# On the Information Rate of Secret Sharing Schemes*

Carlo Blundo, Alfredo De Santis, Luisa Gargano, Ugo Vaccaro

Dipartimento di Informatica ed Applicazioni, Università di Salerno, 84081 Baronissi (SA), Italy

Preliminary version

**Abstract**

We derive new limitations on the information rate and the average information rate of secret sharing schemes for access structure represented by graphs. We give the first proof of the existence of access structures with optimal information rate and optimal average information rate less that $1/2+\epsilon$, where $\epsilon$ is an arbitrary positive constant. We also consider the problem of testing if one of these access structures is a sub-structure of an arbitrary access structure and we show that this problem is NP-complete. We provide several general lower bounds on information rate and average information rate of graphs. In particular, we show that any graph with $n$ vertices admits a secret sharing scheme with information rate $\Omega((\log n)/n)$.

## 1 Introduction

A secret sharing scheme is a method to distribute a secret $s$ among a set of participants $\mathcal{P}$ in such a way that only qualified subsets of $\mathcal{P}$ can reconstruct the value of $s$ whereas any other subset of $\mathcal{P}$, non-qualified to know $s$, cannot determine anything about the value of the secret. We briefly recall the results on secret sharing schemes that are more closely related to the topics of this paper.

Shamir [36] and Blackley [3] were the first to consider the problem of secret sharing and gave secret sharing schemes where each subset $A$ of $\mathcal{P}$ of size $|A| \geq k$ can reconstruct the secret, and any subset $A$ of participants of size $|A| < k$ have absolutely no information on the secret. These schemes are known as $(n, k)$ *threshold schemes*; the value $k$ is the threshold of the scheme and $n$ is the size of $\mathcal{P}$.

Ito, Saito and Nishizeki [25] considered a more general framework and showed how to realize a secret sharing scheme for any access structure. An access structure is a family of all subsets of $\mathcal{P}$ which are qualified to recover the secret. In case of $(n, k)$ threshold schemes the access structure consists of all subsets of $\mathcal{P}$ that have size greater than or equal to $k$. Their technique requires that the size of set where the shares are taken be very large compared to the size of the set where the secret is chosen. Benaloh and Leichter [2] proposed a technique to realize a secret sharing scheme for any access structure more efficient than Ito, Saito and Nishizeki's methodology. Benaloh and Leichter showed that there exist access structures for which any secret sharing scheme must give to some participant a share which is from a domain strictly larger than that of the secret.

Brickell and Davenport [12] analyzed ideal secret sharing schemes in terms of matroids. An ideal secret sharing scheme is a scheme for which the shares are taken from a set that has the same

*Partially supported by Italian Ministry of University and Research (M.U.R.S.T.) and by National Council for Research (C.N.R.) under grant 91.02326.CT12.

size of the set where the secret is chosen. In particular, in case the access structure consists of only those subsets of participants containing an edge of a given graph $G$, Brickell and Davenport [12] proved that an ideal secret sharing scheme exists if and only if $G$ is a complete multipartite graph. Equivalently, if we define the information rate of an access structure as the ratio between the size of the secret and that of the largest share given to any participant, Brickell and Davenport's result can be stated saying that a graph has information rate 1 if and only if it is a complete multipartite graph.

The problem of establishing bounds on the size of the shares to be given to participants in secret sharing schemes, or equivalently on the information rate, is one of the basic problem in the area and has received considerable attention by several researchers. The practical relevance of this issue is based on the following observations: Firstly, the security of any system tends to degrade as the amount of information that must be kept secret, i.e., the shares of the participants, increases. Secondly, if the shares given to participants are too long, the memory requirements for the participants will be too severe and, at the same time, the shares distribution algorithms will become inefficient. Therefore, it is important to derive significative upper and lower bounds on the information rate for classes of access structures.

Brickell and Stinson [14] gave several upper and lower bounds on the information rate of access structures based on graphs. Stinson in [41] presented new lower bounds on general access structures. Capocelli, De Santis, Gargano, and Vaccaro [15] gave the first example of access structures with information rate bounded away from 1.

Blundo, De Santis, Stinson, and Vaccaro [9] analyzed the information rate and the average information rate of secret sharing schemes based on graphs. The average information rate is the ratio between the secret size and the arithmetic mean of the size of the shares for such schemes. They proved the existence of a gap in the values of information rates of graphs, more precisely they strengthened the above quoted result of Brickell and Davenport [12], proving that if a graph $G$ with $n$ vertices is not a complete multipartite graph then any secret sharing scheme for it has information rate not greater than $2/3$ and average information rate not greater than $n/(n+1)$. These upper bounds arise by applying entropy argument due to Capocelli, De Santis, Gargano, and Vaccaro [15].

A discussion of the best bounds known so far and of our improvements is presented in the technical sections of the paper.

The recent survey by Stinson [40] contains an unified description of recent results in the area of secret sharing schemes. For different approaches to the study of secret sharing schemes, for schemes with "extended capabilities" as disenrollment, fault-tolerance, and pre-positioning and for a complete bibliography we recommend the survey article by Simmons [39].

We also mention some "extended capabilities" of secret sharing schemes that have been studied. In [1] and [8] has been addressed the problem of designing secret sharing schemes having the additional feature that qualified minorities can forbid any other set of participants from reconstructing the secret. These schemes are referred to as secret sharing schemes with "veto" capability. Ingemarsson and Simmons [24] solve the question of how to set up a secret sharing scheme in the absence of a trusted party. Prepositioned schemes are studied in [38]. The idea of protecting against cheating by one or more participants is addressed in [30, 43, 35, 37, 13, 16]. In [4] the authors investigated threshold schemes that permit disenrollment of participants. Secret sharing schemes in which the dealer has the feature of being able (after a preprocessing stage) to activate a particular access structure out of a given set and/or to allow the participants to reconstruct different secrets (in different time instants) by sending to all participants the same broadcast message have been analyzed in [6]. Schemes for sharing several non-independent secrets simultaneously have been analyzed in [10]; whereas, schemes where different secrets are associated with different