Partial Secret Sharing[⋆]

Amir Jafari, Reza Kaboli, and Shahram Khazaei

Sharif University of Technology, Tehran, Iran
{ajafari,shahram.khazaei}@sharif.ir

May 30, 2019

Abstract. Information ratio of an access structure is an important parameter for measuring the efficiency of the best secret sharing scheme realizing it. The most common security notion of secret sharing is that of total (perfect) realization. Two well-known relaxations are the notions of *statistical* and *quasi-total* secret sharing. Very little is known about the relation between the information ratio of access structures with respect to different security notions. In this paper, we introduce an extremely relaxed security notion, called *partial secret sharing* and study its properties.

First, we prove that partial and total information ratios coincide for the class of linear secret sharing schemes. One implication of this result is that quasi-total and total information ratios coincide as well for the class of linear schemes. Another implication is that a strong requirement on the linear schemes in the so-called weighted decompositions can be relaxed. *Second*, we prove that the so-called Shannon-type information inequalities provide the same lower-bound on the partial and total information ratios. *Third*, we provide some indication that shows partial and total information ratios probably do not coincide for the class of abelian schemes.

1 Introduction

A (total) *secret sharing scheme* [9, 43] is a cryptographic tool that allows a dealer to share a secret among a set of participants such that only certain *qualified* subsets of them are able to reconstruct the secret. The secret must remain information theoretically hidden from the remaining subsets, called *unqualified*. The collection of all qualified subsets is called an *access structure*, which is supposed to be monotone, i.e., closed under the superset operation. The original definition, known as *threshold* secret sharing, only dealt with access structures that include all subsets of size larger than a certain threshold and the general notion was later introduced in [25]. *Access function* [20] generalizes the notion of access structure in a natural way. An access function is a monotone real function that specifies the percentage of the information on the secret that is obtained by each subset of participants. This concept has been matured by building on a sequence of prior works [10, 33, 44, 47]. Access structures are especial cases of access functions where only all or nothing recovery of the secret is allowed.

[⋆] An update of this paper will be available on eprint

The *information ratio* [11, 13, 37] of a participant in a secret sharing scheme is defined as the ratio of the size of his share and the size of the secret. The information ratio of a secret sharing scheme is the maximum (also sometimes defined as the average) of all participants' information ratios. The information ratio of an access structure is defined as the infimum of the information ratios of all secret sharing schemes that realize it. Computation of information ratio of access structures is a challengingly difficult problem even when we restrict to certain classes of schemes. Information ratio of an access structure can also be defined with respect to a restricted class of schemes, such as the *linear* or *abelian* ones. We refer to the corresponding measures as the linear and abelian information ratio, respectively.

Most of the literature on secret sharing deals with total (perfect) realization of access structures by secret sharing schemes. In this notion, the security is considered for a single scheme, all the qualified sets recover the whole secret, and the secret remains information theoretically hidden from the unqualified sets. These requirements can be relaxed by loosening the reconstruction and privacy requirements. The qualified subsets may miss some information about the secret or may recover it with some error probability. The unqualified subsets are also allowed to gain some information on the secret. By considering a family of schemes, the information leak and incomplete reconstruction are required to be negligible. Two different approaches have been proposed in the literature. The first approach is a standard cryptographic relaxation, called *statistical secret sharing* (see [3] for probably the oldest modern definition and [8] for an old construction). The second one has been introduced in [30, 31], under the name of *quasi-perfect secret sharing*.

For every access structure and every security notion, one can define a corresponding information ratio. It is an open problem if the information ratio of an access structure is invariant with respect to different security notions.

In this paper, we introduce an extremely relaxed security notion, called *partial security*. We study the relation between partial and total information ratios and provide some non-trivial results. We then mention two applications.

1.1 Partial secret sharing and its information ratio

We introduce an extremely relaxed security notion, called *partial* security, and a slightly more liberal one called *semi-partial*. We say that a secret sharing scheme partially realizes an access structure if the amount of information gained by any qualified set is strictly greater than that of any unqualified one. In other words, the qualified sets have a positive *advantage* δ over the unqualified ones with regard to the secret recovery. In the semi-partial realization, we additionally require that the secret remain perfectly hidden from the unqualified sets.

The total information ratio of a secret sharing scheme is defined on its own, i.e., regardless of what access structure it realizes, if any. However, we measure the efficiency of a partial scheme, which we refer to as the *partial information ratio*, with respect to the access structure that it realizes. We define the partial information ratio as a scaled version of the total information ratio where the scale factor is $1/\delta$, where δ is the advantage mentioned above. The intuition behind this choice stems from *decomposition constructions* [23, 46, 47, 49].

1.2 Properties of partial secret sharing

We prove two results and provide an observation (conjecture) about the relation between partial and total information ratios.

Equality of partial and total linear information ratios. We prove that the partial information ratio of an access structure is the same as its total information ratio for the class of all linear secret sharing schemes. To this end, given a partial linear scheme for an access structure, we turn it into a total one for the same access structure with the same information ratio. The proof is somewhat technical and is handled via two linear algebraic lemmas.

Equality of Shannon lower bound. It is easy to show that the lower-bound achieved for statistical and quasi-total information ratios, by merely considering Shannon-type inequalities, is the same as that of total information ratio [30]. We prove that the same thing happens for partial information ratio. To prove this result, we introduce the notion of partial polymatorid for an access structure. Then for a given partial polymatroid for an access structure, we construct a total polymatroid for the same access structure with the same information ratio.

It remains open if our result can be strengthened, e.g., by allowing certain additional non-Shannon type information inequalities [50], e.g., along the lines of [6, 39]. A corollary of our result is that Csirmaz sub-linear lower bound [16] also applies to partial security, which is not clear at a first glance.

On abelian class. Even though we prove that the partial and total security notions coincide with respect to the linear upper-bound and the Shannon lower-bound, it remains open if the two notions coincide for general schemes. We expect the partial and total abelian information ratios not to coincide for the following reason. Recently, an upper-bound on the (total) abelian information ratio of the access structure $\mathcal{F}+\mathcal{N}$—the union of access structures induced by Fano and non-Fano matroids [4, 38]— has been computed in [27] (max$\leqslant 7/6$ and average$\leqslant 41/36$). Moreover, it has been conjectured that a non-trivial lower-bound (i.e., strictly greater than one) exists. In this paper, we show that the partial abelian information ratio of this access structure is one. Therefore, we would not be surprised if total and partial information ratios turn out to become separate for abelian schemes.

1.3 Applications

Our result on equality of partial and total linear information ratios has the following consequences.

Equality of quasi-total and total linear information ratios. We prove that if the partial and total information ratios are equal for some class of schemes, the same holds true for the quasi-total and total information ratios. It remains open if the converse holds true as well. Our result on equality of partial and total linear information ratios then implies that quasi-total and total linear information ratios coincide too.

We remark that even if it turns out that partial and total information ratios coincide for the class of abelian scheme, it is not clear how to show that the same thing happens for quasi-total and total abelian information ratios. The reason is lack of notions such as independence and basis for groups, which exists for vector spaces. However, as we mentioned above, we conjecture that partial and total abelian information ratios not to coincide. This makes it even harder to say anything about the relation between quasi-total and total abelian information ratios.

On decomposition techniques. A common approach for finding upper bounds on the information ratio of access structures is the so-called *decomposition techniques*. These techniques have mainly been used to find upper-bounds on the information ratio of *concrete* access structures on a small number of participants [11,18,23,24,26,34,36,46,48]. They build on Stinson's λ-decomposition [46] by decomposing a given access structure into suitable sub-access structures [49] or sub-access functions [23,47]. In particular, the decomposition theorems in [23, 47] assume that in the linear partial sub-schemes, every subset of participants fully recovers a certain subset of secret elements and nothing more; that is, recovering a non-trivial linear combination of the secret elements is not allowed. Using the notion of partial information ratio and our result on the equality of partial and total linear information ratios, we show this strong requirement can be removed.

1.4 Related work

The relation between different security notions are not well understood. In very few cases, it is known that information ratio with respect to different security notions coincide for some restricted class of schemes. In [3], it has been observed that the statistical and total securities coincide for linear schemes. This result has been recently extended in [28, 29] for a class of schemes which includes group-homomorphic[1] secret sharing schemes. Apart form this result, we are not aware for any coincidence or separation result with respect to different security notions. In [32], it has been proved that statistical security implies quasi-total security. It is easy to argue that the other direction does not necessarily hold true. Nevertheless, it is an open problem if the statistical and quasi-total information ratios coincide.

[1] A secret sharing scheme is called homomorphic if the product of the shares of two secrets produce a share for the product of the secrets. A homomorphic scheme is called group-homomorphic if the secret and share spaces are all groups.

1.5 Paper organization

In Section 2, we present the required preliminaries and introduce our notation. In Section 3, the partial and semi-partial security notions are introduced. Section 4 is devoted to the proof of the equality of (semi-) partial and total information ratios for the class of linear schemes. In Section 5, we prove that the Shannon lower-bound on the partial and total information ratios coincide. Section 6 includes our observation (conjecture) on abelian secret sharing. In Section 7, we study the quasi-total security notion and its relation with partial security. Section 8 studies decomposition techniques regarding our new result on partial secret sharing schemes. Section 9 concludes the paper.

2 Secret sharing schemes

In this section, we provide the basic background along with some notations. We refer the reader to Beimel's survey [2] on secret sharing.

General notations. We denote the support of the random variable $\boldsymbol{X}$ by $\operatorname{supp}(\boldsymbol{X})$. All random variables are discrete in this paper. We assume that the reader is familiar with the Shannon entropy of a random variable $\boldsymbol{X}$, denoted by $\mathrm{H}(\boldsymbol{X})$, and the mutual information of random variables $\boldsymbol{X}, \boldsymbol{Y}$, denoted by $\mathrm{I}(\boldsymbol{X} : \boldsymbol{Y})$. For a positive integer m, we use $[m]$ to represent the set $\{1, \ldots, m\}$. Throughout the paper, $P = \{p_1, \ldots, p_n\}$ stands for a finite set of *participants*. A distinguished participant $p_0 \notin P$ is called *dealer* and we notate $Q = P \cup \{p_0\}$. Unless otherwise stated, we identify the participant p_i with its index i; i.e., $Q = \{0, 1, \ldots, n\}$. The set of positive integers and real numbers are respectively denoted by $\mathbb{N}$ and $\mathbb{R}$. All logarithms are to the base two. The closure of a topological set $\mathcal{X}$ is denoted by $\overline{\mathcal{X}}$, defined as the union of $\mathcal{X}$ with all its limit points.

Definition 2.1 (Access structure) *A non-empty subset $\Gamma \subseteq 2^P$, with $\varnothing \notin \Gamma$, is called an* access structure *on P if it is* monotone*; that is, $A \subseteq B \subseteq P$ and $A \in \Gamma$ imply that that $B \in \Gamma$.*

A subset $A \subseteq P$ is called *qualified* if $A \in \Gamma$; otherwise, it is called *unqualified.* A qualified subset is called *minimal* if none of its proper subsets is qualified.

Definition 2.2 (Access function [20]) *A mapping $\Phi : 2^P \to [0, 1]$ is called an* access function *if $\Phi(\varnothing) = 0$ and it is monotone; i.e., $A \subseteq B \subseteq P$ implies that $\Phi(A) \leqslant \Phi(B)$. An access function is called* rational *if $\Phi(A)$ is rational for every subset A and called* total *if $\Phi(A) \in \{0, 1\}$.*

Definition 2.3 (Secret sharing scheme) *A tuple $\Pi = \left(\boldsymbol{S}_i\right)_{i \in P \cup \{0\}}$ of jointly distributed random variables, with finite supports, is called a* secret sharing scheme *on participant set P when $\mathrm{H}(\boldsymbol{S}_0) > 0$. The random variable $\boldsymbol{S}_0$ is called the* secret *random variable and its support is called the* secret space*. The random variable $\boldsymbol{S}_i$, for any participant $i \in P$, is called the* share *random variable of the participant i and its support is called his* share space*.*

When we say that a secret $s \in \operatorname{supp}(\boldsymbol{S}_0)$ *is shared using* Π, we mean that a tuple $\big(s_i\big)_{i \in P \cup \{0\}}$ is sampled according to the distribution Π conditioned on the event $\{\boldsymbol{S}_0 = s\}$.

A secret sharing scheme Π is said to be *linear* if there exists a finite field $\mathbb{F}$ such that the support of every marginal random variable is an $\mathbb{F}$-vector space of finite dimension; additionally, we require that the joint distribution Π be uniform. When we want to emphasize the underlaid finite field, we call it an $\mathbb{F}$-*linear* scheme. When characteristic of $\mathbb{F}$ is p, a prime, we call it a p-linear scheme.

The most common definition of a linear scheme is based on linear maps. A secret sharing scheme $(\boldsymbol{S}_i)_{i \in Q}$ is said to be *linear* if there are finite dimensional vector spaces E and $(E_i)_{i \in Q}$, and linear maps $\mu_i : E \to E_i$, $i \in Q$ such that $\boldsymbol{S}_i = \mu_i(\boldsymbol{E})$, where $\boldsymbol{E}$ is the uniform distribution on E. In this paper, we use the following equivalent definition (see Appendix B or [27] for justification).

Definition 2.4 (Linear scheme) *A tuple* $\Pi = (T; T_0, T_1, \ldots, T_n)$ *is called an* $\mathbb{F}$*-linear (or simply a linear) secret sharing scheme if* T *is a finite dimensional* $\mathbb{F}$*-vector space,* T_i *is a subspace of* T*, for each* $i \in [n]$*, and* $\dim T_0 \geqslant 1$*. When there is no confusion, we omit* T *and simply write* $\Pi = (T_i)_{i \in P \cup \{0\}}$*. If the characteristic of* $\mathbb{F}$ *is* p*, we call the scheme* p*-linear.*

Definition 2.5 (Total realization) *We say that a secret sharing scheme* $\Pi = \big(\boldsymbol{S}_i\big)_{i \in P \cup \{0\}}$ *is a* (total) scheme *for* Γ*, or it* (totally) realizes Γ*, if the following two hold, where* $\boldsymbol{S}_A = (\boldsymbol{S}_i)_{i \in A}$*, for a subset* $A \subseteq P$*:*

(Correctness) $\mathrm{H}(\boldsymbol{S}_0 | \boldsymbol{S}_A) = 0$ *for every qualified set* $A \in \Gamma$ *and,*
(Privacy) $\mathrm{I}(\boldsymbol{S}_0 : \boldsymbol{S}_B) = 0$ *for every unqualified set* $B \in \Gamma^c$*.*

Definition 2.6 (Access function/convec of a scheme) *The* access function *and the* (total) convec *of a secret sharing scheme* $\Pi = \big(\boldsymbol{S}_i\big)_{i \in P \cup \{0\}}$ *are respectively denoted by* Φ_Π *and* $\mathrm{cv}(\Pi)$ *and defined as follows:*

$$\Phi_\Pi(A) = \frac{\mathrm{I}(\boldsymbol{S}_0 : \boldsymbol{S}_A)}{\mathrm{H}(\boldsymbol{S}_0)}\ , \qquad \mathrm{cv}(\Pi) = \Big(\frac{\mathrm{H}(\boldsymbol{S}_i)}{\mathrm{H}(\boldsymbol{S}_0)}\Big)_{i \in P}\ .$$

For a linear scheme $\Pi = (T_i)_{i \in P \cup \{0\}}$, it is easy to verify that

$$\Phi_\Pi(A) = \frac{\dim(T_0 \cap T_A)}{\dim(T_0)}\ , \qquad \mathrm{cv}(\Pi) = \Big(\frac{\dim(T_i)}{\dim(T_0)}\Big)_{i \in P}\ .$$

Information ratio and convec set. Convec is short for contribution vector [26] and a norm on it can be used as a measure of efficiency of a secret sharing scheme. The convec set of an access structure can be defined with respect to a class of secret sharing schemes (e.g., linear, group-characterizable, abelian, etc).

Definition 2.7 (Total convec set) *The (total) convec set of an access structure Γ, denoted by $\Sigma_{\mathrm{t}}(\Gamma)$, is defined as the set of all convecs of all secret sharing schemes that (totally) realize Γ. When we restrict to the class* C *of secret sharing schemes, we use the notation $\Sigma_{\mathrm{t}}^{\mathrm{C}}(\Gamma)$.*

We use the notation $\Sigma_{\mathrm{t}}^{\mathrm{L}}$ (resp. Σ_{t}^{p}) when the convec set is restricted to the class of all linear (resp. p-linear) secret sharing schemes and call it the linear (resp. p-linear) convec set. The maximum and average information ratios of an access structure Γ on n participants, for the class C of secret sharing schemes, are respectively defined as:

$$\min\{\max(\boldsymbol{x}) : \boldsymbol{x} \in \overline{\Sigma_{\mathrm{t}}^{\mathrm{C}}(\Gamma)}\} \quad \text{and} \quad \tfrac{1}{n}\min\{\textstyle\sum_{i=1}^{n} x_i : (x_1, \ldots, x_n) \in \overline{\Sigma_{\mathrm{t}}^{\mathrm{C}}(\Gamma)}\} \ .$$

The polymatroidal set. Additionally, we introduce the K_{t}-set, called the total polymatroidal set, as a generalization of the κ-parameter [35]. The total polymatroidal set of an access structure Γ on n participants, denoted by $K_{\mathrm{t}}(\Gamma)$, is an n-dimensional polytope derived by taking into account all the Shannon inequalities as well as the correctness and privacy conditions. In Section 5, we present a precise definition; see Definition 5.5.

3 Partial and semi-partial secret sharing

In this section, we introduce two relaxed security notions for secret sharing schemes, referred to as *semi-partial* and *partial* realizations. A scheme is said to partially realize an access structure if the amount of information gained on the secret by every qualified set is strictly larger than that of any unqualified one. The semi-partial definition is less relaxed since it requires that the secret still remain information theoretically hidden from unqualified sets.

As we will see in Section 7 and Section 8, this secuirty notion plays a cruital role for 1) proving that the quasi-total [30] and total convec sets coincide for linear schemes and 2) relaxing the requirements of the weighted-decompositions [23, 47].

3.1 Security definition

We begin by giving a formal definition of partial and semi-partial security notions.

Definition 3.1 (Partial and semi-partial realization) *We say that a secret sharing scheme Π is a* partial scheme *for Γ, or it* partially realizes *Γ, if:*

$$\delta = \min_{A \in \Gamma} \Phi_{\Pi}(A) - \max_{B \in \Gamma^c} \Phi_{\Pi}(B) > 0 \ . \tag{3.1}$$

We call it a semi-partial scheme*, if additionally $\Phi_{\Pi}(B) = 0$, for every unqualified set $B \in \Gamma^c$.*

The parameter δ is a *normalized* measure for quantifying the advantage of the qualified sets over the unqualified ones with respect to the amount of information that they gain on the secret. The intuition behind the choice of this factor and the following definition stems from decomposition constructions [23, 46, 47, 49], in which a similar scale factor appears. We will revisit decomposition methods in Section 8.

3.2 Partial convec

We measure the efficiency of a (semi-) partial scheme for an access structure via a scaled version of its usual (i.e., total) convec, that we call *partial convec.*

Definition 3.2 (Partial convec) *Let Π be a partial scheme for Γ. The* partial convec *of Π (with respect to Γ) is defined and denoted by*

$$\mathrm{pcv}(\Pi, \Gamma) = \frac{1}{\delta}\mathrm{cv}(\Pi),$$

where δ, the (normalized) advantage, is defined as in Equation (3.1). When there is no confusion, we simply use the notation $\mathrm{pcv}(\Pi)$*.*

The notions of partial and semi-partial realization give rise to two new convec sets.

Definition 3.3 (Partial and semi-partial convec sets) *The* partial convec set *of an access structure Γ, denoted by $\Sigma_{\mathrm{p}}(\Gamma)$, is defined as the set of all* partial convecs *of all secret sharing schemes that partially realize Γ. The* semi-partial convec set *is defined similarly and is denoted by $\Sigma_{\mathrm{sp}}(\Gamma)$. When we restrict to the class* C *of secret sharing schemes, we notate $\Sigma_{\mathrm{p}}^{\mathrm{C}}(\Gamma)$ and $\Sigma_{\mathrm{sp}}^{\mathrm{C}}(\Gamma)$.*

The K_{p}, $\Sigma_{\mathrm{p}}^{\mathrm{L}}$ and Σ_{p}^{p}-sets are defined similar to the case of total convec set. Similar notations are used for semi-partial security. The relation $\Sigma_{\mathrm{t}}^{\mathrm{C}}(\Gamma) \subseteq \Sigma_{\mathrm{sp}}^{\mathrm{C}}(\Gamma) \subseteq \Sigma_{\mathrm{p}}^{\mathrm{C}}(\Gamma)$ is immediate for any access structure Γ and any class C of secret sharing schemes. In Section 4 we prove that for the three security notions, the linear convec sets are the same (i.e., $\Sigma_{\mathrm{t}}^{\mathrm{L}}(\Gamma) = \Sigma_{\mathrm{sp}}^{\mathrm{L}}(\Gamma) = \Sigma_{\mathrm{p}}^{\mathrm{L}}(\Gamma)$). Also, in Section 5, we prove that the Shannon inequalities give the same lower-bound for the convec set (i.e., $K_{\mathrm{t}}(\Gamma) = K_{\mathrm{sp}}(\Gamma) = K_{\mathrm{p}}(\Gamma)$). In Section 6, we provide some evidence that for the class C of abelian schemes the inclusion $\Sigma_{\mathrm{t}}^{\mathrm{C}}(\Gamma) \subseteq \Sigma_{\mathrm{sp}}^{\mathrm{C}}(\Gamma)$ might be proper. The following proposition then follows.

Proposition 3.4 (Convec set relations) *For any access structure Γ, we have*

$$\Sigma_{\mathrm{t}}^{\mathrm{L}}(\Gamma) \subseteq \Sigma_{\mathrm{t}}(\Gamma) \subseteq \Sigma_{\mathrm{sp}}(\Gamma) \subseteq \Sigma_{\mathrm{p}}(\Gamma) \subseteq K_{\mathrm{t}}(\Gamma)\ .$$

Separation. Separation result between closures of $\Sigma_{\mathrm{t}}^{\mathrm{L}}$ and Σ_{t} has been proved in a recent work [27][2]. Separation between closure of Σ_{t} and K_{t} is also known [5] (based on an old result by Seymour [42]). It is easy to find examples that separate between Σ_{p} and K_{t}. Proving or disproving separations between Σ_{t} and Σ_{sp} and also between Σ_{sp} and Σ_{p} remains open.

Convexity. It is easy to show that the total convec set of any access structure is a set with *convex closure*. It remains open if this is also the case for the partial and semi-partial security notions.

4 Equality of total and partial linear convec sets

In this section, we prove that the linear convec set is the same for the total, partial and semi-partial security notions. Two linear algebraic lemmas lie at the core of our proofs. The first one is used in Proposition 4.4 for transforming a semi-partial linear secret sharing scheme for a given access structure into a total one without changing its (partial) convec. But we also need the second lemma in Proposition 4.5 for proving a similar claim for partial schemes. The following theorem is then a direct corollary of both propositions.

Theorem 4.1 (Equality of partial and total linear convec sets) *Let p be a prime and Γ be an access structure. Then, $\Sigma_{\mathrm{p}}^{p}(\Gamma) = \Sigma_{\mathrm{sp}}^{p}(\Gamma) = \Sigma_{\mathrm{t}}^{p}(\Gamma)$, and in particular,*

$$\Sigma_{\mathrm{p}}^{\mathrm{L}}(\Gamma) = \Sigma_{\mathrm{sp}}^{\mathrm{L}}(\Gamma) = \Sigma_{\mathrm{t}}^{\mathrm{L}}(\Gamma) \ .$$

It remains open if the claim of Theorem 4.1 holds for other classes of schemes. In Section 6, we show that they probably become separate for the class of abelian schemes. However, their separation/coincidence for general secret sharing remains unclear.

4.1 Two linear algebraic lemmas

Our first lemma promises the existence of some linear maps that work for *any* subspace over a given finite field. The lemma does not hold if the space is not defined over a field that is not finite. So the claim is truly a property of finite fields.

[2] In this paper, we only focus on amortized definition of information ratio, i.e. the secret can be arbitrarily long. Refer to [1] for the role of amortization in secret sharing. In fact our definition of a linear scheme allows arbitrary secret dimension, which is usually called *multi-linear* in the literature. In another variant, which we call *scaler-linear*, the secret is allowed to contain only one field element. Separation between scaler-linear and non-linear secret sharing was first proved by Beimel and Ishai in [3] under some plausible assumption. Later, such a separation was proved in [7] without relying on any assumption.

Lemma 4.2 (Linear transformation lemma) *Let $1 \leqslant \lambda \leqslant m$ be integers. Let T_0 be a vector space over some finite field with dimension m. Then, there exist m linear maps $L_1, \ldots, L_m : T_0 \to T_0^{\lambda}$ such that for any subspace $E \subseteq T_0$ of dimension $\dim E \geqslant \lambda$, the following holds*

$$\sum_{i=1}^{m} L_i(E) = T_0^{\lambda} \ .$$

Proof. Without loss of generality we can assume that $T_0 = \mathbb{F}^m$, where $\mathbb{F}$ is the underlying finite field. We show that there exist m linear maps $L_1, \ldots, L_m : \mathbb{F}^m \to \mathbb{F}^{m\lambda}$, such that for any λ linearly independent vectors $x_1, \ldots, x_\lambda \in \mathbb{F}^m$, the $m\lambda$ vectors $L_i(x_j) \in \mathbb{F}^{m\lambda}$, $i \in [m]$ and $j \in [\lambda]$, are linearly independent. The construction is explicit and is as follows.

Let $|\mathbb{F}| = q$ and identify $\mathbb{F}^m$ with a finite field $\mathbb{K}$ with q^m elements that is an extension of $\mathbb{F}$ with degree m. Choose a basis $w_1, ..., w_m$ for $\mathbb{K}$ over $\mathbb{F}$ and identify $\mathbb{F}^{m\lambda}$ with $\mathbb{K}^{\lambda}$.

Define L_i by sending $x \in \mathbb{K}$ to $(w_i x, w_i x^q, ..., w_i x^{q^{\lambda-1}}) \in \mathbb{K}^{\lambda}$. Note that the mappings $x \longmapsto x^q$ is an $\mathbb{F}$-linear map from $\mathbb{K}$ to $\mathbb{K}$ and $x \longmapsto x^{q^i}$ is the composition of this map with itself i times. Therefore, the mapping L_i is $\mathbb{F}$-linear too, for every $i \in [m]$. If there exist coefficients c_{ij}, $i \in [m]$ and $j \in [\lambda]$, such that $\Sigma_{j=1}^{\lambda} \Sigma_{i=1}^{m} c_{ij} L_i(x_j) = 0$, then $\sum_{j=1}^{\lambda} (\sum_{i=1}^{m} c_{ij} w_i) x_j^{q^{k-1}} = 0$ for every $k \in [\lambda]$. Since the $\lambda \times \lambda$ matrix $M = \left(x_i^{q^{k-1}} \right)_{i \in [\lambda], k \in [\lambda]}$ is invertible (to be proved at the end), we have $\sum_{i=1}^{m} c_{ij} w_i = 0$ for all $j \in [\lambda]$ and thus $c_{ij} = 0$, for every $i \in [m]$ and $j \in [\lambda]$, as the vectors $w_1, ..., w_m$ are linearly independent over $\mathbb{F}$. Therefore, the vectors $L_i(x_j)$, $i \in [m]$ and $j \in [\lambda]$, are linearly independent over $\mathbb{F}$.

We complete the proof by showing that the matrix M is invertible. Assume for a row vector $y = (y_1, \ldots, y_\lambda)$, we have $yM = 0$, hence $y_1 x + y_2 x^q + \ldots + y_\lambda x^{q^{\lambda-1}} = 0$ for every $x = x_1, \ldots, x_\lambda$. Since this polynomial is linear over the field $\mathbb{F}$, it vanishes on the span of these independent vectors over $\mathbb{F}$, a space with q^{λ} elements. However, as the polynomial is of degree $q^{\lambda-1}$, it is identically zero; i.e., $y = 0$. This shows that M is invertible. □

The following lemma is true for finite fields that are sufficiently large. In Appendix A we present an interesting probabilistic proof, proposed by one the Eurocrypt reviewers, but with a slightly stronger requirement on the field size.

Lemma 4.3 (Non-intersecting subspace lemma) *Let T_0 be a vector space of dimension m over a finite field with q elements and let $E_1, \ldots, E_N$ be subspaces of T_0 of dimension at most ω, $1 \leqslant \omega < m$. If $N < \frac{q^m - 1}{q^{m-1} - 1}$, then there is a subspace $S \subset T_0$ of dimension $m - \omega$ such that $S \cap E_i = 0$, for every $i \in [N]$.*

Proof. Without loss of generality we can assume that $\dim E_i = \omega$. Let $\mathbb{F}$ be the underlying finite field with q elements. We show that if $N < \frac{q^m - 1}{q^{m-1} - 1}$, then the required subspace S of dimension $m - w$ with zero intersection with E_i's exists. We prove this by induction on $m - w$. If $m - w = 1$, then each E_i has $q^{m-1} - 1$ non-zero elements so we have at most $N(q^{m-1} - 1)$ non-zero elements in their union. If $N < \frac{q^m-1}{q^{m-1}-1}$ then there is a non-zero element outside this union that generates the required subspace S. If E_i's are of dimension w, then since $N < \frac{q^m-1}{q^w-1}$ the above proof shows that there is a non-zero vector u outside their union. If we add this vector to each E_i we get subspace E'_i of dimension $w + 1$. Therefore, by induction, we have a subspace S' of dimension $m - w - 1$ that has zero intersection with each E'_i. Now the space generated by S and u is the required subspace of dimension $m - w$ and zero intersection with each E_i. □

4.2 A convec-preserving total linear scheme from a semi-partial linear one

The following proposition will be generalized in next subsection. However, we present it separately in this subsection since we will build on its proof in the course of the proof of Proposition 4.5.

Proposition 4.4 ($\boldsymbol{\Sigma^p_{\mathrm{sp}}} = \boldsymbol{\Sigma^p_{\mathrm{t}}}$) *Let Γ be an access structure and Π' be a semi-partial $\mathbb{F}$-linear secret sharing scheme for it. Then, there exists a total $\mathbb{F}$-linear secret sharing scheme Π for Γ such that* $\mathrm{cv}(\Pi) = \mathrm{pcv}(\Pi')$.

Proof. We first provide an informal proof by using duals of the linear maps introduced in Lemma 4.2. Identify the secret space of Π' by $\mathbb{F}^m$. Since Π' is a semi-partial scheme for Γ, there exists an integer λ, with $1 \leqslant \lambda \leqslant m$, such that every qualified participant set discovers at least λ independent linear relations on the secret. With a slight abuse of notation, let $L^\star_1, \dots, L^\star_m : \mathbb{F}^{m\lambda} \to \mathbb{F}^m$ be the dual (transpose) of the linear maps of Lemma 4.2. We construct a total linear scheme Π for Γ with secret space $\mathbb{F}^{m\lambda}$ such that its convec is the same as the partial convec of Π'. To share a secret $s \in \mathbb{F}^{m\lambda}$, we share each of the m secrets $L^\star_1(s), \dots, L^\star_m(s) \in \mathbb{F}^m$ using an independent instance of Π'. Each participant in Π receives a share from each instance of Π'. Hence, while the secret length has been multiplied by λ, the share of each participant has increased by a factor of at most m. By adding dummy shares, one can achieve an exact factor of m. Therefore, the total convec of Π and semi-partial convec of Π' are equal. Note that since the m different instances of Π' use independent randomnesses, any qualified set gains no information on the secret. By Lemma 4.2, each qualified set gets $m\lambda$ independent linear relations on s. We conclude that the scheme Π is total.

We now prove the lemma more formally by direct use of linear maps of Lemma 4.2. Let $\Pi' = (T'; T'_0, T'_1, \dots, T'_n)$ be the $\mathbb{F}$-linear semi-partial scheme that satisfies $\lambda = \min_{A \in \Gamma}\{\dim(T'_A \cap T'_0)\} \geqslant 1$ and $\dim(T'_A \cap T'_0) = 0$ for all $A \in \Gamma^c$. Let $m = \dim(T_0) \geqslant 1$.

Our goal is to build a total $\mathbb{F}$-linear scheme $\Pi = (T; T_0, T_1, \dots, T_n)$ such that $\dim(T_i) \leqslant m \dim(T'_i)$ for every $i \in [n]$ and $\dim(T_0) = m\lambda$.

Find an orthogonal complement R' for T'_0 inside T'; hence, $T' = T'_0 \oplus R'$. Let $T = {T'}^{\lambda}_0 \oplus {R'}^m$.

Let $L_1, \ldots, L_m : T'_0 \to {T'}_0^{\lambda}$ be the linear maps of Lemma 4.2 and define $\phi : {T'}^m \to T$ by

$$\phi(s_1, \ldots, s_m, r_1, \ldots, r_m) = \big(\sum_{i=1}^{m} L_i(s_i), r_1, \ldots, r_m \big) \ ,$$

where $s_1, \ldots, s_m \in T'_0$ and $r_1, \ldots, r_m \in R'$.

We let $T_0 = {T'}_0^{\lambda}$ and $T_i = \phi({T'}_i^m)$. Then, the conditions on dimensions are clear and consequently $\mathrm{cv}(\mathit{\Pi}) \preceq \mathrm{pcv}(\mathit{\Pi}')$. It is straightforward to tweak the scheme such that the claimed vector equality holds. It remains to prove that $\mathit{\Pi}$ totally realizes $\mathit{\Gamma}$.

For $A \subseteq [n]$, by linearity of ϕ, we have $T_A = \phi({T'}_A^m)$. Also, we have:

$$\begin{aligned} T_A \cap T_0 &= \phi({T'}_A^m) \cap {T'}_0^{\lambda} \\ &= \phi({T'}_A^m \cap {T'}_0^m) \\ &= \phi\big((T'_A \cap T'_0)^m\big) \\ &= \textstyle\sum_{i=1}^m L_i(T'_A \cap T'_0) \ , \end{aligned}$$

where the second equality follows from the following fact: $\phi(x) \in {T'}_0^{\lambda}$ if and only if $x \in {T'}_0^m$.

If $A \in \mathit{\Gamma}$, then $\dim(T'_A \cap T'_0) \geqslant \lambda$. Therefore, by Lemma 4.2, we have $T_A \cap T_0 = T_0$. Also, if $B \in \mathit{\Gamma}^c$, then $T'_B \cap T'_0 = 0$ and hence $T_B \cap T_0 = 0$. This shows that $\mathit{\Pi}$ is a total scheme for $\mathit{\Gamma}$. □

4.3 A convec-preserving total linear scheme from a partial linear one

The following proposition is a generalization of Proposition 4.4. The proof expands on the proof of Proposition 4.4 by appropriately using Lemma 4.2.

Proposition 4.5 ($\boldsymbol{\Sigma}^{\boldsymbol{p}}_{\mathbf{p}} = \boldsymbol{\Sigma}^{\boldsymbol{p}}_{\mathbf{t}}$) *Let $\mathit{\Gamma}$ be an access structure and $\mathit{\Pi}'$ be a partial $\mathbb{F}$-linear secret sharing scheme for it. Then, there exists a finite extension $\mathbb{K}$ of $\mathbb{F}$ and a total $\mathbb{K}$-linear secret sharing scheme $\mathit{\Pi}$ for $\mathit{\Gamma}$ such that* $\mathrm{cv}(\mathit{\Pi}) = \mathrm{pcv}(\mathit{\Pi}')$. *Consequently, $\mathit{\Sigma}^p_{\mathrm{p}}(\mathit{\Gamma}) = \mathit{\Sigma}^p_{\mathrm{t}}(\mathit{\Gamma})$, for every prime p.*

Proof. Let $\mathit{\Pi}' = (T'_0, \ldots, T'_n)$ and denote

$$\begin{aligned} \lambda &= \min\nolimits_{A \in \mathit{\Gamma}} \{\dim(T'_A \cap T'_0)\} \\ \omega &= \max\nolimits_{A \in \mathit{\Gamma}^c} \{\dim(T'_A \cap T'_0)\} \\ m &= \dim T'_0 \end{aligned}$$

where $1 \leqslant \lambda - \omega \leqslant m$.

Let N be the number of maximal unqualified subsets in $\mathit{\Gamma}^c$ and $\mathbb{K}$ be an extension of $\mathbb{F}$ that satisfies $|\mathbb{K}| \geqslant N$. By the process of extending scalers, we can turn $\mathit{\Pi}'$ into a $\mathbb{K}$-linear scheme with the same convec, access function and dimensions. For simplicity, we use the same notation for the new scheme; i.e., from now on $\mathit{\Pi}'$ is considered to be a $\mathbb{K}$-linear scheme. In particular, the relations for λ, ω, m are still valid.

Construct $(T_0, \ldots, T_n)$ from Π' the same way as in the proof of Proposition 4.4 and recall that $\dim T_0 = m\lambda$ and $\dim T_i \leqslant m \dim T_i'$. The same argument, which was used in the proof of Proposition 4.4, shows that for any $A \in \Gamma$, we have $T_A \cap T_0 = T_0$. It is also trivial that for every $B \in \Gamma$, we have $\dim \left(T_B \cap T_0\right) \leqslant m\omega$.

By Lemma 4.3 (E_i is $T_B \cap T_0$ for some maximal unqualified set B, $\dim E_i \leqslant m\omega$ and $\dim T_0 = m\lambda$), one can choose $S \subseteq T_0$ of dimension $m(\lambda - \omega)$ such that $T_B \cap S = 0$, for every $B \in \Gamma^c$. Also, it is trivial that $T_A \cap S = S$, for every $A \in \Gamma$. Now, it is clear that $\Pi = (S, T_1, \ldots, T_n)$ is a total secret sharing scheme for Γ such that $\dim S = m(\lambda - \omega)$. Therefore, $\mathrm{cv}(\Pi) \preceq \mathrm{pcv}(\Pi')$. Again, it is straightforward to tweak the scheme such that the convec equality holds. □

5 Shannon lower-bound for partial information ratio

The main result of this section is to prove that the Shannon inequalities give the same lower-bound for the total and partial security notions. In other words, the polymatroidal sets of an access structure with respect to all security definitions are equal. It remains open if our result can be strengthened, e.g., by allowing certain additional non-Shannon type information inequalities, e.g., along the lines of [6, 39]). Our result shows that Csirmaz sub-linear lower bound [16] also applies to partial security.

We define the polymatroidal sets precisely and then prove our claim. We use the following definition for a polymatroid, first introduced by Edmonds [19] in 1970. The relation between polymatroids and random variables was realized by Fujishige [22] in 1978. We refer the reader to Padro's lecture notes [40] for a leaner introduction to matroids, polymatroids and their connection to secret sharing.

Definition 5.1 (Polymatroid) *Let Q be a finite set. We say that $\mathcal{S} = (Q, r)$ is a polymatroid with ground set Q and rank function $r : 2^Q \to \mathbb{R}$, when:*

a) $r(\varnothing) = 0$,
b) $r(X) \leqslant r(Y)$, *for every subsets* $X \subseteq Y \subseteq Q$ *(monotonicity),*
c) $r(X) + r(Y) \geqslant r(X \cup Y) + r(X \cap Y)$, *for every subsets* $X, Y \subseteq Q$ *(submodularity).*

We simply denote the rank function of a singleton set $\{p\}$ by $r(p)$. We let $Q = P \cup \{p_0\}$ where $P = \{p_1, \cdots, p_n\}$ and assume that $r(p_0) > 0$. We borrow the following notation from [20].

Notation 5.2 *Let $\mathcal{S} = (Q, r)$ be a polymatroid and A and B be subsets of Q. We notate*

$$r(A|B) = r(AB) - r(B),$$

$$\Delta_r(A : B) = r(A) + r(B) - r(AB).$$

5.1 Total polymatroidal set

Informally, the total polymatroidal set of an access structure $\mathit{\Gamma}$ on n participants, denoted by $K_{\mathrm{t}}(\mathit{\Gamma})$, is the n-dimensional polytope derived by taking into account all the Shannon inequalities as well as the correctness and privacy conditions.

Definition 5.3 (Total polymatroid) *Let $\mathit{\Gamma}$ be an access structure on P and $\mathcal{S} = (Q, r)$ be a polymatroid. We say that $\mathcal{S}$ is a* total polymatroid *for $\mathit{\Gamma}$ when:*

a) $\mathit{\Delta}_r(\{p_0\} : A) = r(p_0)$, for every qualified set $A \in \mathit{\Gamma}$ and,
b) $\mathit{\Delta}_r(\{p_0\} : B) = 0$, for every unqualified set $B \in \mathit{\Gamma}^c$.

Definition 5.4 (Total convec of a polymatroid) *The* total convec *of a polymatroid $\mathcal{S} = (Q, r)$ is defined and denoted by* $\mathrm{cv}(\mathcal{S}) = \frac{1}{r(p_0)}(r(p))_{p \in P}$.

Definition 5.5 (Total polymatroidal set) *The K_{t}-set or* total polymatroidal set *of an access structure $\mathit{\Gamma}$, denoted by $K_{\mathrm{t}}(\mathit{\Gamma})$, is defined as the set of all total convecs of all polymatroids for $\mathit{\Gamma}$.*

The following proposition is an extention of the inequality $\kappa(\mathit{\Gamma}) \leqslant \sigma(\mathit{\Gamma})$ [35].

Proposition 5.6 ($\boldsymbol{\Sigma}_{\mathbf{t}}(\boldsymbol{\Gamma}) \subseteq \boldsymbol{K}_{\mathbf{t}}(\boldsymbol{\Gamma})$) *For any access structure $\mathit{\Gamma}$, it holds that $\mathit{\Sigma}_{\mathrm{t}}(\mathit{\Gamma}) \subseteq K_{\mathrm{t}}(\mathit{\Gamma})$.*

5.2 Partial and semi-partial polymatroidal sets

Definition 5.7 (Partial and semi-partial polymatroid) *Let $\mathit{\Gamma}$ be an access structure on P and $\mathcal{S} = (Q, r)$ be a polymatroid. We say that $\mathcal{S}$ is a* partial polymatroid *for $\mathit{\Gamma}$ when:*

$$\delta = \min_{A \in \mathit{\Gamma}} \mathit{\Delta}_r(\{p_0\} : A) - \max_{B \in \mathit{\Gamma}^c} \mathit{\Delta}_r(\{p_0\} : B) > 0 \ . \tag{5.1}$$

If for every unqualified set $B \in \mathit{\Gamma}^c$ it additionally holds that $\mathit{\Delta}_r(\{p_0\} : B) = 0$, we call it a semi-partial polymatroid for $\mathit{\Gamma}$.

Definition 5.8 (Partial and semi-partial convec of a polymatroid) *Let $\mathit{\Gamma}$ be an access structure on P and $\mathcal{S} = (Q, r)$ be a partial polymatroid for $\mathit{\Gamma}$. The* partial convec *of $\mathcal{S}$ (with respect to $\mathit{\Gamma}$) is defined and denoted by*

$$\mathrm{pcv}(\mathcal{S}, \mathit{\Gamma}) = \frac{1}{\delta}(r(p))_{p \in P} \ .$$

where δ, the advantage, is defined as in Equation (5.1). When there is no confusion, we simply use the notation $\mathrm{pcv}(\mathcal{S})$.

Definition 5.9 (Partial and semi-partial polymatroidal convec sets) *The* partial polymatroidal convec set *of an access structure $\mathit{\Gamma}$, denoted by $K_{\mathrm{p}}(\mathit{\Gamma})$, is defined as the set of all* partial convecs *of all polymatroids that partially realize $\mathit{\Gamma}$. The* semi-partial polymatroidal convec set *is defined similarly and is denoted by $K_{\mathrm{sp}}(\mathit{\Gamma})$.*

Proposition 5.6 also holds for the partial security; that is, for any access structure $\mathit{\Gamma}$, it holds that $\mathit{\Sigma}_{\mathrm{p}}(\mathit{\Gamma}) \subseteq K_{\mathrm{p}}(\mathit{\Gamma})$ and $\mathit{\Sigma}_{\mathrm{sp}}(\mathit{\Gamma}) \subseteq K_{\mathrm{sp}}(\mathit{\Gamma})$. The relation $K_{\mathrm{t}}(\mathit{\Gamma}) \subseteq K_{\mathrm{sp}}(\mathit{\Gamma}) \subseteq K_{\mathrm{p}}(\mathit{\Gamma})$ is immediate for any access structure $\mathit{\Gamma}$. In next section we prove that these sets are indeed the same.

5.3 Main claim

Even though the K_{t}-set is trivially a polytope, it is not trivial that so are the other two sets, let alone being identical to the K_{t}-set.

Theorem 5.10 ($\boldsymbol{K_{\mathrm{p}} = K_{\mathrm{sp}} = K_{\mathrm{t}}}$) *For any access structure, the total, partial and semi-partial polymatroidal sets are identical.*

Proof. We know that $K_{\mathrm{t}}(\mathit{\Gamma}) \subseteq K_{\mathrm{sp}}(\mathit{\Gamma}) \subseteq K_{\mathrm{p}}(\mathit{\Gamma})$ for any access structure $\mathit{\Gamma}$. It is sufficient to prove that $K_{\mathrm{p}}(\mathit{\Gamma}) \subseteq K_{\mathrm{t}}(\mathit{\Gamma})$. Suppose that $\boldsymbol{a}' \in K_{\mathrm{p}}(\mathit{\Gamma})$. Then, there exists a partial polymatroid $\mathcal{S}' = (P \cup \{p_0\}, r')$ for $\mathit{\Gamma}$ and $\boldsymbol{a}' = \mathrm{pcv}(\mathcal{S}')$. We construct a total polymatroid $\mathcal{S} = (P \cup \{p_0\}, r)$ from $\mathcal{S}'$ for $\mathit{\Gamma}$ such that $\mathrm{cv}(\mathcal{S}) = \mathrm{pcv}(\mathcal{S}')$. Let δ be as in Definition 5.1 and define α, β as follows,

$$\alpha = \min_{A \in \mathit{\Gamma}} \mathit{\Delta}_r(\{p_0\} : A)/r'(p_0) \quad , \quad \beta = \max_{B \in \mathit{\Gamma}^c} \mathit{\Delta}_r(\{p_0\} : B)/r'(p_0).$$

Define the function $r : 2^{P \cup \{p_0\}} \to [0, \infty)$ as follows:

$r(A) = r'(A)/\alpha$ for $A \in \mathit{\Gamma}^c$,
$r(A) = r'(A|\{p_0\})/\alpha + r'(p_0)$ for $A \in \mathit{\Gamma}$,
$r(A \cup \{p_0\}) = r(A)$ for $A \in \mathit{\Gamma}$,
$r(A \cup \{p_0\}) = r(A) + \frac{\alpha-\beta}{\alpha} r'(p_0)$ for $A \in \mathit{\Gamma}^c$;

Note that we have $r(\varnothing) = 0$ and $r(p_0) = \frac{\alpha-\beta}{\alpha} r'(p_0)$.

We claim that r is a rank function of a polymatroid with ground set $P \cup \{p_0\}$. First, we show that r has the monotonicity property. We check the monotonicity property only for the following nontrivial case: $A \cup \{p_0\} \subseteq B \cup \{p_0\}$ where A is a unqualified set and B is qualified. Checking the monotonicity property for the other cases is easier and left to the reader. Since $A \cup \{p_0\} \subseteq B \cup \{p_0\}$, the monotonicity of r' implies that $r'(A \cup \{p_0\}) \leqslant r'(B \cup \{p_0\})$. Therefore $r'(A|\{p_0\}) \leqslant r'(B|\{p_0\})$. Since A is unqualified we have $r'(A) \leqslant r'(A|\{p_0\}) + \beta r'(\{p_0\})$. Thus

$$\begin{aligned}
r(A \cup \{p_0\}) &= r(A) + \frac{\alpha-\beta}{\alpha} r'(\{p_0\}) \\
&= \frac{r'(A)}{\alpha} + r'(\{p_0\}) - \frac{\beta}{\alpha} r'(\{p_0\}) \\
&\leqslant \frac{r'(A|\{p_0\})}{\alpha} + \frac{\beta}{\alpha} r'(\{p_0\}) + r'(\{p_0\}) - \frac{\beta}{\alpha} r'(\{p_0\}) \\
&\leqslant \frac{r'(B|\{p_0\})}{\alpha} + r'(\{p_0\}) \\
&= r(B) \\
&= r(B \cup \{p_0\}).
\end{aligned}$$

For the sub-modularity property, we only check the sets $A, B \subseteq P$ where A, B and $A \cap B$ are unqualified and $A \cup B$ is qualified and other cases which are simpler are left to the reader. Since r' is sub-modular, we have $r'(A) + r'(B) \geqslant r'(A \cup B) + r'(A \cap B)$. Since $A \cup B$ is qualified, by definition of α we have $\alpha \leqslant \Delta_{r'}(\{p_0\} : A \cup B)/r'(\{p_0\})$, or equivalently, $r'(A \cup B) \geqslant r'(A \cup B|\{p_0\}) + \alpha r(p_0)$. We observe that

$$\begin{aligned} r(A) + r(B) &= r'(A)/\alpha + r'(B)/\alpha \\ &= \frac{1}{\alpha}[r'(A) + r'(B)] \\ &\geqslant \frac{1}{\alpha}[r'(A \cup B) + r'(A \cap B)] \\ &\geqslant \frac{1}{\alpha}[r'(A \cup B|\{p_0\}) + \alpha r'(p_0) + r'(A \cap B)] \\ &= \big(r'(A \cup B|\{p_0\})/\alpha + r'(p_0)\big) + \big(r'(A \cap B)/\alpha\big) \\ &= r(A \cup B) + r(A \cap B). \end{aligned}$$

Now, we show that $\mathcal{S}$ is a total polymatroid for Γ. For every qualified set $A \in \Gamma$, we have $r(A \cup \{p_0\}) = r(A)$ by definition of r. Also, for every unqualified set $B \in \Gamma^c$, we have $r(B \cup \{p_0\}) = r(B) + r(p_0)$. Therefore $\mathcal{S} = (P \cup \{p_0\}, r)$ is total for Γ.

It remains to show that $\mathrm{cv}(\mathcal{S}) = \mathrm{pcv}(\mathcal{S}')$. Therefore, by definition of r, we have $r(p) = r'(p)/\alpha$ for any participant $p \in P$ (we have assumed that no singleton set is qualified, but it is easy to remove this assumption). Thus,

$$\begin{aligned} \mathrm{cv}(\mathcal{S}) &= \frac{1}{r(\{p_0\})}\big(r(\{p\})\big)_{p \in P} \\ &= \frac{1}{\frac{\alpha-\beta}{\alpha} r'(\{p_0\})}\big(r'(\{p\})/\alpha\big)_{p \in P} \\ &= \frac{1}{(\alpha-\beta) r'(p_0)}(r'(p))_{p \in P} \\ &= \frac{1}{\delta}(r'(p))_{p \in P} \\ &= \mathrm{pcv}(\mathcal{S}') \end{aligned}$$

Consequently, $K_{\mathrm{p}}(\Gamma) \subseteq K_{\mathrm{t}}(\Gamma)$. □

6 On abelian information ratio

Equality of total and partial linear information ratios was proved in Section 4 and equality of Shannon lower bound with respect to these security notions was proved in Section 5. In this section, we provide some evidence that the abelian information ratios probably do not match.

We study $\mathcal{F} + \mathcal{N}$, a well-known 12-participant access structure [4, 38] which has both Fano ($\mathcal{F}$) and non-Fano ($\mathcal{N}$) access structures as minors. The access structure $\mathcal{F}$ (resp. $\mathcal{N}$) is the port of Fano (resp. non-Fano) matroid and it is known [38] to be ideal only on finite fields with even (resp. odd) characteristic. As a result, their union (i.e., $\mathcal{F}+\mathcal{N}$) is *nearly ideal*. That is, its information ratio is one without admitting an ideal scheme. Recently, in [27], the exact value of its linear information ratio has been determined (max= 4/3 and average= 41/36). Also, an upper-bound on its abelian information ratio has been provided (max$\leqslant$ 7/6 and average$\leqslant$ 41/36). Additionally, it has been conjectured in [27], that the exact value of its (total) abelian information ratio is strictly greater than one. Below, we show that the semi-partial abelian ramification ratio of this access structure is one.

Abelian schemes. An abelian scheme on a set P of participants is a collection $(G_i)_{i\in Q}$ of subgroups of a finite group G. An abelian scheme $\Pi = (G_i)_{i\in Q}$ realizes an access structure if 1) for every qualified set $A \subseteq P$ we have $G_0 \cap G_A = G_0$ and 2) for every unqualified set $A \subseteq P$ we have $G_0 \cap G_A = \{0\}$, where $G_A = \sum_{i\in A} G_i$.

The convec and access function of an abelian scheme $\Pi = (G_i)_{i\in Q}$ are computed as follows:

$$\Phi_\Pi(A) = \frac{\log|G_0 \cap G_A|}{\log|G_0|}\ , \qquad\qquad \mathrm{cv}(\Pi) = \big(\frac{\log|G_i|}{\log|G_0|}\big)_{i\in P}\ .$$

Every linear scheme is abelian. If $\Pi = (G_i)_{i\in Q}$ and $\Pi' = (G'_i)_{i\in Q}$ are abelian schemes for an access structure Γ, so is their direct sum $\Pi\oplus\Pi' = (G_i\oplus G'_i)_{i\in Q}$. In particular, if Π and Π' are linear schemes for Γ, then $\Pi\oplus\Pi'$ is an abelian scheme for Γ. The following corollary then becomes trivial. We refer to Appendix B or [27] for further discussion on abelian schemes.

Corollary 6.1 *For every even (resp. odd) number m, there exists an ideal abelian scheme for Fano (resp. non-Fano) access structure such that the order of all subgroups are m.*

A nearly ideal semi-partial abelian scheme for $\mathcal{F}+\mathcal{N}$. Let $k \in \mathbb{N}$ be an integer. Let $\Pi_k^{\mathcal{F}}$ (resp. $\Pi_k^{\mathcal{N}}$) be an ideal abelian scheme for $\mathcal{F}$ (resp. $\mathcal{N}$) whose subgroups all have order 2^k (resp. $2^k + 1$). We construct a nearly ideal semi-partial family of schemes $\{\Pi_k\}$ for $\mathcal{F}+\mathcal{N}$. Instead of describing the scheme Π_k using formal notation, we describe it informally. The secret space of Π_k is the direct sum of the secret spaces of $\Pi_k^{\mathcal{F}}$ and $\Pi_k^{\mathcal{N}}$, i.e., $G_0^{\mathcal{F}} \oplus G_0^{\mathcal{N}}$. To share a secret $(s^{\mathcal{F}}, s^{\mathcal{N}}) \in G_0^{\mathcal{F}} \oplus G_0^{\mathcal{N}}$, we share $s^{\mathcal{F}}$ via $\Pi_k^{\mathcal{F}}$ and share $s^{\mathcal{N}}$ via $\Pi_k^{\mathcal{N}}$, using independent randomnesses. It is easy see that Π_k is a semi-partial abelian scheme for $\mathcal{F}+\mathcal{N}$ and its information ratio converges to one as k goes to infinity.

Summary. Table 1 summarizes the known results on the $\mathcal{F}+\mathcal{N}$ access structure. We believe that, for the class of abelian schemes, computing the total information ratio of $\mathcal{F}+\mathcal{N}$ is reachable within known techniques (e.g., by manually using the *common information* method of [21] in a clever way), but as we will discuss in Section 7.2, computing its quasi-total abelian information ratio probably demands substantially more advanced ideas and techniques.

		total	quasi-total	(semi-)partial	reference
general	max	1			[4, 38]
	average				
abelian	max	$1 \leqslant \cdot \leqslant 7/6$	$1 \leqslant \cdot \leqslant 7/6$	1	[27]
	average	$1 \leqslant \cdot \leqslant 41/36$	$1 \leqslant \cdot \leqslant 41/36$		
linear	max	4/3			Theorems 4.1, Corollary 7.5
	average	41/36			[27], [3]

Table 1: Known results on the max/average information ratio of the access structure $\mathcal{F} + \mathcal{N}$ w.r.t. different security notions and different classes of schemes.

7 On quasi-total security

In this section, we review the notion of quasi-total security, proposed in [30, 31], though its connection to partial security notion. We prove that if partial and total information ratios coincide for any class of secret sharing schemes, the same thing happens for the total and quasi-total information ratios. As a corollary of Theorem 4.1, the partial, quasi-total and total information ratios are all equal for the class of linear schemes.

7.1 Definition

We need the following definition before giving a formal definition of the quasi-total secret sharing and quasi-total convec set.

Definition 7.1 (Convec-converging family of schemes) *A sequence $\mathcal{F} = \{\Pi_k\}_{k\in\mathbb{N}}$ of secret sharing schemes on participants set P is called a* convec-converging family of schemes *if i) the entropy of secret does not vanish; i.e., $\mathrm{H}(\boldsymbol{S}_0^k) = \Omega(1)$ and, ii) the sequence $\{\mathrm{cv}(\Pi_k)\}_{k\in\mathbb{N}}$ is converging. The convec of the convec-converging family $\mathcal{F}$ is defined as $\mathrm{cv}(\mathcal{F}) = \lim_{k\to\infty} \mathrm{cv}(\Pi_k)$.*

Definition 7.2 (Quasi-total realization [30]) *Let Γ be an access structure on P and $\mathcal{F} = \{\Pi_k\}_{k\in\mathbb{N}}$ be a convec-converging family of secret sharing schemes. We say that $\mathcal{F}$ is a quasi-total family for Γ if $\lim_{k\to\infty} \Phi_{\Pi_k} = \Phi_\Gamma$, where $\Phi_\Gamma : 2^P \to \{0, 1\}$ is a (monotone) mapping defined as $\Phi_\Gamma(A) = 1 \iff A \in \Gamma$.*

Definition 7.3 (Quasi-total convec set) *The quasi-total convec set of an access structure Γ, denoted by $\Sigma_{\mathrm{qt}}(\Gamma)$, is defined as the set of all convecs of all quasi-total families for Γ. When we restrict ourselves to the class C of secret sharing schemes, we use the notation $\Sigma_{\mathrm{qt}}^{\mathrm{C}}$.*

Notice that the quasi-total convec sets are closed. It is easy to prove that the Σ_{qt}-set (similar to the $\overline{\Sigma_{\mathrm{t}}}$-set) is convex, but recall that the closure convexity of the (semi-) partial convec set was left open.

7.2 Connections with partial and total security notions

We prove that if the partial and total convec sets are equal for some class of schemes, the same holds true for the quasi-total and total convec sets. It remains open if the reverse holds true as well.

Proposition 7.4 ($\overline{\boldsymbol{\Sigma}^{\mathbf{C}}_{\mathbf{p}}} = \overline{\boldsymbol{\Sigma}^{\mathbf{C}}_{\mathbf{t}}} \implies \boldsymbol{\Sigma}^{\mathbf{C}}_{\mathbf{qt}} = \overline{\boldsymbol{\Sigma}^{\mathbf{C}}_{\mathbf{t}}}$) *For any class* C *of schemes and any access structure Γ, if $\overline{\Sigma^{\mathrm{C}}_{\mathrm{p}}} = \overline{\Sigma^{\mathrm{C}}_{\mathrm{t}}}$ then $\Sigma^{\mathrm{C}}_{\mathrm{qt}} = \overline{\Sigma^{\mathrm{C}}_{\mathrm{t}}}$.*

Proof. It suffices to prove the inclusion $\Sigma^{\mathrm{C}}_{\mathrm{qt}}(\Gamma) \subseteq \overline{\Sigma^{\mathrm{C}}_{\mathrm{t}}(\Gamma)}$. Equivalently, we show that for every $\boldsymbol{\sigma} \in \Sigma^{\mathrm{C}}_{\mathrm{qt}}(\Gamma)$ we have $\boldsymbol{\sigma} \in \overline{\Sigma^{\mathrm{C}}_{\mathrm{t}}(\Gamma)}$. Let $\mathcal{F} = \{\Pi_k\}_{k\in\mathbb{N}}$ be a quasi-total family of class-C schemes for Γ with $\mathrm{cv}(\mathcal{F}) = \boldsymbol{\sigma}$. We construct a convec-converging family $\mathcal{F}' = \{\Pi'_k\}_{k\in\mathbb{N}}$ of class-C schemes such that: i) Π'_k is a total scheme for Γ for sufficiently large k and ii) $\mathrm{cv}(\mathcal{F}') = \boldsymbol{\sigma}$. This proves that $\boldsymbol{\sigma} \in \overline{\Sigma^{\mathrm{C}}_{\mathrm{t}}(\Gamma)}$.

Define $\lambda_k = \min_{A\in\Gamma}\{\Phi_{\Pi_k}(A)\}$ and $\omega_k = \max_{B\notin\Gamma}\{\Phi_{\Pi_k}(B)\}$. Since λ_k and ω_k respectively converge to 1 and 0, we have $\delta_k = \lambda_k - \omega_k > 0$ for sufficiently large k. This shows that Π_k is a partial class-C secret sharing scheme for Γ with partial convec $\mathrm{cv}(\Pi_k)/\delta_k$. By assumption, there exists a convec-converging family of class-C total schemes $\{\Pi'_{kj}\}_{j\in\mathbb{N}}$ for Γ with $\lim_{j\to\infty} \mathrm{cv}(\Pi'_{kj}) = \mathrm{cv}(\Pi_k)/\delta_k$. Let $\Pi'_k = \Pi'_{kk}$. Clearly, $\mathcal{F}' = \{\Pi'_k\}_{k\in\mathbb{N}}$ is a family of class-C total schemes for Γ with $\mathrm{cv}(\mathcal{F}') = \mathrm{cv}(\mathcal{F})$ since $\delta_k \to 1$, proving (i) and (ii). □

One of the main consequences of properties of partial security (Proposition 4.5), together with the above proposition, provides the following non-trivial corollary.

Corollary 7.5 ($\boldsymbol{\Sigma}^{\mathbf{L}}_{\mathbf{qt}} = \overline{\boldsymbol{\Sigma}^{\mathbf{L}}_{\mathbf{t}}}$) *For any access structure Γ and any prime p, we have $\Sigma^{p}_{\mathrm{qt}}(\Gamma) = \overline{\Sigma^{p}_{\mathrm{t}}(\Gamma)}$ and, consequently, $\Sigma^{\mathrm{L}}_{\mathrm{qt}}(\Gamma) = \overline{\Sigma^{\mathrm{L}}_{\mathrm{t}}(\Gamma)}$.*

It remains open if the claim of Corollary 7.5 holds for a class substantially larger than linear schemes. Even if it turns out that the partial and total convec sets do not coincide on some class larger than linear ones (e.g., the abelian ones which we guess to be the case and will discuss in Section 6), it does not provide sufficient evidence that this is also the case for total and quasi-total security notions. Therefore, we believe that proving coincidence/separation for larger classes demands innovative ideas and more advanced techniques.

8 On decomposition theorems

The (λ, ω)-weighted-decomposition theorem of [23] (as well as its predecessor [47]) has the following limitation. They require that in the linear sub-schemes every subset of participants fully recovers a certain subset of the secret elements and nothing more; in other words, recovering a non-trivial linear combination of the secret elements is not allowed.

In Section 8.1, we show that the above strong requirement on the (λ,ω)-weighted-decomposition can be removed. The main tool that allows us to do this is the notion of partial secret sharing and the result of Section 4 on the equality of partial and total linear information ratios.

In Section 8.2, we present a unified decomposition theorem, that we refer to as the δ-decomposition, which captures the advantages of the (λ,ω)-decomposition [17,49] and the (λ,ω)-weighted-decomposition [23] at one place. The theorem is essentially a restatement of known and folklore results. We introduce the notion of δ-decomposition, first, for the sake of completeness and, second, to provide the intuition behind the definition of partial security (Definition 3.1) and partial convec (Definition 3.2). The reader may compare those definitions with Definition 8.3.

Notation. In this section, we use the simplified notation Σ for total convec set and Λ (resp. Λ_p) for its restrictions to the class of all linear (resp. p-linear) schemes. We remark that the linear convec set of a (rational-valued) access function Φ is defined as the set of all convecs of all linear secret sharing schemes whose access function is Φ.

8.1 $(\boldsymbol{\lambda},\boldsymbol{\omega})$-weighted-decomposition revisited

The following definition is a restatement of Definition 3.4 in [23].

Definition 8.1 ($(\boldsymbol{\lambda},\boldsymbol{\omega})$–weighted decomposition) *Let $\lambda,\omega,N,m_1,\cdots,m_N$, be non-negative integers, with $0 \leqslant \omega < \lambda$. Let Γ be an access structure and $\Phi_1,\ldots,\Phi_N$ be (rational) access functions all defined on the same participants set and further assume that $m_j\Phi_j$ is an integer-valued function for every $j \in [N]$. We call $(m_1,\Phi_1),\ldots,(m_N,\Phi_N)$ a (λ,ω)-weighted-decomposition for Γ if the following two hold:*

- $\sum_{j=1}^{N} m_j\Phi_j(A) \geqslant \lambda$, *for every qualified set $A \in \Gamma$,*
- $\sum_{j=1}^{N} m_j\Phi_j(B) \leqslant \omega$, *for every unqualified set $B \in \Gamma^c$.*

The following decomposition theorem is an extension of Theorem 3.2 in [23], which was stated for a subclass of linear schemes. The proof essentially relies on Proposition 4.5

Theorem 8.2 ($(\boldsymbol{\lambda},\boldsymbol{\omega})$–weighted decomposition) *Let p be a prime. Consider a (λ,ω)-weighted-decomposition $(m_1,\Phi_1),\ldots,(m_N,\Phi_N)$ for an access structure Γ and let $\boldsymbol{\sigma}_j \in \Lambda_p(\Phi_j)$, $j \in [N]$. Then, $\frac{1}{\lambda-\omega}\sum_{j=1}^{N} m_j\boldsymbol{\sigma}_j \in \Lambda_p(\Gamma)$.*

Proof. Let $\Pi_j = (T_{ij})_{i\in P}$ be a p-linear secret sharing scheme for Φ_j with convec $\boldsymbol{\sigma}_j$, for $j \in [N]$. Without loss of generality, we assume that all sub-schemes are $\mathbb{F}$-linear for a common finite field $\mathbb{F}$ with characteristic p. Let $T_i' = \oplus_{j\in[N]}T_{ij}$, for every $i \in P$. For every $i \in P$, we have $\dim T_i' = \sum_{j\in[N]}\dim T_{ij}$ which implies that

$$\big(\dim T_i'\big)_{i\in P} = \textstyle\sum_{j=1}^{N} m_j \boldsymbol{\sigma}_j \ .$$

Also, for every subset A of participants, it holds that:

$$\begin{aligned}\dim(T_A' \cap T_0') &= \textstyle\sum_{j\in[N]} \dim(T_A \cap T_0)\\ &= \textstyle\sum_{j\in[N]} m_j \varPhi_{\varPi_j}(A)\\ &= \textstyle\sum_{j\in[N]} m_j \varPhi_j(A)\ .\end{aligned}$$

By definition of the (λ,ω)–weighted decomposition, we have

$$\varDelta = \min_{A\in\varGamma} \dim(T_A' \cap T_0') - \max_{B\in\varGamma^c} \dim(T_B' \cap T_0') \geqslant \lambda - \omega\ .$$

Consequently, $\varPi' = (T_i')_{i\in P}$ is an $\mathbb{F}$-linear partial secret sharing scheme for $\varGamma$ with the following partial convec:

$$\mathrm{pcv}(\varPi') = \frac{1}{\varDelta}\sum_{j=1}^{N} m_j \boldsymbol{\sigma}_j\ .$$

Then, by Proposition 4.5, there exists a finite extension $\mathbb{K}$ of $\mathbb{F}$, such that $\varGamma$ has a total $\mathbb{K}$-linear scheme $\varPi$ with the above convec. It is straightforward to modify the scheme to have a scheme with the convec $\frac{1}{\lambda-\omega}\sum_{j=1}^{N} m_j\boldsymbol{\sigma}_j$. □

8.2 δ-decomposition

We present the notion of δ-decomposition, which captures all the weighted [23,47] and non-weighted [17, 45] decompositions simultaneously, and even in a more general form. It also justifies the intuition behind the definition of partial security (Definition 3.1) and partial convec (Definition 3.2).

Definition 8.3 (δ-decomposition) *Let N be an integer and $\delta, h_1, \dots, h_N$ be positive real numbers. Let $\varGamma$ be an access structure and $\varPhi_1, \dots, \varPhi_N$ be access functions all on participants set P. We say that $(h_1, \varPhi_1), \dots, (h_N, \varPhi_N)$ is a δ–decomposition for $\varGamma$ if*

$$\delta = \min_{A\in\varGamma} \sum_{j=1}^{N} h_j\varPhi_j(A) - \max_{B\in\varGamma^c} \sum_{j=1}^{N} h_j\varPhi_j(B)\ .$$

The proof of the following theorem is easy and we leave it to the reader.

Theorem 8.4 (δ-decomposition) *Let $\varGamma$ be an access structure and consider a δ–decomposition $(h_1, \varPhi_1), \dots, (h_N, \varPhi_N)$ for it. Then, the followings hold:*

(i) ***(Rational sub-access functions)*** *Let p be a prime, $\varPhi_j$ be rational and $\boldsymbol{\sigma}_j \in \overline{\varLambda_p(\varPhi_j)}$, for every $j \in [N]$. Then $\boldsymbol{\sigma} = \frac{1}{\delta}\sum_{j=1}^{N} h_j\boldsymbol{\sigma}_j \in \overline{\varLambda_p(\varGamma)}$.*

(ii) ***(Total sub-access functions)*** *Let $\varPhi_j$ be total and $\boldsymbol{\sigma}_j \in \overline{\varSigma(\varPhi_j)}$, for every $j \in [N]$. Then, $\boldsymbol{\sigma} = \frac{1}{\delta}\sum_{j=1}^{N} h_j\boldsymbol{\sigma}_j \in \overline{\varSigma(\varGamma)}$.*

9 Conclusion

In this paper, we introduced a new relaxed security notion for secret sharing schemes, called partial security. Even though, partial security may not be suitable for practical applications, it turned out to be useful to close some gaps in our knowledge about secret sharing schemes. In particular, partial security was the missing ingredient for proving coincidence of quasi-total and total linear information ratios. Also, it helped us to remove a strong requirement that were needed for the linear sub-schemes in the weighted decompositions.

It remains challengingly an open problem that for which classes of schemes the partial (resp. quasi-total) and total information ratios coincide. It also remains open for which classes of information inequalities, the lower bound on partial and total information ratios coincide. We proved that partial and total information ratios coincide with respect to linear upper-bound and Shannon lower-bound. We conjecture that the partial and total information ratios probably do not coincide for the class of abelian schemes and provided some evidence to support our conjecture. However, it remains much harder to say something about separation/coincidence of quasi-total and total information ratios with respect to abelian schemes.

References

1. Applebaum, B., Arkis, B.: On the power of amortization in secret sharing: d-uniform secret sharing and CDS with constant information rate. In: Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part I. pp. 317–344 (2018). https://doi.org/10.1007/978-3-030-03807-6_12, https://doi.org/10.1007/978-3-030-03807-6_12
2. Beimel, A.: Secret-sharing schemes: A survey. In: Coding and Cryptology - Third International Workshop, IWCC 2011, Qingdao, China, May 30-June 3, 2011. Proceedings. pp. 11–46 (2011), http://dx.doi.org/10.1007/978-3-642-20901-7_2
3. Beimel, A., Ishai, Y.: On the power of nonlinear secret-sharing. In: Proceedings of the 16th Annual IEEE Conference on Computational Complexity, Chicago, Illinois, USA, June 18-21, 2001. pp. 188–202 (2001), https://doi.org/10.1109/CCC.2001.933886
4. Beimel, A., Livne, N.: On matroids and nonideal secret sharing. IEEE Trans. Information Theory **54**(6), 2626–2643 (2008), https://doi.org/10.1109/TIT.2008.921708
5. Beimel, A., Livne, N., Padró, C.: Matroids can be far from ideal secret sharing. In: Theory of Cryptography, Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008. pp. 194–212 (2008). https://doi.org/10.1007/978-3-540-78524-8_12, https://doi.org/10.1007/978-3-540-78524-8_12
6. Beimel, A., Orlov, I.: Secret sharing and non-shannon information inequalities. IEEE Trans. Information Theory **57**(9), 5634–5649 (2011), https://doi.org/10.1109/TIT.2011.2162183
7. Beimel, A., Weinreb, E.: Separating the power of monotone span programs over different fields. SIAM J. Comput. **34**(5), 1196–1215 (2005).

https://doi.org/10.1137/S0097539704444038, https://doi.org/10.1137/S0097539704444038

8. Bertilsson, M., Ingemarsson, I.: A construction of practical secret sharing schemes using linear block codes. In: Advances in Cryptology - AUSCRYPT '92, Workshop on the Theory and Application of Cryptographic Techniques, Gold Coast, Queensland, Australia, December 13-16, 1992, Proceedings. pp. 67–79 (1992), https://doi.org/10.1007/3-540-57220-1_53
9. Blakley, G.R.: Safeguarding cryptographic keys. Proc. of the National Computer Conference1979 **48**, 313–317 (1979)
10. Blakley, G.R., Meadows, C.: Security of ramp schemes. In: Workshop on the Theory and Application of Cryptographic Techniques. pp. 242–268. Springer (1984)
11. Blundo, C., Santis, A.D., Stinson, D.R., Vaccaro, U.: Graph decompositions and secret sharing schemes. In: Advances in Cryptology - EUROCRYPT '92, Workshop on the Theory and Application of of Cryptographic Techniques, Balatonfüred, Hungary, May 24-28, 1992, Proceedings. pp. 1–24 (1992), http://dx.doi.org/10.1007/3-540-47555-9_1
12. Blundo, C., Santis, A.D., Vaccaro, U.: On secret sharing schemes. Inf. Process. Lett. **65**(1), 25–32 (1998), http://dx.doi.org/10.1016/S0020-0190(97)00194-4
13. Brickell, E.F., Stinson, D.R.: Some improved bounds on the information rate of perfect secret sharing schemes. J. Cryptology **5**(3), 153–166 (1992), http://dx.doi.org/10.1007/BF02451112
14. Chan, T.H., Yeung, R.W.: On a relation between information inequalities and group theory. IEEE Trans. Information Theory **48**(7), 1992–1995 (2002), https://doi.org/10.1109/TIT.2002.1013138
15. Cover, T.M., Thomas, J.A.: Elements of information theory (2. ed.). Wiley (2006)
16. Csirmaz, L.: The size of a share must be large. J. Cryptology **10**(4), 223–231 (1997), https://doi.org/10.1007/s001459900029
17. van Dijk, M., Jackson, W., Martin, K.M.: A general decomposition construction for incomplete secret sharing schemes. Des. Codes Cryptography **15**(3), 301–321 (1998), https://doi.org/10.1023/A:1008381427667
18. van Dijk, M., Kevenaar, T.A.M., Schrijen, G.J., Tuyls, P.: Improved constructions of secret sharing schemes by applying (lambda, omega)-decompositions. Inf. Process. Lett. **99**(4), 154–157 (2006). https://doi.org/10.1016/j.ipl.2006.01.016, https://doi.org/10.1016/j.ipl.2006.01.016
19. Edmonds, J.: Submodular functions, matroids, and certain polyhedra. Combinatorial structures and their applications pp. 69–87 (1970)
20. Farràs, O., Hansen, T.B., Kaced, T., Padró, C.: On the information ratio of non-perfect secret sharing schemes. Algorithmica **79**(4), 987–1013 (2017). https://doi.org/10.1007/s00453-016-0217-9, https://doi.org/10.1007/s00453-016-0217-9
21. Farràs, O., Kaced, T., Molleví, S.M., Padró, C.: Improving the linear programming technique in the search for lower bounds in secret sharing. In: Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I. pp. 597–621 (2018), https://doi.org/10.1007/978-3-319-78381-9_22
22. Fujishige, S.: Polymatroidal dependence structure of a set of random variables. Information and Control **39**(1), 55–72 (1978). https://doi.org/10.1016/S0019-9958(78)91063-X, https://doi.org/10.1016/S0019-9958(78)91063-X

23. Gharahi, M., Khazaei, S.: Optimal linear secret sharing schemes for graph access structures on six participants. Theoretical Computer Science (2018), https://doi.org/10.1016/j.tcs.2018.11.007
24. Gharahi, M., Khazaei, S.: Reduced access structures with four minimal qualified subsets on six participants. Advances in Mathematics of Communications **12**(1), 199–214 (2018)
25. Ito, M., Saito, A., Nishizeki, T.: Secret sharing scheme realizing general access structure. Electronics and Communications in Japan (Part III: Fundamental Electronic Science) **72**(9), 56–64 (1989)
26. Jackson, W.A., Martin, K.M.: Perfect secret sharing schemes on five participants. Designs, Codes and Cryptography **9**(3), 267–286 (1996)
27. Jafari, A., Khazaei, S.: On abelian secret sharing: duality and separation. Cryptology ePrint Archive, Report 2019/575 (2019), https://eprint.iacr.org/2019/575
28. Jafari, A., Khazaei, S.: On relaxed security notions for secret sharing. IACR Cryptology ePrint Archive **2019**, ?? (2019)
29. Kaboli, R., Khazaei, S., Parviz, M.: Group-homomorphic secret sharing schemes are group-characterizable with normal subgroups. Cryptology ePrint Archive, Report 2019/576 (2019), https://eprint.iacr.org/2019/576
30. Kaced, T.: Almost-perfect secret sharing. In: 2011 IEEE International Symposium on Information Theory Proceedings, ISIT 2011, St. Petersburg, Russia, July 31 - August 5, 2011. pp. 1603–1607 (2011), https://doi.org/10.1109/ISIT.2011.6033816
31. Kaced, T.: Secret Sharing and Algorithmic Information Theory. (Partage de secret et the'orie algorithmique de l'information). Ph.D. thesis, Montpellier 2 University, France (2012), https://tel.archives-ouvertes.fr/tel-00763117
32. Khazaei, S.: Conjecturally superpolynomial lower bound for share size. Cryptology ePrint Archive, Report 2018/143 (2018), https://eprint.iacr.org/2018/143
33. Kurosawa, K., Okada, K., Sakano, K., Ogata, W., Tsujii, S.: Nonperfect secret sharing schemes and matroids. In: Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings. pp. 126–141 (1993), https://doi.org/10.1007/3-540-48285-7_11
34. Li, Q., Li, X.X., Lai, X.J., Chen, K.F.: Optimal assignment schemes for general access structures based on linear programming. Designs, Codes and Cryptography **74**(3), 623–644 (2015)
35. Martí-Farré, J., Padró, C.: On secret sharing schemes, matroids and polymatroids. J. Mathematical Cryptology **4**(2), 95–120 (2010), https://doi.org/10.1515/jmc.2010.004
36. Martí-Farré, J., Padró, C., Vázquez, L.: Optimal complexity of secret sharing schemes with four minimal qualified subsets. Designs, Codes and Cryptography **61**(2), 167–186 (2011)
37. Martin, K.M.: New secret sharing schemes from old. J. Combin. Math. Combin. Comput **14**, 65–77 (1993)
38. Matús, F.: Two constructions on limits of entropy functions. IEEE Trans. Information Theory **53**(1), 320–330 (2007), https://doi.org/10.1109/TIT.2006.887090
39. Molleví, S.M., Padró, C., Yang, A.: Secret sharing, rank inequalities, and information inequalities. IEEE Trans. Information Theory **62**(1), 599–609 (2016), https://doi.org/10.1109/TIT.2015.2500232
40. Padró, C.: Lecture notes in secret sharing. IACR Cryptology ePrint Archive **2012**, 674 (2012), http://eprint.iacr.org/2012/674

41. Rogers, R.M., Roth, A., Smith, A.D., Thakkar, O.: Max-information, differential privacy, and post-selection hypothesis testing. In: IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016, 9-11 October 2016, Hyatt Regency, New Brunswick, New Jersey, USA. pp. 487–494 (2016). https://doi.org/10.1109/FOCS.2016.59, https://doi.org/10.1109/FOCS.2016.59
42. Seymour, P.D.: On secret-sharing matroids. J. Comb. Theory, Ser. B **56**(1), 69–73 (1992). https://doi.org/10.1016/0095-8956(92)90007-K, https://doi.org/10.1016/0095-8956(92)90007-K
43. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979), http://doi.acm.org/10.1145/359168.359176
44. Srinathan, K., Rajan, N.T., Rangan, C.P.: Non-perfect secret sharing over general access structures. In: Progress in Cryptology - INDOCRYPT 2002, Third International Conference on Cryptology in India, Hyderabad, India, December 16-18, 2002. pp. 409–421 (2002), https://doi.org/10.1007/3-540-36231-2_32
45. Stinson, D.R.: An explication of secret sharing schemes. Des. Codes Cryptography **2**(4), 357–390 (1992), http://dx.doi.org/10.1007/BF00125203
46. Stinson, D.R.: Decomposition constructions for secret-sharing schemes. IEEE Transactions on Information Theory **40**(1), 118–125 (1994)
47. Sun, H.M., Chen, B.L.: Weighted decomposition construction for perfect secret sharing schemes. Computers & Mathematics with Applications **43**(6), 877–887 (2002)
48. Van Dijk, M.: On the information rate of perfect secret sharing schemes. Designs, Codes and Cryptography **6**(2), 143–169 (1995)
49. Van Dijk, M., Jackson, W.A., Martin, K.M.: A general decomposition construction for incomplete secret sharing schemes. Designs, Codes and Cryptography **15**(3), 301–321 (1998)
50. Zhang, Z., Yeung, R.W.: A non-shannon-type conditional inequality of information quantities. IEEE Trans. Information Theory **43**(6), 1982–1986 (1997), https://doi.org/10.1109/18.641561

A A probabilistic proof of Lemma 4.3 for $N < \frac{q-1}{q^{m-w}-1}\frac{q^m-1}{q^w-1}$

Without loss of generality we can assume that $\dim E_i = \omega$. Let $\mathbb{F}$ be the underlying finite field with q elements. Given a random subspace S of dimension $m-w$ there are exactly $\frac{q^{m-w}-1}{q-1}$ lines in S through the origin. For a given random line, the probability that it lies inside a subspace E_i of dimension w is $(q^w-1)/(q^m-1)$. Therefore, by the union bound, the probability that at least one of the lines in S is inside E_i is at most

$$\frac{q^{m-w}-1}{q-1}\frac{q^w-1}{q^m-1} .$$

Hence if $N < \frac{q-1}{q^{m-w}-1}\frac{q^m-1}{q^w-1}$, the probability that S has a non-trivial intersection with one of these subspaces is less than 1 and hence there exists a subspace of dimension $m-w$ that has zero intersection with all of the E_i's.

Notice that if $w=1$, this bound coincides with the bound $N < \frac{q^m-1}{q^{m-1}-1}$ of Lemma 4.3, proved using a non-probabilistic argument. Even though the bound of Lemma 4.3 is better in general, the difference is negligible (the maximum happens at $w = m/2$).

B Abelian and linear secret sharing

A group-characterizable scheme [14] is defined as follows.

Definition B.1 (Group-characterizable scheme [14]) *A tuple* $\varPi = (G : G_0, G_1, \ldots, G_n)$ *is called a group-characterizable secret sharing scheme if* G *is a finite group,* G_i *is a subgroup of* G*, for each* $i \in [n]$*, and* $|G|/|G_0| \geqslant 2$*.*

A group-characterizable scheme $\varPi = (G : G_0, G_1, \ldots, G_n)$ induces a secret sharing scheme $(\boldsymbol{S}_0, \boldsymbol{S}_1, \ldots, \boldsymbol{S}_n)$ by letting $\boldsymbol{S}_i = \boldsymbol{X} G_i$, where $\boldsymbol{X}$ is a uniform random variable on G; hence, the support of $\boldsymbol{S}_i$ is the left cosets of G_i.

A group-characterizable scheme $\varPi = (G : G_0, G_1, \ldots, G_n)$ is called *abelian* if its main group G is abelian. It is easy to show that (e.g., see [27]) every abelian scheme $\varPi = (G : G_0, G_1, \ldots, G_n)$, with respect to this definition induces an abelian scheme $\varPi' = (G'; G'_0, G_1, \ldots, G'_n)$, with respect to the following definition, and vice versa, with the same access function and convec.

Definition B.2 (Abelian scheme) *A tuple* $\varPi = (G; G_0, G_1, \ldots, G_n)$ *is called an abelian secret sharing scheme if* G *is a finite abelian group,* G_i *is a subgroup of* G*, for each* $i \in [n]$*, and* $|G_0| \geqslant 2$*. When there is no confusion, we simply write* $\varPi = (G_i)_{i \in P \cup \{0\}}$*.*

Definition B.3 (Linear scheme) *When* T *is a finite dimensional vector space on some finite field and* $T_0, T_1, \ldots, T_n$ *are sup-spaces of* T*, the abelian secret sharing scheme* $\varPi = (T; T_0, T_1, \ldots, T_n)$ *is called linear.*

Table 2 shows the simplified access functions and convecs for different types of schemes.

type	$\varPi$	$\varPhi_{\varPi}(A)$	$\mathrm{cv}(\varPi)$	notation
group char.	$(G : G_0, G_1, \ldots, G_n)$	$\dfrac{\log\left(\lvert G\rvert/\lvert G_A * G_0\rvert\right)}{\log\left(\lvert G\rvert/\lvert G_0\rvert\right)}$	$\left(\dfrac{\log\left(\lvert G\rvert/\lvert G_i\rvert\right)}{\log\left(\lvert G\rvert/\lvert G_0\rvert\right)}\right)_{i \in [n]}$	$G_A = \bigcap_{i \in A} G_i$
abelian	$(G; G_0, G_1, \ldots, G_n)$	$\dfrac{\log \lvert G_0 \cap G_A\rvert}{\log \lvert G_0\rvert}$	$\left(\dfrac{\log \lvert G_i\rvert}{\log \lvert G_0\rvert}\right)_{i \in [n]}$	$G_A = \sum_{i \in A} G_i$
linear	$(T; T_0, T_1, \ldots, T_n)$	$\dfrac{\dim(T_0 \cap T_A)}{\dim(T_0)}$	$\left(\dfrac{\dim(T_i)}{\dim(T_0)}\right)_{i \in [n]}$	$T_A = \sum_{i \in A} T_i$

Table 2: The access function and convec of different scheme types.