharing schemes for some classes of hypergraphs, namely hyperpaths, hypercycles and hypertrees. We can show that these schemes improve on the previously known secret sharing schemes. We further present upper bounds on the average information rate for some classes of hypergraphs, namely, hyperpaths, hypercycles and hypertrees.

5.1 Upper Bounds on the Average Information Rate

Given a hypergraph H, we construct a new hypergraph H' we call the *foundation* of H. The idea is to construct a hypergraph that contains all the vertices that will receive a share whose size is strictly greater than the size of the secret. More formally we have:

Definition 2 (Foundation). *Let $H = (V, E)$ be a hypergraph. The foundation of H is a hypergraph $H' = (V', E')$, where $V' = \cup_{E_i \in E'} E_i$ and for any hyperedge $E_i \in E$, $E_i \in E'$ if and only if there exist two hyperedges E_j, E_k such that:*

- $E_i \cap E_j \neq \emptyset$ *and* $E_i \cap E_k \neq \emptyset$
- $E_i \cap E_j \not\subseteq E_k$ *and* $E_i \cap E_k \not\subseteq E_j$

Consider a hyperedge E_i in the foundation hypergraph of H. We denote by $N(E_i)$ the set of hyperedges incident to E_i and satisfying the conditions of Definition 2. Moreover, for each E_i in the foundation hypergraph, there exist at least two regions, say $B_{i,1} = E_i \cap E_j$ and $B_{i,2} = E_i \cap E_k$ with $E_j, E_k \in N(E_i)$. By Lemma 1, some of the parties in these regions will receive shares whose size is strictly greater than the size of the secret. Two possible cases can arise:

- $E_i \cap E_j \cap E_k = \emptyset$. In this case, the three hyperedges form a hyperpath of length three that, by Theorem 2, is not ideal.
- $E_i \cap E_j \cap E_k \neq \emptyset$. In this case the three hyperedges form a hyperstar with three hyperedges and two 2-regions that, by Lemma 1 is not ideal.

Given H, we consider the following linear programming problem $\mathcal{A}(\mathcal{H})$.

$$\begin{aligned} \text{Minimize } C &= \textstyle\sum_{v \in V} a_v \\ a_v &\geq 0, v \in V \\ a_v + a_w &\geq 1, \forall E_i \in E', \forall E_j, E_k \in N(E_i), \forall v \in E_i \cap E_j, w \in E_i \cap E_k, j \neq k \end{aligned}$$

Theorem 3. *Let $H = (V, E)$ be a hypergraph with foundation H'. Let C^* the optimal solution for the problem $\mathcal{A}(H)$. Then $\widetilde{\rho}^*(H) \leq |V|/(C^* + |V|)$.*

Theorem 3 defines an upper bound on the average information rate for general access structures. In the next sections we are going to give specific upper bounds for particular classes of access structures, namely hyperpaths, hypercycles and hypertrees.

Before going on, we are going to prove a result that will be used in the rest of this section. For any hyperedge $E_j \in E'$ in the foundation hypergraph there are at least two *non-ideal regions* we call $B_{j,1}$ and $B_{j,2}$ with weight $w_{B_{j,1}} = |B_{j,1}|$ and $w_{Bj,2} = |B_{j,2}|$ respectively. Denote by $w_j = \min\{w_{B_{j,1}}, w_{B_{j,2}}\}$, $w_{min} = \min\{w_{B_{j,1}}, w_{B_{j,2}} | j = 1, \ldots |E'|\}$, and $w_{max} = \max\{w_{B_{j,1}}, w_{B_{j,2}} | j = 1, \ldots |E'|\}$.

Theorem 4. *Let H be a hypergraph, let $H' = (V', E')$ be its foundation and let $r = w_{min}/w_{max}$. If the vertices in V' have degree at most d than $C^* \geq r|E'|/d$.*

From this theorem it is possible to derive some interesting results on some classes of hypergraphs.

HyperCycles. The first class of hypergraphs we are going to consider is the class of hypercycles. It is not hard to see that the foundation hypergraph of C_m is the C_m itself. Moreover, the non-ideal regions in C_m are exactly all its 2-regions. Since C_m has maximum degree 2, by Theorem 4 we can obtain the following:

Corollary 1. *Let $C_m = (V, E)$ be a hypercycle, let $B_1, \ldots, B_m$ be its 2-regions and let $w_i =| B_i |$ for $i = 1, \ldots, m$. The it holds that: $\widetilde{\rho} \leq |V|/(rm/2 + |V|)$ where $r = \min_{1 \leq j \leq m} w_j / \max_{1 \leq j \leq m} w_j$*

HyperPaths. The next bound we are going to show is the upper bound on the average information rate for hyperpaths. It is not hard to see that the foundation hypergraph of a hyperpath P_m is isomorphic to P_{m-2}. More precisely, given a hyperpath P_m, its foundation hypergraph is obtained by removing the first and the last hyperedge in the hyperpath. Indeed all the other hyperedges in the hyperpath will be the middle-hyperedge of some subpaths of length 3.

Corollary 2. *Let $P_m = (V, E)$ be a hyperpath, and let P_{m-2} be its foundation hypergraph. Moreover let $B_1, \ldots, B_{m-2}$ be the 2-regions of P_{m-2} and let $w_i = |B_i|$ for $i = 1, \ldots, m-2$. The it holds that: $\widetilde{\rho} \leq |V|/(r(m-2)/2 + |V|)$ where $r = \min_{1 \leq j \leq m-2} w_j / \max_{1 \leq j \leq m-2} w_j$*

Hypertrees. Let H be a hypertree with at least four hyperedges. The foundation hypergraph of a hypertree contains at least all the internal vertices of the tree.

Corollary 3. *Let H be a hypertree with maximum degree d, let H' be its foundation and let $r = w_{min}/w_{max}$. It holds that $C^* \geq r|E'|/d$*

6 Optimal Information Rate

In this section we present a general lower bound on the information rate based on the multiple hypergraph decomposition. We shall show that using this technique it is possible to construct optimal secret sharing schemes for some classes of hypergraphs such as hyperpaths, hypercycles and hyperstars w.r.t. the information rate. For a hypergraph H define

$$\rho^*(H) = \sup\{\rho : \exists \text{ perfect secret sharing scheme for } H \text{ with information rate } \rho\}$$

We are interested in the best information rate we can obtain by multiple hypergraph decomposition. To this aim we define $\rho^*_M(H)$ to be this optimal information rate. It is immediate that $\rho^*_M(H) \leq \rho^*(H)$. We first generalize a result in [5] that allows to compute the value of $\rho^*_M(H)$.

Let $H = (V, E)$ be an hypergraph and assume $\Delta_j = \{H_{j1}, \ldots, H_{jk_j}\}$, with $j = 1, 2$ be two hypergraph decompositions of H. We can define a partial order on the Δ_j's as follows: Let $R_{jv} = |\{i : v \in H_{ji}\}|$. We say that $\Delta_i \leq \Delta_j$ if and only if $R_{iv} \leq R_{jv}$ for any $v \in V$. Define a hypergraph decomposition Δ_i to be *minimal* if there does not exists Δ_j such that $\Delta_j \leq \Delta_i$ and $\Delta_j \neq \Delta_i$. Now assume that $\Delta_j = \{H_{j1}, \ldots, H_{jk_j}\}$, with $j = 1, \ldots, L$ be a complete enumeration of all minimal hypergraph decomposition of H and for every vertex $v \in V$ and for any $j = 1, \ldots, L$ define $R_{jv} = |\{i : v \in H_{ji}\}|$. Consider the following optimization problem $\mathcal{I}(H)$

$$\begin{aligned} &\text{Minimize } R = \max\{\textstyle\sum_{j=1}^{L} a_j R_{jv} : v \in V\} \\ &\text{Subject to:} \quad a_j \geq 0, 1 \leq j \leq L \text{ such that } \textstyle\sum_{j=1}^{L} a_j = 1, \end{aligned}$$

The proof of the following theorem is a straightforward extension of the corresponding theorem in [5].

Theorem 5. *Let R^* be the optimal solution to $\mathcal{I}(H)$. Then $\rho^*_M(H) = 1/R^*$.*

Theorem 6. *Let P_m be the hyperpath with m hyperedges. Then $\rho^*(P_m) = 2/3$.*

Theorem 7. *Let C_m be the hypercycle with $m \geq 3$ hyperedges. Then if m is even $\rho^*(C_m) = 2/3$ otherwise $\rho^*_M(C_m) = (2n+1)/(3n+2)$*

Theorem 8. *Let H be a non-ideal hyperstar with three hyperedges. It holds that $\rho^*(H) = 2/3$.*

Corollary 4. *Let H be a non-ideal hyperstar with m hyperedges then $\rho^*(H) \leq 2/3$.*

References

1. J. Benaloh and J. Leichter, *Generalized secret sharing and monotone functions*, in Advances in Cryptology – CRYPTO '88, S. Goldwasser, ed., Lecture Notes in Computer Science 403 (1989), 27–35.
2. G. R. Blakley, *Safeguarding cryptographic keys*, in Proceedings of the National Computer Conference, 1979, American Federation of Information Processing Societies Proceedings 48 (1979), 313–317.
3. C. Blundo, A. De Santis, R. De Simone, and U. Vaccaro, *Tight Bounds on the Information Rate of Secret Sharing Schemes*, Design, Codes, and Cryptography, vol. 11, 1997, pp. 107–122.
4. C. Blundo, A. De Santis, L. Gargano and U. Vaccaro, *On the Information Rate of Secret Sharing Schemes,* in Theoretical Computer Science, vol. 154, pp. 283–306, 1996.
5. 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. Preliminary version appeared in EuroCrypt 92.
6. E. F. Brickell, D.M. Davenport, *On the Classification of Ideal Secret Sharing Schemes*, Journal of Cryptology, Vol. 4 (1991), pp. 123–134.
7. R.M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro, *On the Size of Shares for Secret Sharing Schemes*, Journal of Cryptology, vol. 6, n. 3, pp. 157–169, 1993.
8. T.M. Cover and J.A. Thomas, *Elements of Information Theory*, John Wiley & Sons, Singapore, 1991.
9. L. Csirmaz, *The Size of a Share Must be Large,* Journal of Cryptology, Vol. **10**, n. 4, pp. 223–231, 1997.
10. M. Ito, A. Saito and T. Nishizeki, *Secret sharing scheme realizing general access structure*, in Proceedings of the IEEE Global Telecommunications Conference, Globecom '87, IEEE Press, 1987, 99–102.
11. A. Shamir, *How to share a secret*, Communications of the ACM 22 (1979), 612–613.
12. D. R. Stinson, *New General Lower ounds on the Information Rate of Secret Sharing Schemes*, in Advances in Cryptology – CRYPTO '92, Lecture Notes in Computer Science 740 (1993), 170–184.
13. D. R. Stinson, *Decomposition Constructions for Secret Sharing Schemes*, IEEE Transactions on Information Theory, vol. 40, 1994.
14. D. R. Stinson, *An Explication of Secret Sharing Schemes*, Design, Codes and Cryptography, Vol. **2**, pp. 357–390, 1992.
15. M. van Dijk, *On the Information Rate of Perfect Secret Sharing Schemes,* in Design, Codes and Cryptography, vol. 6, pp. 143–169, 1995.