Optimal Non-Perfect Uniform Secret Sharing Schemes *

Oriol Farràs [1], Torben Hansen [2], Tarik Kaced [3], and Carles Padró [4]

[1]Universitat Rovira i Virgili, Tarragona, Catalonia, Spain
[2]Aarhus University, Aarhus, Denmark
[3]The Chinese University of Hong Kong, Hong Kong
[4]Nanyang Technological University, Singapore

February 17, 2014

Abstract

A secret sharing scheme is non-perfect if some subsets of participants cannot recover the secret value but have some information about it. This work is dedicated to the search of efficient non-perfect secret sharing schemes. The efficiency is measured by means of the information ratio, the ratio between the maximum length of the shares and the length of the secret value.

In order to study perfect and non-perfect secret sharing schemes with all generality, we describe the structure of the schemes through their access function, a real function that measures the amount of information that every subset of participants knows about the secret value. We present new tools for the construction of secret sharing schemes. In particular, we construct a secret sharing scheme for every access function.

We extend the connections between polymatroids and perfect secret sharing schemes to the non-perfect ones to find new results on the information ratio. We find a new lower bound on the information ratio that is better than the ones previously known. In particular, this bound is tight for uniform access functions. The access function of a secret sharing scheme is uniform if all participants play the same role in a scheme (e.g. ramp secret sharing schemes). Moreover, we construct a secret sharing scheme with optimal information ratio for every rational uniform access function.

Key words. Secret sharing, Non-perfect secret sharing scheme, Information Ratio, Polymatroid

1 Introduction

A *secret sharing scheme* is a method to protect a secret value by distributing it into *shares* among a set of participants in order to prevent the disclosure of the secret. *Authorized* subsets are those subsets of participants that can fully recover the secret, while *forbidden* subsets are

*Part of the material in this paper has been submitted for publication. Oriol Farràs is supported by the European Comission under FP7 project "Inter-Trust", by the Spanish Government through projects TIN2011C27076-C03-01 "Co-Privacy" and Consolider Ingenio 695 2010 CSD2007-00004 "ARES", and by the Government of Catalonia under Grant 2009 SGR 1135. email: oriol.farras@urv.cat. Tarik Kaced is supported by a grant from University Grants Committee of the Hong Kong S.A.R. (Project No. AoE/E-02/08). email:tarik@inc.cuhk.edu.hk. Carles Padró is supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03. email: CarlesPL@ntu.edu.sg.

those that cannot obtain any information about the secret in the information theoretic sense. A secret sharing scheme is said to be *perfect* whenever non-authorized subsets are forbidden, and *non-perfect* if some subsets are neither authorized nor forbidden.

Secret sharing was introduced by Shamir [30] and Blakley [4] in 1979. Namely, they presented threshold secret sharing schemes. These schemes are perfect and have a fundamental role in several areas of cryptography such as secure multiparty computation and distributed cryptography. Blakley and Meadows [5] presented the ramp secret sharing schemes, the first non-perfect secret sharing schemes. The structure of these schemes can be described by means of two thresholds t and r. The subsets of size smaller or equal than t cannot obtain any information about the secret, while the ones of size greater or equal than r can recover the secret. The subsets of size k with $t < k < r$ have a certain amount of information of the secret that is proportional to $(k-t)/(r-t)$. Ramp schemes, as well as other non-perfect secret sharing schemes, have also been used for building efficient secure multiparty computation protocols [8]. Both threshold and ramp secret sharing schemes are *uniform*, because the role of all participants in the scheme is the same.

It is common to describe the structure of perfect secret sharing schemes by their *access structure*, the family of authorized subsets. For non-perfect schemes, there is currently not a standard way to describe it [13, 16, 21, 25, 28], it depends on the amount of detail that is needed. Most of them classify the subsets into different families, according to the amount of information they know about the secret. Ishai, Kushilevitz, and Strulovich [16] introduced the fractional access structures, monotone functions whose image is $\{1, \ldots, m\}$ that measure the amount of information known about the secret.

In this work we consider more general monotone functions that record the fraction of information known about the secret for any subset. An *access function* on a set of participants P is a monotone increasing function whose range is $[0, 1]$. The access function of a secret sharing scheme is a (real-valued) function which tells, for every subset, the amount of information known about the secret. The image of forbidden subsets is 0, while the image of authorized subsets is 1. Hence, the access function of perfect secret sharing schemes is a Boolean function. This definition encapsulates the previous attemps at defining the structure of non-perfect access structures. As customary with a new structure definition, the following question arises:

Question 1.1. Is every access function realizable?

We answer this question in the affirmative. This result is not entirely obvious since the usual approach of using linear schemes cannot work. Indeed, there are only countably many linear secret sharing schemes, while there are uncountably many access functions. Therefore, some access functions are inherently non-linear or might only be realized in the limit by a sequence of linear schemes.

The second natural question is related to the efficiency of schemes. In this work we measure the efficiency by means of the *information ratio*, the ratio between the entropy of the largest share and the entropy of the secret. The *optimal information ratio* of an access function F is the infimum of the information ratio of all the secret sharing schemes for F.

Question 1.2. What is the optimal information ratio of an access function?

This problem is wide open, even for perfect secret sharing schemes, and is one of the most important problems in secret sharing. A related open problem is the construction of optimal secret sharing schemes. For perfect secret sharing the length of every share is at least the length of the secret. However, for non-perfect secret sharing schemes the length of the shares can be smaller. We provide new tools by means of which we solve these open problems for some families of access functions.

The third main question we consider is related to secret sharing schemes with uniform rational access functions. These schemes were studied in [16], and some constructions were presented. Moreover, the following open problem is stated:

Question 1.3. For which uniform rational access functions do there exist a secret sharing scheme with information ratio equal to one?

We solve this problem, by showing that every uniform rational access function has this property. Furthermore, for every one of these access functions we compute their optimal information ratio and we provide an explicit linear secret sharing scheme whose information ratio attains this value.

1.1 Related Work

Several works investigated non-perfect schemes through different angles. Blakley and Meadows [5] presented the ramp secret sharing schemes, the first non-perfect secret sharing schemes, and some subsequent works analyzed this particular family of uniform schemes. Kurosawa, Ogata, and Tsujii [25] were the first that considered the problem of the optimization of non-perfect secret sharing schemes for general access functions. Matroids play a fundamental role in the characterization of ideal perfect secret sharing schemes. Some works extended this connection to the non-perfect case in order to find equivalent results [13, 21, 28]. In this work we extend the connection the connection between polymatroids and perfect secret sharing schemes [11] to the non-perfect ones.

Ishai, Kushilevitz, and Strulovich [16] introduced the notion of fractional access structures, and found a connection between non-perfect secret sharing schemes and Markov chains. They constructed secret sharing schemes for every rational access function. The properties of non-perfect secret sharing schemes in which the size of the secret is small have been studied in [7]. Due to the use of secret sharing in secure multiparty computation, some works (e.g. [8]) studied the use of non-perfect secret sharing schemes for building efficient protocols.

Non-perfect secret sharing schemes can be seen as entropic points. That is, points defined by the list of entropies of all the possible subsets. In the case of uniform functions, Chen and Yeung studied in [9] similar concepts. They proved that only Shannon-type information inequalities are needed in this setting. We confirm and give another proof of their result using other methods. The entropy method is the most used tool in order to get bounds for the information ratio of perfect schemes, see e.g. [11]. This method can also be used for non-perfect schemes (see [19]).

1.2 Our Results

We provide a new general framework for the study of secret sharing schemes. Our framework covers the previous results on perfect and non-perfect secret sharing schemes, and allows the generalization of fundamental results on the efficiency of perfect secret sharing schemes to the non-perfect ones. We describe the structure of a secret sharing schemes by means of its access function. In Theorem 3.1 we answer Question 1.1 by constructing a secret sharing scheme for every access function. This strongly motivates the use of access functions for describing the structure of secret sharing schemes.

We extend the connection between polymatroids and perfect secret sharing schemes to non-perfect secret sharing schemes. This connection is very important, not only from the theoretical point of view. Based on this connection, we study Question 1.2 and we provide a new lower bound on the optimal information ratio, that is better that previously known bounds. For rational uniform access functions we show in Theorem 7.4 that this bound is tight.

Moreover, Theorem 7.4 also answers Question 1.3. For every rational uniform access function we compute the optimal information ratio and we construct an optimal linear secret sharing scheme for it. Theorem 7.4 provides interesting corollaries on the nature of the uniform secrt sharing schemes. The proof of the theorem uses new general tools for convex combinations of access functions (Proposition 3.2)

For non-rational access functions we also provide tools for the construction of secret sharing schemes and results on their optimal information ratio. Among them, explicit constructions of secret sharing schemes and (asymptotically) optimal secret sharing schemes for any uniform access functions. We further discuss the size of the secret and the linearity of the resulting schemes.

2 Secret Sharing Schemes

In this work we consider a definition of secret sharing schemes that is based on information theory. For a complete introduction to secret sharing, see [1, 26], and for a textbook on information theory see [10]. We begin by introducing some notation. For a finite set Q, we use $\mathcal{P}(Q)$ to denote its *power set*, that is, the set of all subsets of Q. We use a compact notation for set unions, that is, we write XY for $X \cup Y$ and Xy for $X \cup \{y\}$. In addition, we write $X - Y$ for the set difference and $X - x$ for $X - \{x\}$. Let $X = \{1, \ldots, t\}$ be a set and let $(S_i)_{i \in X}$ be a tuple of discrete random variables. We write S_X for the random variable $S_1 \times \cdots \times S_t$, and $H(S_X)$ for its Shannon entropy. All through the paper, P and Q stand for finite sets with $Q = Pp_o$ for some $p_o \notin P$.

Definition 2.1. Let Q be a finite set of *participants*, let $p_o \in Q$ be a distinguished participant, which is called *dealer*, and take $P = Q - p_o$. A *secret sharing scheme* Σ on the set P is a collection $(S_i)_{i \in Q}$ of discrete random variables such that

- $H(S_{p_o}) > 0$, and
- $H(S_{p_o}|S_P) = 0$.

The random variable S_{p_o} corresponds to the *secret*, and $(S_i)_{i \in P}$ correspond to the *shares* of the secret that are distributed among the participants in P.

Definition 2.2. An *access function* on a set P is a monotone increasing function

$$F : \mathcal{P}(P) \to [0, 1]$$

with $F(\emptyset) = 0$ and $F(P) = 1$. Here, monotone increasing means that $F(X) \leq F(Y)$ if $X \subseteq Y$. An access function is said to be *perfect* if its only values are 0 and 1.

Definition 2.3. The *access function F of a secret sharing scheme* $\Sigma = (S_i)_{i \in Q}$ is defined by

$$F(X) = \frac{I(S_{p_o}{:}S_X)}{H(S_{p_o})},$$

where $I(S_{p_o}{:}S_X)$ denotes the mutual information between these random variables.

A subset $X \subseteq P$ is *authorized* if $F(X) = 1$, and it is *forbidden* if $F(X) = 0$. Observe that P is always an authorized subset, and the empty set is always forbidden. A secret sharing scheme is *perfect* if its access function is perfect. In this case, every set of participants is either authorized or forbidden. For every access function F we define its *gap* as

$$g(F) = \min\{|B - A| \,:\, F(A) = 0, F(B) = 1\}.$$

The gap of a perfect access function is one, but this is not a sufficient condition for an access function to be perfect.

Definition 2.4. Given integers t, r with $0 \leq t < r \leq |P|$, the (t, r)-*ramp access function* on P is defined by: $F(X) = 0$ if $|X| \leq t$, and $F(X) = (|X| - t)/(r - t)$ if $t < |X| < r$, and $F(X) = 1$ if $|X| \geq r$. The gap of this access function is $g = r - t$. If $t = r - 1$, the ramp access function is perfect, and it corresponds to a threshold access structure.

Example 2.5. A variant of Shamir's [30] threshold scheme provides a secret sharing scheme for every ramp access function. This construction was first presented in the seminal work on non-perfect secret sharing by Blakley and Meadows [5]. Consider the (t, r)-ramp access function on the set $P = \{1, \ldots, n\}$. Let $\mathbb{K}$ be a finite field of size $|\mathbb{K}| \geq n + g$, where $g = r - t$, and take $n+g$ different elements $y_1, \ldots, y_g, x_1, \ldots, x_n \in \mathbb{K}$. By choosing uniformly at random a polynomial $f \in \mathbb{K}[X]$ with degree at most $r - 1$, one obtains random variables $S_{p_o} = (f(y_1), \ldots, f(y_g)) \in \mathbb{K}^g$ and $S_i = f(x_i) \in \mathbb{K}$ for every $i \in P$. It is not difficult to check that these random variables define a secret sharing scheme for the (t, r)-ramp access function on P.

We use the Shannon entropy as an approximation of the shortest binary codification. The *information ratio* $\sigma(\Sigma)$ of a secret sharing $\Sigma = (S_i)_{i \in Q}$ is the ratio between the maximum length of the shares and the length of the secret value, that is,

$$\sigma(\Sigma) = \frac{\max_{p \in P} H(S_p)}{H(S_{p_o})}.$$

The *optimal information ratio* $\sigma(F)$ *of an access function* F is defined as the infimum of the information ratio of the secret sharing schemes for F. A secret sharing scheme attaining $\sigma(F)$ is called *optimal*. The optimal information ratio of every perfect access function is at least 1. In general, $\sigma(F) \geq 1/g(F)$ [13, 25].

Let $\mathbb{K}$ be a finite field. In a $\mathbb{K}$-*linear* (or simply *linear*) secret sharing scheme, the random variables $(S_i)_{i \in Q}$ are given by surjective $\mathbb{K}$-linear maps $S_i : E \to E_i$, where the uniform probability distribution is taken on E. Observe that, for every $X \subseteq Q$, the random variable S_X is uniform on its support. Because of that, $H(S_X) = \operatorname{rank} S_X \cdot \log |\mathbb{K}|$, and hence $I(S_{p_o}{:}S_X) = (\operatorname{rank} S_{p_o} + \operatorname{rank} S_X - \operatorname{rank} S_{Xp_o}) \log |\mathbb{K}|$. This implies that the access function of every linear secret sharing scheme is rational-valued and its information ratio is rational too. For a rational access function F, we define $\lambda(F)$ as the infimum of the information ratios of the linear secret sharing schemes for F. Clearly, $\lambda(F)$ is an upper bound of $\sigma(F)$.

Example 2.6. The secret sharing scheme presented in Example 2.5 is linear. It is optimal because its information ratio is $1/g$.

3 Construction of Secret Sharing Schemes

It is well known that every perfect access function admits a perfect secret sharing scheme [3, 17]. In Theorem 3.1 we present an extension of this result to the general case. We also show in Proposition 3.2 a method to construct non-perfect secret sharing schemes.

Theorem 3.1. *Every access function admits a secret sharing scheme.*

Proof. Let F be an access function on the set of participants P. Define k to be a large enough integer such that: for every $A, B \subseteq P$, if $kF(A) \neq kF(B)$ then $\lceil kF(A) \rceil \neq \lceil kF(B) \rceil$. We construct a secret sharing scheme $\Sigma = (S_i)_{i \in Q}$ for F with $S_{p_o} = S^1 \times \cdots \times S^k$, where all

S^i are independent and have entropy one. If $kF(A)$ is not an integer, let $i = \lceil kF(A) \rceil$ and $\epsilon_A = i - kF(A)$. In this case we define $S^i = S_0^i \times S_1^i$, where S_0^i and S_1^i are independent binary random variables with $\Pr[S_0^i = 0] = h^{-1}(\epsilon_A)$ and $\Pr[S_1^i = 0] = h^{-1}(1 - \epsilon_A)$, where h is the binary entropy function. This is always possible since $\epsilon_A \in (0, 1)$. By definition of k, all S^i are well-defined and we have

$$H(S_0^i) = 1 - H(S_1^i) = \epsilon_A;$$

for all other indices i, S^i is a uniformly random bit.

In order to describe S_i for $i \in P$, we define a family of secret sharing schemes. For every $A \subseteq P$, we define a secret sharing scheme $\Sigma_A = (S_{i,A})_{i \in Q}$ with access function F_A satisfying $F_A(B) = 1$ if $A \subseteq B$ and $F(B) = 0$ else. Observe that participants not in A are irrelevant in Σ_A. These schemes are ideal and perfect, and are well known [17]. Let A' be a proper subset of A satisfying that $F(A') \geq F(B)$ for every $B \subsetneq A$. If $kF(A)$ is an integer, then we define

$$S_{p_o,A} = S^p \times \cdots \times S^q, \text{ with } p = \lceil 1 + kF(A') \rceil \text{ and } q = \lfloor kF(A) \rfloor.$$

If $kF(A')$ is non-integer we add the extra S_1^{p-1}, and if $kF(A)$ is non-integer we add S_0^{q+1}.

Then we define $S_i = (S_{i,A})_{A \subseteq P}$ for every $i \in P$. Observe that $I(S_{p_o}{:}S_{A,B}) = 0$ for every $A \subsetneq B \subseteq P$, and so $I(S_{p_o}{:}S_A) = I(S_{p_o}{:}S_{A,A}) + I(S_{p_o}{:}S_{A,A'}) = H(S_{p_o,A}) + kF(A') = kF(A)$ for every $A \subseteq P$. □

If all the values of an access function are rational, then for a large enough k the construction presented above is a linear secret sharing scheme. If the access function is not rational, then the resulting scheme is not linear. The above construction can be very inefficient: In the worst case the information ratio is exponential in the number of participants. It is not difficult to see that the proof can be modified to construct a (possibly non-linear) scheme for any large enough secret size.

For any two access functions F_0 and F_1 on the same set and for any $\rho \in [0, 1]$, we define the access function $F_\rho = \rho F_1 + (1 - \rho)F_0$. Next we study the construction of secret sharing schemes for F_ρ from secret sharing schemes for F_0 and F_1. The results can be naturally extended to any finite convex combination of access functions.

Proposition 3.2. *For $i = 0, 1$ let F_i be an access function on P that admits a secret sharing scheme $\Sigma_i = (S_{ij})_{j \in Q}$ with information ratio σ_i. Let $r = H(S_{0p_o})/H(S_{1p_o})$ and let $\rho = [1 + \frac{q_0}{q_1} r]^{-1}$, where q_0, q_1 are positive integers. Then F_ρ admits a secret sharing scheme with information ratio at most σ. If Σ_0 and Σ_1 are $\mathbb{K}$-linear for a finite field $\mathbb{K}$, then F_ρ admits a $\mathbb{K}$-linear secret sharing scheme with information ratio at most σ.*

Proof. Let q_0, q_1 be two positive integers satisfying $\rho = [1 + \frac{q_0}{q_1} r]^{-1}$. Consider the secret sharing scheme $\Sigma = (S_j)_{j \in Q}$ defined as the concatenation of q_0 instances of Σ_0 and q_1 instances of Σ_1. That is, $S_j = (S_{0j})^{q_0} \times (S_{1j})^{q_1}$ for $j \in Q$. Then $H(S_{p_o}) = q_0 H(S_{0p_o}) + q_1 H(S_{1p_o})$ and $I(S_{p_o}{:}S_A) = q_0 I(S_{0p_o}{:}S_{0A}) + q_1 I(S_{1p_o}{:}S_{1A})$ for every $A \subseteq P$. Hence the access function of Σ is F and

$$\sigma(\Sigma) \leq \frac{q_1 \sigma_1 H(S_{1p_o}) + q_0 \sigma_0 H(S_{0p_o})}{q_1 H(S_{1p_o}) + q_0 H(S_{0p_o})} = \rho\sigma_1 + (1 - \rho)\sigma_0.$$

□

Remark 3.3. If there is a participant in P that holds the largest share in both Σ_0 and Σ_1, then the information ratio of the scheme we construct in the proof is $\rho\sigma(\Sigma_1) + (1 - \rho)\sigma(\Sigma_0)$.

The next result is a corollary of Theorem 3.1 and Proposition 3.2. The proof is moved to the appendix.

Corollary 3.4. *For $i = 0, 1$ let F_i be an access function on P that admits a secret sharing scheme $\Sigma_i = (S_{ij})_{j \in Q}$ with information ratio σ_i. Then for any $\rho \in (0, 1)$, and any $\delta > 0$, there exists a scheme realizing F_ρ whose information ratio is less than $\rho\sigma_1 + (1 - \rho)\sigma_0 + \delta$.*

Proof. Choose λ such that $\rho = \lambda + \epsilon$ and $\rho + m\epsilon \leq 1$, where $\lambda = \left[1 + \frac{q_0 H(S_{0p_o})}{q_1 H(S_{1p_o})}\right]^{-1}$ and q_0, q_1 are integers. Notice that

$$(m + 1)F_\rho = mF_\lambda + F_{\rho+m\epsilon}. \tag{1}$$

Using the previous Proposition, there is a scheme Σ_λ for F_λ with information ratio not greater than $\rho\sigma_1 + (1 - \rho)\sigma_0$. By Theorem 3.1, $F_{\rho+m\epsilon}$ can be realized for any large enough secret, so we choose the secret to be the same as in the scheme Σ_λ and call the resulting scheme $\Sigma_{\rho+m\epsilon}$.

Recalling (1): We implement F_ρ by concatenating m copies of Σ_λ with the scheme for $F_{\rho+m\epsilon}$. The resulting scheme Σ satisfies:

$$\frac{I(S_{p_o}{:}A)}{H(S_{p_o})} = \frac{m}{m+1}F_\lambda(A) + \frac{1}{m+1}F_{\rho+m\epsilon}(A) = F_\rho(A), \text{ and}$$
$$\sigma(\Sigma) \leq \frac{m}{m+1}\sigma(\Sigma_\lambda) + \frac{1}{m+1}\sigma(\Sigma_{\rho+m\epsilon}) \leq \sigma(\Sigma_\lambda) + \mathcal{O}(m^{-1})$$

where the last inequality is valid since by Theorem 3.1, the information ratio of $\Sigma_{\rho+m\epsilon}$ is bounded by a constant depending only on $|P|$. We conclude the proof by noticing that our choice of ϵ implies $\sigma(\Sigma) \leq \rho\sigma_1 + (1 - \rho)\sigma_0 + \mathcal{O}(m^{-1})$. □

The relation between δ and the size of the secret of the scheme in the previous proof depends on the accuracy of the Diophantine approximations of ρ. The construction is asymmetric: the condition $m\epsilon \leq 1$ is slightly easier to achieve when ρ is close to zero.

4 Polymatroids and Secret Sharing

The connection between perfect secret sharing schemes and polymatroids has been used in order to obtain bounds on the information ratio. It is derived from the connection between polymatroids and Shannon entropy that was discovered by Fujishige [14, 15] and is described here in Theorem 4.3. In this section, we present an extension of this connection to non-perfect secret sharing schemes. We use it in the following sections to obtain lower bounds on the information ratio.

For a function $f : \mathcal{P}(Q) \to \mathbb{R}$, a subset $X \subseteq Q$ and $y, z \in Q$, we notate

$$\Delta_f(X; y, z) = f(Xy) + f(Xz) - f(Xyz) - f(X).$$

Definition 4.1. A *polymatroid* is a pair $\mathcal{S} = (Q, f)$ formed by a finite set Q, the *ground set*, and a *rank function* $f\colon \mathcal{P}(Q) \to \mathbb{R}$ satisfying the following properties.

- $f(\emptyset) = 0$.
- f is *monotone increasing*: if $X \subseteq Y \subseteq Q$, then $f(X) \leq f(Y)$.
- f is *submodular*: $f(X \cup Y) + f(X \cap Y) \leq f(X) + f(Y)$ for every $X, Y \subseteq Q$.

The following characterization of rank functions of polymatroids is a straightforward consequence of [29, Theorem 44.1].

Proposition 4.2. *A map $f\colon \mathcal{P}(Q) \to \mathbb{R}$ is the rank function of a polymatroid with ground set Q if and only if $f(\emptyset) = 0$ and $\Delta_f(X; y, z) \geq 0$ for every $X \subseteq Q$ and $y, z \in Q$.*

Theorem 4.3. *If $(S_i)_{i\in Q}$ is a tuple of discrete random variables, then the map $f\colon \mathcal{P}(Q) \to \mathbb{R}$ defined by $f(X) = H(S_X)$ is the rank function of a polymatroid with ground set Q.*

Because of the connection between polymatroids and the Shannon entropy described in the previous theorem, and by analogy to the conditional entropy, we write $f(X|Y) = f(XY) - f(Y)$ for every $X, Y \subseteq Q$. The polymatroid axioms imply that $f(X|Y) \geq 0$ and $f(X|Y) \geq f(X|YZ)$ for every $X, Y, Z \subseteq Q$. In addition,

$$f(X_1 \dots X_r) = \sum_{i=1}^{t} f(X_i|X_1 \dots X_{i-1})$$

for all $X_1, \dots, X_t \subseteq Q$. Moreover, $f(X|YZ) = f(X|Y)$ if $f(Z|Y) = 0$.

As a consequence of Theorem 4.3, every secret sharing scheme determines a polymatroid. For perfect secret sharing schemes, this connection was first used in [11]. This is a useful tool for the study of secret sharing schemes.

Definition 4.4. Let $\Sigma = (S_i)_{i\in Q}$ be a secret sharing scheme on P. Every multiple of the polymatroid (Q, f), where $f(X) = H(S_X)$ for every $X \subseteq Q$, is called a *Σ-polymatroid*.

Definition 4.5. Let F be an access function on P and let $\mathcal{S} = (Q, f)$ be a polymatroid. Then $\mathcal{S}$ is an *F-polymatroid* if

$$F(A) = \frac{f(p_o) - f(p_o|A)}{f(p_o)}$$

for every $A \subseteq P$.

We say that a polymatroid $\mathcal{S} = (Q, f)$ is *normalized* if $f(p_o) = 1$. A polymatroid $\mathcal{S} = (P, f)$ is *compatible* with the access function F if $\mathcal{S}$ can be extended to a normalized F-polymatroid $\mathcal{S}' = (Q, f)$. The following is a generalization of a result by Csirmaz [11, Proposition 2.3] on perfect secret sharing.

Proposition 4.6. *A polymatroid $\mathcal{S} = (P, f)$ is compatible with an access function F on P if and only if $\Delta_f(X; y, z) \geq \Delta_F(X; y, z)$ for every $X \subseteq P$ and $y, z \in P$.*

Proof. Extend the rank function f of $\mathcal{S}$ to $\mathcal{P}(Q)$ by taking $f(Xp_o) = f(X) + 1 - F(X)$ for every $X \subseteq P$. This is the only possible extension of f that can produce a normalized F-polymatroid. Therefore, $\mathcal{S}$ is compatible with F if and only if (Q, f) is a polymatroid. By Proposition 4.2 and taking into account that (P, f) is a polymatroid, (Q, f) is a polymatroid if and only if $\Delta_f(X; y, z) \geq 0$ whenever $p_o \in X$ or $p_o = y$. It is not difficult to check that this is equivalent to the condition in the statement. □

5 Lower Bounds on the Information Ratio

On the basis of the connection between secret sharing and polymatroids, we introduce in this section two parameters, $\kappa(F)$ and $\epsilon(F)$, that provide lower bounds on the optimal information ratio $\sigma(F)$. The first one is a straightforward generalization of the corresponding parameter for perfect secret sharing that was introduced in [22]. The second one is only relevant for non-perfect secret sharing. It makes it possible to generalize a previous results by Csirmaz on the limitation of Shannon inequalities to find lower bounds on the information ratio and, more importantly, to find a tight lower bound on the optimal information ratio of uniform access functions.

For a polymatroid $\mathcal{S} = (Q, f)$ we define

$$\sigma_{p_o}(\mathcal{S}) = \frac{\max_{x \in P} f(x)}{f(p_o)}.$$

If $\mathcal{S}$ is a Σ-polymatroid, then $\sigma(\Sigma) = \sigma_{p_o}(\mathcal{S})$. In addition, we define

$$\kappa(F) = \inf\{\sigma_{p_o}(\mathcal{S}) \,:\, \mathcal{S} \text{ is an } F\text{-polymatroid}\}. \tag{2}$$

Observe that, if Σ is a secret sharing with access function F, then every Σ-polymatroid is an F-polymatroid. Because of that, $\kappa(F) \leq \sigma(F)$. It is not difficult to prove that $\kappa(F) \geq 1/g(F)$ for every access function F [13, 25]. In particular, this implies the well known fact that the information ratio of every perfect secret sharing scheme is at least 1.

The search of $\kappa(F)$ for an access function F can be restricted to the family of the normalized F-polymatroids. The value of $\kappa(F)$, which is a lower bound on $\sigma(F)$, can be computed by means of the linear programming program determined by the Shannon information inequalities and the access function. This approach has been used in several works on perfect secret sharing, as for instance [12]. The infimum in (2) is a minimum and, moreover, $\kappa(F)$ is rational if F is rational-valued.

For an ordering $\tau = (\tau_1, \ldots, \tau_n)$ of the participants in P, we take $A_0^\tau = \emptyset$ and $A_i^\tau = \{\tau_1, \ldots, \tau_i\}$ for every $i = 1, \ldots, n$. For a function $G : \mathcal{P}(P) \to \mathbb{R}$ and for $i = 1, \ldots, n$, consider $\delta_i^\tau(G) = \Delta_G(A_{i-1}^\tau; \tau_i, \tau_n)$. Observe that $\sum_{i=1}^n \delta_i^\tau(G) = G(\tau_n) - G(\emptyset)$.

Definition 5.1. Let F be an access function on P, with $|P| = n$. We define $\epsilon(F)$ as the maximum, among all orderings τ of P, of $\sum_{i=1}^n \max\{0, \delta_i^\tau(F)\}$.

Observe that $\max\{0, \delta_i^\tau(F)\} \leq F(A_i^\tau) - F(A_{i-1}^\tau)$, and hence $\epsilon(F) \leq 1$. Moreover, $\epsilon(F) = 1$ if F is a perfect access function. It is known that $1 \leq \kappa(F) \leq |P|$ for every perfect access function [11, 20]. These bounds on κ are extended to the non-perfect case in Propositions 5.2 and 5.4. In addition, we prove in Proposition 5.3 that $\epsilon(F)$ is in general a better lower bound on $\kappa(F)$ than $1/g(F)$.

Proposition 5.2. *$\kappa(F) \geq \epsilon(F)$ for every access function F.*

Proof. Let F be an access function on a set P with n participants and let (Q, f) be a normalized F-polymatroid. Let τ be an ordering of P such that $\epsilon(F) = \sum_{i=1}^n \max\{0, \delta_i^\tau(F)\}$ and take $x = \tau_n$. By Propositions 4.2 and 4.6, $f(x) = \sum_{i=1}^n \delta_i^\tau(f) \geq \sum_{i=1}^n \max\{0, \delta_i^\tau(F)\} = \epsilon(F)$. □

Proposition 5.3. *Let F be an access function on P. Then $\epsilon(F) \geq F(Xy) - F(X)$ for every $X \subseteq P$ and $y \in P - X$. As a consequence, $\epsilon(F) \geq 1/g(F)$.*

Proof. Take $\ell = |X|$ and $n = |P|$ and consider an ordering τ of P such that $A_\ell^\tau = X$ and $\tau_n = y$. Then

$$\epsilon(F) \geq \sum_{i=1}^{n} \max\{0, \delta_i^\tau(F)\} \geq \sum_{i=\ell+1}^{n} \delta_i^\tau(F) = F(Xy) - F(X).$$

Finally, it is clear that there exist $X \subseteq P$ and $y \in P$ such that $F(Xy) \geq F(X) + 1/g(F)$. □

Proposition 5.4. *Let F be an access function on a set of n participants. Then $\kappa(F) \leq n\epsilon(F)$.*

Proof. We prove it constructively by showing that there exists an F-polymatroid $\mathcal{S}$ with $\sigma_{p_o}(\mathcal{S}) = n\epsilon(F)$. Consider the polymatroid (P, f) with $f(X) = \epsilon(F) \sum_{i=1}^{|X|}(n - i + 1)$ for every nonempty set X. Then $\Delta_f(X; y, z) = \epsilon(F) \geq \Delta_F(X; y, z)$ for every $X \subseteq P$ and $y, z \in P$ with $y, z \notin X$. Therefore, by Proposition 4.6, the polymatroid (P, f) is compatible with the access function F. □

6 Duality and Minors

Duality and minors are operations that play a fundamental role in the study of secret sharing, matroids and polymatroids. The dual and the minors of perfect access functions have been studied in many works (see for instance [22]). In this section we study these operations for general access functions. The proofs of the results have been moved to the Appendix.

Let F be an access function on a set P. For any $B \subseteq P$, we consider on the set $P - B$ the access functions $F \setminus B$ and F/B defined by $(F \setminus B)(A) = F(A)$ and $(F/B)(A) = F(A \cup B)$. These operations are called *deletion* and *contraction*, respectively. Any access function obtained by a sequence of deletions and contractions of subsets of P is a *minor* of F. Minors of access functions correspond to natural scenarios. Namely, if several participants leave the scheme and maybe some of them reveal their shares, then the new access function will be a minor of the original one.

The *dual* F^* of an access function F on P is the access function on P defined by $F^*(A) = 1 - F(P - A)$. Obviously, $F^{**} = F$. Moreover, it is not difficult to check that $(F/B)^* = F^* \setminus B$ and $(F \setminus B)^* = F^*/B$.

For a polymatroid $\mathcal{S} = (Q, h)$ and a subset $B \subseteq Q$, we consider the polymatroids $\mathcal{S} \setminus B = (Q - B, h_{\setminus B})$ and $\mathcal{S}/B = (Q - B, h_{/B})$ with $h_{\setminus B}(X) = h(X)$ and $h_{/B}(X) = h(X \cup B) - h(B)$ for every $X \subseteq Q \setminus B$. Every polymatroid that is obtained from $\mathcal{S}$ by a sequence of such operations is a *minor* of $\mathcal{S}$. If $\mathcal{S}$ is a F-polymatroid and $B \subseteq P$, then $\mathcal{S} \setminus B$ is a $(F \setminus B)$-polymatroid and $\mathcal{S}/B$ is a (F/B)-polymatroid. Thus $\kappa(F') \leq \kappa(F)$ for every minor F' of F. In addition, the aforementioned connection between minors and secret sharing implies that $\sigma(F') \leq \sigma(F)$ and $\lambda(F') \leq \lambda(F)$.

Example 6.1. Let F be the (t, r)-ramp access function on a set P of size n. Then F^* is the $(n - r, n - t)$-ramp access function on P. Suppose that $1 < t < r < n$ and take $p \in P$. Then $F \setminus \{p\}$ and $F/\{p\}$, are ramp access functions on $P - p$ with parameters (t, r) and $(t - 1, r - 1)$, respectively.

Proposition 6.2. *For every access function F, $\epsilon(F) = \epsilon(F^*)$.*

Proof. Let F be an access function on a set P of size n and let τ be an ordering of P with $\epsilon(F) = \sum_{i=1}^{n} \max\{0, \delta_i^\tau(F)\}$. Consider the ordering $\tau^* = (\tau_{n-1}, \ldots, \tau_1, \tau_n)$ of P. Clearly,

$$\delta_i^\tau(F) = -\delta_{n-i}^{\tau^*}(F^*)$$

for all $i = 1, \ldots, n-1$. Let $I \subseteq \{1, \ldots, n-1\}$ be the set of indices i with $\delta_i^\tau(F) > 0$. Then

$$\epsilon(F) = \delta_n^\tau(F) + \sum_{i \in I} \delta_i^\tau(F) = F^*(\tau_n^*) - \sum_{i \in I} \delta_{n-i}^{\tau^*}(F^*).$$

Since $\sum_{i=1}^{n} \delta_i^{\tau^*}(F^*) = F^*(\tau_n^*)$,

$$\epsilon(F) = \sum_{i=1}^{n} \max\{0, \delta_i^{\tau^*}(F^*)\} \leq \epsilon(F^*).$$

Finally, $\epsilon(F) \geq \epsilon(F^*)$ because $F^{**} = F$. □

In the perfect case, the parameters λ and κ are invariant by duality, as it was proved in [18] and [22], respectively. We extend the result on κ and λ to the non-perfect case. The relation between $\sigma(F)$ and $\sigma(F^*)$ is an open problem, even in the perfect case. Similarly to the perfect case, the proof of Proposition 6.3 is based on duality in polymatroids. The reader is addressed to [29, Chapter 44.6f] or [22] for more information on this topic.

Proposition 6.3. *For every access function F, $\kappa(F) = \kappa(F^*)$.*

Proof. Let F be an access function on P and let $\mathcal{S} = (Q, f)$ be a normalized F-polymatroid. We will show that there is a normalized F^*-polymatroid $\mathcal{S}^*$ with $\sigma_{p_o}(\mathcal{S}^*) \leq \sigma_{p_o}(\mathcal{S})$. Indeed, consider the dual polymatroid $\mathcal{S}^* = (Q, f^*)$ defined by

$$f^*(X) = f(Q - X) - f(Q) + \sum_{x \in X} f(x)$$

for every $X \subseteq Q$. Since $f(Q) = f(P)$, we have that $f^*(\{p_o\}) = f(\{p_o\}) = 1$. For every $X \subseteq P$,

$$1 - f^*(p_o|X) = 1 - f^*(Xp_o) + f^*(X) = f(p_o|P - X) = 1 - F(P - X) = F^*(X),$$

and hence $\mathcal{S}^*$ is an F^*-polymatroid. In addition, $f^*(x) = f(Q - x) - f(Q) + f(x) \leq f(x)$ for every $x \in P$. Therefore, $\sigma_{p_o}(\mathcal{S}^*) \leq \sigma_{p_o}(\mathcal{S})$. □

Proposition 6.4. *For every rational access function F, $\lambda(F) = \lambda(F^*)$.*

Sketch of the proof. Let $\Sigma = (S_i)_{i \in Q}$ be a $\mathbb{K}$-linear secret sharing scheme with access function F. One can construct a $\mathbb{K}$-linear code C from Σ. The generator matrix of this code is obtained by concatenating the matrices of the linear maps S_i, and every codeword is a concatenation of vectors that correspond to the secret value and to the shares. Similarly to the perfect case, one can prove that the dual code $C^\perp$ defines a $\mathbb{K}$-linear secret sharing scheme Σ^* with access function F^* and with the same information ratio as Σ. □

7 Uniform Secret Sharing Schemes

Definition 7.1. An access function F on P is *uniform* if $F(A) = F(B)$ for every $A, B \subseteq P$ with $|A| = |B|$. *Uniform* secret sharing schemes are those with uniform access function.

Uniform access functions are a generalization of the threshold ones, because the perfect uniform access functions are the threshold ones. In Lemma 7.3 we compute the ϵ bound for uniform access functions, and in Theorem 7.4 we construct linear secret sharing schemes whose information ratio attain this bound. We dedicate the rest of the section to the consequences of this theorem.

Let P be a set with $|P| = n$ and let F be a uniform access function on P. For $i = 1, \ldots, n$ we define $r_i = F(A)$, where $A \subseteq P$ and $|A| = i$. Observe that $0 = r_0 \leq r_1 \leq \ldots \leq r_n = 1$. Define $r'_i = r_{i+1} - r_i$ for $i = 0, \ldots, n-1$ and $r''_i = r_{i+1} - 2r_i + r_{i-1}$ for $i = 1, \ldots, n-1$. We call r'_i and r''_i the *first* and the *second derivatives* of F at i, respectively.

Example 7.2. Ramp secret sharing schemes are uniform. In a $(t, t+g)$-ramp access function on a set of n participants, $r'_i = 1/g$ if $t \leq i < t+g$ and else $r'_i = 0$. Moreover $r''_t = 1/g$, $r''_{t+g} = -1/g$, and $r''_i = 0$ for $i \neq t, t+g$.

Lemma 7.3. *Let F be a uniform access function on a set P of size n. Then*

$$\epsilon(F) = r'_{n-1} + \sum_{i=1}^{n-1} \max\{0, -r''_i\},$$

where r'_i and r''_i are the first and the second derivatives of F, respectively.

Proof. Let $\tau = (\tau_1, \ldots, \tau_n)$ be an ordering of P. Observe that $\delta^\tau_i(F) = -r''_i$ for $i = 1, \ldots, n-1$ and $\delta^\tau_n(F) = r'_{n-1}$. □

Theorem 7.4. *Let F be a rational uniform access function on a set of participants P. For every finite field $\mathbb{K}$ with $|\mathbb{K}| \geq |P| + g(F)$ it admits a $\mathbb{K}$-linear secret sharing scheme whose information ratio is equal to $\epsilon(F)$.*

Proof. We prove this result by induction on the size of the gap of the access function. Any uniform access function F with $g(F) = 1$ admits a $|\mathbb{K}|$-linear threshold secret sharing scheme Σ. In this case, $\sigma(\Sigma) = 1 = \epsilon(F)$.

Let F be an access function on a set P of size n with $g = g(F) > 1$. Let $\mathbb{K}$ be a finite field of size $n + g$. Let t be the integer for which $r_i = 0$ for $0 \leq i \leq t$ and $r_i = 1$ for $t + g \leq i \leq n$. Let $\ell \in [t, t + g - 1]$ be the smallest integer satisfying $r'_\ell = \min\{r'_i : t \leq i < t + g\}$. Let F_1 be the $(t, t + g)$-ramp access function on n participants and $\rho = g \cdot r'_\ell$. If $\rho = 1$, then $F = F_1$ and the proof is completed because F it admits a $\mathbb{K}$-linear secret sharing scheme with information ratio $\epsilon(F) = 1/g$.

Suppose that $\rho < 1$. Let F_2 be a rational uniform access function defined by $F_2(A) = s_{|A|}$, where $s_i = 0$ for $0 \leq i \leq t$, $s_i = 1$ for $i \geq t + g$, and

$$s_i = \frac{1}{1-\rho}\left(r_i - \rho\frac{i-t}{g}\right)$$

for $t < i < t + g$. Let $s'_i = s_{i+1} - s_i$ for $i = 0, \ldots, n-1$ and $s''_i = s_{i+1} - 2s_i + s_{i-1}$ for $i = 1, \ldots, n-1$. Observe that $F = \rho F_1 + (1-\rho)F_2$.

Now we compute $\epsilon(F)$. Taking into account Example 7.2 it is direct to see that $r'_i = 0 + (1-\rho)s'_i = 0$ for $0 \leq i < t$ and $t + g \leq i < n$, and $r'_i = r'_\ell + (1-\rho)s'_j$ for $t \leq i < t + g$. Hence $r''_i = r'_i - r'_{i-1} = (1-\rho)(s'_i - s'_{i-1}) = (1-\rho)s''_j$ for every $0 \leq i < n$, $i \neq t, t + g$. Moreover $r''_t = r'_\ell + (1-\rho)s''_t > 0$ because both summands are positive, $r''_{t+g} = -r'_\ell + (1-\rho)s''_{t+g} < 0$ if $t + g < n$, and $r'_{n-1} = -r'_\ell + (1-\rho)s'_{n-1}$ if $t + g = n$. It is straightforward to see that $\epsilon(F) = \rho\epsilon(F_1) + (1-\rho)\epsilon(F_2)$.

The access function F_1 admits a $(t, t + g)$-ramp secret sharing scheme with information ratio $\epsilon(F_1) = 1/g$. Next we show that there is a $\mathbb{K}$-linear secret sharing scheme for F_2 with information ratio equals to $\epsilon(F_2)$. The proof is concluded because of Proposition 3.2 and Remark 3.3.

Since $s'_\ell = 0$, if $\ell = t$ or $\ell = t + g - 1$ then $g(F_2) < g$ and so we can apply the induction hypothesis. Suppose that $t < \ell < t + g - 1$. Let F_3 and F_4 be two uniform access functions on P with $F_3(A) = \min\{s_{|A|}/s_\ell, 1\}$ and $F_4(A) = \max\{(s_{|A|} - s_\ell)/(1 - s_\ell), 0\}$ for every $A \subseteq P$. Then $\epsilon(F_2) = s'_{n-1} + \sum_{i=\ell+1}^{n-1} \max\{0, -s''_i\} + \sum_{i=1}^{\ell} \max\{0, -s''_i\} = (1 - s_\ell)\epsilon(F_4) + s_\ell\epsilon(F_3)$. Since both F_3 and F_4 have gap smaller than g, by the induction hypothesis there exist two $\mathbb{K}$-linear secret sharing schemes with access function F_3 and F_4 and information ratio $\epsilon(F_3)$ and $\epsilon(F_4)$, respectively. By Proposition 3.2 and Remark 3.3 there is a $\mathbb{K}$-linear secret sharing scheme for F_2 with information ratio $\epsilon(F_2)$. □

The rest of this section is dedicated to the results that derive from Theorem 7.4. The next corollary presents an alternative construction whose information rate is higher, but it uses threshold secret sharing schemes instead of ramp secret sharing schemes. It is related to the one presented in [16].

Corollary 7.5. *Every rational uniform access function admits a linear secret sharing scheme with information ratio one made of threshold secret sharing schemes.*

Proof. Let F be a uniform access function on a set of n participants P. For $i = 0, \ldots, n-1$, let F_i be the access function of a $i + 1$-threshold secret sharing scheme on P defined over a finite field $\mathbb{K}$ with $|\mathbb{K}| > n$. Then observe that $F = \sum_{i=0}^{n-1} r'_i F_i$. Since $\sigma(F_i) = 1$ and $\sum_{i=0}^{n-1} r'_i = 1$, using Proposition 3.2 and Remark 3.3 we obtain a $\mathbb{K}$-linear secret sharing scheme with access function F and information ratio 1. □

Corollary 7.6. *For every rational uniform access function F, $\kappa(F) = \sigma(F) = \lambda(F) = \epsilon(F)$.*

Proof. On the one hand $\epsilon(F) \leq \kappa(F)$ by Theorem 5.2 and Lemma 7.3. On the other hand, $\lambda(F) \leq \epsilon(F)$ by Theorem 7.4. □

Corollary 7.7. *For every rational access function there is an optimal secret sharing scheme whose associated polymatroid is a convex combination of ramp polymatroids.*

Proof. Let F be a rational access function on P and let Σ be the optimal secret sharing scheme constructed in the proof of Theorem 7.4. Let $\mathcal{S}$ be the polymatroid associated to Σ, and let $\mathcal{S}_{tr}$ the polymatroid associated to the (t, r)-polymatroid on P. It is direct to see that $\mathcal{S}$ is a linear combination of the polymatroids $\mathcal{S}_{tr}$ with $1 \leq t < r \leq n$. □

The fact that $\kappa(F) = \sigma(F) = \lambda(F)$ for a rational uniform access function F, proved in Corollary 7.6, can also be derived from [9]. The result was obtained independently by means of different techniques. However, the computation of the explicit optimal information ratio, and the construction of the optimal scheme was an open problem. As a direct consequence of Theorem 7.4 and Proposition 6.2, the optimal information ratio of a rational uniform access function is the same as the optimal information ratio of its dual and its minors.

The results presented in Theorem 7.4 and the consequent corollaries deal with rational access functions. For some non-rational access functions, we can also apply the techniques used in the proof of Theorem 7.4 and construct optimal schemes (see Example 7.8). Nevertheless, in general we do not have a method to construct an optimal scheme for every non-rational access function. For every non-rational access function F on a set P, there is a sequence of rational access functions $(F_i)_{i\in\mathbb{N}}$ satisfying that $\lim_{i\to\infty} \sum_{A\subseteq P} |F(A) - F_i(A)| \to 0$. Since $\lim_{i\to\infty} \epsilon(F_i) \to \epsilon(F)$ and $\epsilon(F_i) = \sigma(F_i)$, there is a sequence of linear secret sharing schemes $(\Sigma_i)_{i\in\mathbb{N}}$ satisfying $F(\Sigma_i) \to F$ and $\sigma(\Sigma_i) \to \epsilon(F)$.

Example 7.8. Let F be a uniform access function on a set P of size 3 with $r_0 = r_1 = 0$, $r_2 = \log 5/(2\log 5 + \log 7)$, and $r_3 = 1$. Observe that $\epsilon(F) = 1 - r_2$. Let Σ_1 be a $(1, 3)$-ramp secret sharing scheme over $\mathbb{F}_5$, and let Σ_2 be a 3-threshold secret sharing scheme over $\mathbb{F}_7$. The access function of the concatenation of Σ_1 and Σ_2 is F, and its information ratio is $(\log 5 + \log 7)/(2\log 5 + \log 7) = 1 - r_2$. Hence it is an optimal scheme for F.

Corollary 7.9. *For every uniform access function F there exist*

1. *a sequence of secret sharing schemes (Σ_i) realizing F whose information ratio $\sigma(\Sigma_i)$ converges to $\epsilon(F)$ as $i \to \infty$; and*

2. *a sequence of linear secret sharing schemes (Σ'_i) realizing F_i whose information ratio $\sigma(\Sigma'_i)$ converges to $\epsilon(F)$ as $i \to \infty$ and such that $\lim_{i\to\infty} \sum_{A\subseteq P} |F(A) - F_i(A)| \to 0$.*

8 Conclusion and Open Problems

In this work we present a new framework for the study of non-perfect secret sharing schemes. We present a new lower bound on the information ratio and new constructions. These techniques are enough to compute the optimal information ratio of rational uniform access functions, and to construct optimal linear secret sharing schemes for them. For non-uniform access functions we are very far from understanding the constraints of this optimization problem. From Theorem 3.1 we can obtain a bound on λ, but taking into account Proposition 5.4 we know that it is very far from κ. This is also the case of perfect secret sharing schemes [1, 11]. It will be worth to use

non-Shannon inequalities for the study of the information ratio, but we will face the limitations that have already been found in the perfect case [23]. Hence it is clear that we need new tools for solving the open problems on the efficiency of secret sharing schemes.

Linear secret sharing schemes play a fundamental role in cryptography because of their homomorphic properties. Non-perfect schemes with multiplicative properties (e.g. [8]) and schemes defined over rings are also of great interest, and so it will be worth to apply the techniques presented herein to the study of them.

In several contexts, the access function provide too many details about the structure of the scheme. For instance, in some contexts the unique specifications are the families of forbidden and authorized subsets. Even in this case, our framework is still suitable for the study of the schemes that satisfy these requirements.

In Theorem 7.4 we construct a secret sharing scheme for every rational uniform access function. The interest of the construction is that it attains the optimal information ratio, and that it is linear. We do not consider limitations on the size of the secret, and for certain access functions the secret can be large. For example, if the difference between two values of the access function is small. An interesting open problem, considered in [7] for certain access functions, is the construction of efficient secret sharing schemes when the size of the secret is fixed.

References

[1] A. Beimel. Secret-Sharing Schemes: A Survey. *Coding and Cryptology, Third International Workshop, IWCC 2011, Lecture Notes in Comput. Sci.* **6639** (2011) 11–46.

[2] A. Beimel, and N. Livne. On matroids and non-ideal secret sharing. *Theory of Cryptography, Springer Berlin Heidelberg* (2006) 482-501.

[3] J. Benaloh, J. Leichter. Generalized secret sharing and monotone functions. *Advances in Cryptology, CRYPTO'88. Lecture Notes in Comput. Sci.* **403** (1990) 27–35.

[4] G. R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings.*, **48** (1979) 313–317.

[5] G. R. Blakley, C. Meadows. Security of Ramp Schemes. *Advances in Cryptology, Crypto'84. Lecture Notes in Comput. Sci.* **196** (1985) 242–268.

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

[7] I. Cascudo Pueyo, R. Cramer, C. Xing. Bounds on the Threshold Gap in Secret Sharing over Small Fields. *I*EEE Transactions on Information Theory, **59** number 9 (2013) 5600–5612.

[8] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, V. Vaikuntanathan. Secure Computation from Random Error Correcting Codes. *Advances in Cryptology - EUROCRYPT 2007*, **4515** (2007) 291–310

[9] C. Chen, R.W Yeung. Two-Partition-Symmetrical Entropy Function Regions. *ITW* (2013) 1–5.

[10] T.M. Cover, J.A. Thomas. *Elements of Information Theory*, 2nd ed. Wiley, New York, 2006.

[11] L. Csirmaz. The size of a share must be large. *J. Cryptology*, **10** (1997) 223–231.

[12] O. Farràs, J. R. Metcalf-Burton, C. Padró, L. Vázquez. On the Optimization of Bipartite Secret Sharing Schemes. *Des. Codes Cryptogr.* **63**, Issue 2 (2012) 255–271.

[13] O. Farràs, C. Padró. Extending Brickell–Davenport theorem to non-perfect secret sharing schemes. *Des. Codes Cryptogr.*, Online First (2013).

[14] S. Fujishige. Polymatroidal Dependence Structure of a Set of Random Variables. *Information and Control*, **39** (1978) 55–72.

[15] S. Fujishige. Entropy functions and polymatroids—combinatorial structures in information theory. *Electron. Comm. Japan* **61** (1978) 14–18.

[16] Y. Ishai, E. Kushilevitz, O. Strulovich. Lossy Chains and Fractional Secret Sharing. *STACS, LIPIcs*, **20** (2013) 160–171.

[17] M. Ito, A. Saito, T. Nishizeki. Secret sharing scheme realizing any access structure. *Proc. IEEE Globecom'87.*, (1987) 99–102.

[18] W.-A. Jackson, K.M. Martin. Geometric secret sharing schemes and their duals. *Des. Codes Cryptogr.* **4** (1994) 83–95.

[19] T. Kaced. Almost-perfect secret sharing. http://arxiv.org/abs/1103.2544.

[20] E.D. Karnin, J.W. Greene, and M.E. Hellman, On secret sharing systems, *IEEE Trans. Inform. Theory* **29** (1983), 35–41.

[21] K. Kurosawa, K. Okada, K. Sakano, W. Ogata, S. Tsujii. Nonperfect Secret Sharing Schemes and Matroids. *Advances in Cryptology, EUROCRYPT 1993, Lecture Notes in Comput. Sci.* **765** (1994) 126–141.

[22] J. Martí-Farré, C. Padró. On Secret Sharing Schemes, Matroids and Polymatroids. *J. Math. Cryptol.* **4** (2010) 95–120.

[23] S. Martín Molleví, C. Padró, A. Yang. Secret Sharing, Rank Inequalities and Information Inequalities. *Advances in Cryptology, CRYPTO 2013. Lecture Notes in Comput. Sci.* **8043** (2012) 277–288.

[24] W. Ogata and K. Kurosawa. Some basic properties of general nonperfect secret sharing schemes. *Journal of Universal Computer Science* **4** (1998) 690–704.

[25] W. Ogata, K. Kurosawa, S. Tsujii. Nonperfect Secret Sharing Schemes. *Advances in Cryptology, Auscrypt 92, Lecture Notes in Comput. Sci.* **718** (1993) 56–66.

[26] C. Padró. Lecture Notes in Secret Sharing. *Cryptology ePrint Archive* 2012/674.

[27] C. Padró, L. Vázquez. Finding Lower Bounds on the Complexity of Secret Sharing Schemes by Linear Programming. *Ninth Latin American Theoretical Informatics Symposium, LATIN 2010, Lecture Notes in Computer Science* **6034** (2010) 344–355.

[28] P. Paillier. On ideal non-perfect secret sharing schemes. *Security Protocols, 5th International Workshop, Lecture Notes in Comput. Sci.* **1361** (1998) 207–216.

[29] A. Schrijver. *Combinatorial Optimization. Polyhedra and Efficiency.* Springer-Verlag, Berlin, 2003.

[30] A. Shamir. How to share a secret. *Commun. of the ACM*, **22** (1979) pp. 612–613.

[31] D. J. A. Welsh. *Matroid Theory.* Academic Press, London, 1976.