On Abelian and Homomorphic Secret Sharing Schemes

Amir Jafari and Shahram Khazaei

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

Abstract. Abelian secret sharing schemes (SSS) are generalization of multi-linear SSS and similar to them, abelian schemes are homomorphic. There are numerous results on linear and multi-linear SSSs in the literature and a few ones on homomorphic SSSs too. Nevertheless, the abelian schemes have not taken that much attention. We present three main results on abelian and homomorphic SSSs in this paper: (1) abelian schemes are more powerful than multi-linear schemes (we achieve a constant factor improvement), (2) the information ratio of dual access structures are the same for the class of abelian schemes, and (3) every ideal homomorphic scheme can be transformed into an ideal multi-linear scheme with the same access structure.
Our results on abelian and homomorphic SSSs have been motivated by the following concerns and questions. All known linear rank inequities have been derived using the so-called common information property of random variables [Dougherty, Freiling and Zeger, 2009], and it is an open problem that if common information is complete for deriving all such inequalities (Q1). The common information property has also been used in linear programming to find lower bounds for the information ratio of access structures [Farràs, Kaced, Molleví and Padró, 2018] and it is an open problem that if the method is complete for finding the optimal information ratio for the class of multi-linear schemes (Q2). Also, it was realized by the latter authors that the obtained lower bound does not have a good behavior with respect to duality and it is an open problem that if this behavior is inherent to their method (Q3).
Our first result provides a negative answer to Q2. Even though, we are not able to completely answer Q1 and Q3, we have some observations about them.

Keywords: Secret sharing· Information theory · Linear rank inequality · Homomorphic secret sharing · Duality.

1 Introduction

A *secret sharing scheme* (SSS) [15, 51] is used to share a secret among a set of participants by giving a share to each one. The most common security definition of a SSS is that of *prefect* realization. In a perfect scheme, only certain prespecified subsets of participants are qualified to recover the secret. Every other

subset of participants must not gain any information on the secret. The set of all qualified subsets is called an *access structure* [39].

The most common type of SSS is the class of *multi-linear* schemes. In these schemes, the secret is composed of some finite field elements and the sharing is done by applying some fixed linear mapping on the secret elements and some randomly chosen elements from the finite field. When the secret is a single field element, the scheme is called *linear* in the literature.

A SSS is said to be *ideal* if every participants share size is equal to the secret size. An access structure is said to be ideal if it admits a (perfect) ideal scheme. Ideal access structures are the most desirable ones, since in perfect SSSs every share size is at least as large as the secret size [44]. Ideal SSSs are closely related to matroids and this connection was realized in early seminal works [17, 18, 50]. Classification of ideal access structures, except in very few cases (e.g., [1, 18]), is still an open problem.

The efficiency of a SSS is measured by its *information ratio*, defined as the ratio between the largest share size (entropy) and the secret size. The information ratio of an access structure is the infimum of all information ratios of all SSSs for that access structure. Computation of the optimal information ratio has turned out to be a challenging problem.

There is a natural notion of *duality* for access structures [40] and more generally access functions [27]. The relation between the information ratios of dual access structures is a long standing open problem. This problem is even open for the class of ideal access structures. However, it is known that the information ratios of dual access structures are the same for the class of multi-linear SSSs [40].

Several techniques have been devised for finding lower bounds for the information ratio of access structures during the past three decades. One important category of such techniques employs the so-called *information inequalities* to derive a lower bound, which applies to general SSSs. This method was first used by Capocelli, De Santis, Gargano and Vaccaro [19] and was later refined and formalizes by Csirmaz in [21]. It was noticed in [12] that, by taking into account the *linear rank inequalities* [25, 38], instead of the so-called non-Shanon type information inequalities [57], a lower bound can be found for multi-linear SSSs.

A SSS is said to be *homomorphic* [14], if the secret and share spaces have group structures and, additionally, it has the following property: the product of the shares of a participant produces a share for the product of their corresponding secrets. Our understanding of homomorphic SSSs is very limited and their characterization, even for the case of ideal homomorphic schemes, is an open problem. A few results are known about homomorphic SSSs. Frankel, Desmedt and Burmester [30] have proved that the secret space of every homomorphic scheme is an abelian group. In a subsequent work, Frankel and Desmedt [29] showed that, when the scheme is ideal, the share spaces are all isomorphic to the secret space, and hence abelian too. In a recent work [42], it has been proved that homomorphic SSSs are equivalent to the so-called group-characterizable random variables with normal subgroups, which will be defined in next paragraph.

Secret sharing as random variables. A SSS is usually defined as a probabilistic algorithm that given the secret computes the shares. By considering a probability distribution on the secret space, a SSS can equivalently be considered as a joint distribution of the secret and shares. In this paper, we study different classes of SSSs as special cases of random variables. In particular, all classes of SSSs which are studied in this paper (including multi-linear, abelian and homomorphic) can be considered as subclasses of *group-characterizable* random variables. A group-characterizable random variable, introduced by Chan and Yeung in [20], is a vector of jointly distributed random variables $(\mathbf{g}G_1, \ldots, \mathbf{g}G_n)$ on the left cosets of subgroups $G_1, \ldots, G_n$ of a finite group G, called the *main group*, where $\mathbf{g}$ is a uniform random variable on G. We say that a group-characterizable scheme is multi-linear if the main group is a vector space. This definition is equivalent to two other more common definitions of multi-linear SSS in the literature[1]. It is called *abelian* if the main group is abelian. Furthermore, homomorphic schemes are equivalent to group-characterizable schemes whose subgroups are *normal* in the main group [42]. Therefore, multi-linear schemes are abelian and abelian schemes are homomorphic.

On the power of different classes of schemes. Simonis and Ashikhmin [52] have shown that multi-linear SSSs are more powerful than linear schemes by studying the access structure induced by the Non-Pappus matroid. The first indication of superiority of general schemes to linear schemes was provided by Beimel and Ishai [9] as their result was valid assuming some plausible number-theoretic assumption holds true. Later, Beimel and Weinreb [13] proved the result without relying on any assumption. To the best of our knowledge, there is no result on the power of abelian and homomorphic SSSs; nor any result on superiority of general secret sharing to multi-linear schemes.

1.1 Motivations and results

The contributions of this paper have been inspired by the following two main motivations.

First motivation. A linear rank inequality (LRI) [38] is an inequality of the form $\sum_A c_A \mathrm{H}(\boldsymbol{X}_A) \geqslant 0$ that holds for every linear random variable $(\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n)$ where $\boldsymbol{X}_A = (\boldsymbol{X}_i)_{i \in A}$, H is the Shannon entropy function, and c_A's are real coefficients. All Shannon type information inequalities are LRIs and the first example of non-Shannon type LRI was found by Ingleton [38] in 1971. LRIs can be used to provide lower bounds on the information ratio for the class of multi-linear SSSs. Dougherty, Freiling and Zeger [25] have used the so-called *common information* (CI) property of random variables—first defined by Gács and Körner [31] in 1973—to develop a method for deriving LRIs, which is called the *DFZ method* in this paper. All known LRIs have been derived using the DFZ method. The

[1] One definition is based on a collection of linear maps and the other one is the so-called (multi-target) monotone span program [43].

DFZ method has successfully derived all LRIs up to five variables [25] and so far millions of LRIs on six variables [24] have been found. The following question has been explicitly raised in the conclusion of [25]: *Is the DFZ method complete for determining all linear rank inequalities?*

A related question can be asked in the context of SSSs. In Eurocrypt 2018 [28], Farràs, Kaced, Molleví and Padró used the CI property in a clever way in an improved linear programing and introduced a new lower bound technique, which we call *FKMP method* in this paper. The obtained lower bound by FKMP method applies not only to multi-linear SSSs, but also to a larger class that includes the abelian schemes. Using the FKMP method, the authors were able to determine the optimal "multi-linear information ratio"[2] of several small access structures which had remained open for a long time. The following question is then natural to ask: *Is the FKMP method complete for determining the optimal multi-linear information ratio of access structures?*

We noticed that in order to show the incompleteness of the FKMP method, it is enough to show that abelian SSSs are superior to multi-linear schemes. However, the incompleteness of the DFZ method remains unanswered.

First result. We prove that abelian SSSs (in particular mixed-linear ones to be defined below) outperform multi-linear schemes. Consequently, the FKMP method is incomplete for computing the optimal multi-linear information ratio of access structures. We remark that we achieve only a constant factor gain and it remains open if the class of abelian schemes contains schemes except for mix-linear schemes, or a supper constant gain can be achieved. Note that historically many improvements have first been achieved only with constant gain and much later supper constant gains have been derived (one notable example is the case of multi-linear secret sharing which will be discussed in Section 1.3).

We construct abelian schemes by mixing several multi-linear SSSs, possibly with different field characteristics, and we refer to such schemes as *mixed-linear*. The share space of a mixed-linear scheme is the product of the share spaces of the underlying multi-linear schemes. To share a secret, we share each component independently using its corresponding multi-linear scheme. Mixed-linear schemes are abelian.

It remains open if there is any better way to construct abelian schemes; that is, if abelian SSSs could be superior over mixed-linear schemes. This problem will be formalized using the concept of *convec set* for access structures. Convec is short for *contribution vector* and the convec of a SSS is a vector formed by all participants share sizes divided by the secret size. The convec set of an access structure contains convecs of all perfect SSSs realizing the access structure. It is a more general parameter than the information ratio and, as we will see in the paper, it is useful for studying the *entropy region* [57].

[2] By the multi-linear (resp. abelian) information ratio of an access structure, we mean its information ratio when restricted to the class of multi-linear (resp. abelian) schemes.

Second motivation. Despite the fact that dual access structures have the same multi-linear information ratio, the authors of [28] sometimes had to apply the FKMP method to the dual of an access structure as well. The reason was that the technique did not result in the same value for dual access structures. Consequently, it was left open if the FKMP method has a good behavior with respect to duality or not. In other words, it was left open if the misbehavior is inherent to the method. A potential negative answer can be justified due to the following fact. The FKMP method integrates the properties of the CI of random variables in a linear programing for computing a lower bound on the information ratio. Therefore, the bound applies not only to multi-linear SSSs but also to any class of schemes that satisfies the CI property. The CI property is known to hold for abelian schemes too [28, Remark 3.7]. In this paper, using properties of finite groups, we identify a subclass of group-characterizable schemes that satisfies the CI property; additionally, we show that the homomorphic schemes are included in this class. That is, the CI property holds not only for abelian, but also for homomorphic schemes and even larger classes. It is then natural to ask the following two questions: *Do the dual access structures have the same information ratios for the class of abelian schemes? How about the class of homomorphic schemes?* A negative answer to any of these questions would be a proof of inherent misbehavior of the FKMP method with respect to duality. Even though we do not have much to say about the duality of homomorphic SSSs (except for the case of ideal schemes which follows by our third result), we show that the answer is positive for duality of abelian SSSs.

Second result. We extend the result on duality of multi-linear secret sharing [27, 40] to the class of abelian schemes. In other words, we show that the abelian information ratios of dual access structures are the same.

As we mentioned above, it remains open if our result on duality of abelian schemes can be extended to homomorphic schemes. However, we show that the duality of homomorphic schemes holds for the special case of ideal homomorphic schemes. In particular, we prove the following result which is of independent interest (note: it is a long standing open problem if any ideal scheme can be converted into an ideal multi-linear scheme with the same access structure [52]).

Third result. Every ideal homomorphic SSS can be (constructively) transformed into a multi-linear ideal SSS for the same access structure.

As we mentioned above, it remains open if abelian schemes are superior over mixed-linear schemes. It also remains open if homomorphic schemes are superior over abelian schemes. If the answer to any of these problems is negative, we will show that the DFZ method is not complete for deriving all LRIs.

1.2 Ideas and techniques

The results of this paper are based on—but not limited to—the following main ideas and techniques.

- **A new lower bound technique.** Our main idea to achieve our first result—i.e., superiority of abelian SSSs to mixed-linear ones—is to look for an access structure whose multi-linear information ratio depends on the characteristic of the underlaying finite field. To this end, we develop *a new lower-bound technique* that can be applied to multi-linear schemes over finite fields with a *specific characteristic*. We then apply our method to the *Fano* and *non-Fano* access structures and determine the exact value of their characteristic-dependent information ratios. Next, we consider the union of Fano and non-Fano access structures, which is a well-known 12-participant access structure and has already been studied in [11, 47]. It is non-ideal, but its information ratio is one and there is no result on its multi-linear information ratio. We determine the exact value of its multi-linear and mixed-linear information ratios. The latter one turns out to be smaller than the first one; therefore, an upper bound on its abelian information ratio is found too. To the best of our knowledge, none of the known techniques in the literature—including [13] which also takes the characteristic into account—could have been used to achieve our result.
  Our lower bound technique is purely algebraic. Two linear algebraic lemmas, that we call the *minimal subspace lemma* (Lemma 4.1) and the *kernel lemma* (Lemma 4.3), in companion with other concepts from linear algebra, lie at the heart of our method. To derive a non-trivial lower bound, we consider a collection of minimal subspaces, associated to different minimal qualified sets, and use certain notions from linear algebra to show that the sum of dimensions of their intersections has a non-trivial upper bound. To do this, often the characteristic of the underlying finite field plays a crucial role.
- **An equivalent definition of abelian schemes.** A multi-linear SSS is often defined as a collection of *linear maps* in the literature that produces the shares using the secret and randomness as inputs. The authors of [27] employ this definition to prove the duality of multi-linear SSSs. However, extending their proof to the class of abelian schemes is not straightforward at a first glance. Also, working with the above-mentioned definition of an abelian random variable (i.e., as a group-characterizable random variable whose main group is abelian) seems an obstacle to advance. To achieve our result, using the notion of *Pontryagin duality* in group theory, we will first provide an equivalent definition of *abelian random variables* which is much easier to work with. Our definition is a generalization of the method that has been used in [37] to construct a linear random variable based on a given collection of subspaces of a vector space. Then, using properties of Pontryagin duality, we prove that the information ratios of dual access structures are the same for the class of abelian schemes.
- **Building on old results on homomorphic schemes.** We revisit the results by Frankel, Desmedt and Burmester [29, 30] on homomorphic secret

sharing, which was presented in 1992. Using concepts form abstract and linear algebra, we then transform an ideal homomorphic scheme—in a non-trivial way—into an ideal multi-linear one with the same access structure.

1.3 Related work and known results

We are not aware of any significant result regarding duality of secret sharing schemes and common information property in the literature except those mentioned earlier. In this section, we discuss other important relevant results.

On known lower bound techniques. There are mainly two different approaches for determining a lower bound on the information ratio of an access structure.

The *first* one is based on the properties of *entropy* of random variables. The so-called *Shannon-type information inequalities*, were first used by Capocelli, De Santis, Gargano and Vaccaro [19] due to the connection between Shannon entropies and polymatroids. The method was later refined by Csirmaz [21], using which he could prove his well-known $\Omega(n/\log n)$ lower bound on information ratio. It was further improved in [12] by taking into account the so-called *non-Shannon-type* information inequities [57] for general secret sharing or *linear rank inequalities* [25, 38] for multi-linear secret sharing schemes. The recent modification by Farràs, Kaced, Molleví and Padró [28] takes advantage of the non-Shannon-type information inequalities implicitly by using the so-called *Ahlswede-Körner* [23] and *common information* [25] properties, for deriving lower bounds on general and abelian secret sharing, respectively. All above methods find a lower bound for arbitrarily long secrets but it fails to work for restricted situations (e.g., for a specific secret space size or a specific field characteristic[3]).

The *second* method has mainly been used to derive lower bound on linear secret sharing schemes (with [7] being an exception which also works for multi-linear schemes). This method is based on *counting* and *combinatorial-algebraic arguments*, first introduced by Beimel, Gál and Paterson [8], based on the equivalence of secret sharing schemes and *monotone span programs* [43]. This method has been mainly applied to linear secret sharing (i.e., when the secret is a single field element) and was refined in [4, 5]. It was further improved by Gál in [32], based on combinatorial-algebraic ideas of Raz [49], to prove a $\Omega(n^{\log n})$ lower-bound. Building on ideas from [33], Gál's lower-bound was later shown in [6] to hold for multi-linear secret sharing as well. An exponential lower bound on linear secret sharing has been recently proved in [48] along the same lines. Lower bounds, merely based on counting arguments, have also been applied to the

[3] We remark that examples of characteristic-dependent linear rank inequalities exists in the literature [16, 26], however, we were not able to successfully apply them to Fano and non-Fano access structures in an automated linear programing. This was not very surprising because already it had been realized that the success of direct use of linear rank inequities in linear programs is quite limited, and actually it was for this reason that the CI method [28] was introduced.

class of forbidden graph access structures [54] and their generalization known as uniform access structures [1, 10, 45], respectively, in [7] and [3].

We emphasize that none of these methods can be used for our purposes. In particular, even though the method used in [13] also takes the characteristic of the underlying finite field into account, it can not be applied to a specific access structure. On the other hand, this method is algebraic-combinatorial and only works for linear schemes. It is not even clear if it can be extended to multi-linear schemes, let alone proving superiority of abelian schemes to multi-linear ones.

On the power of different classes of schemes. Our results show that mixed-linear (and hence general) secret sharing schemes are superior to multi-linear schemes. To the best of our knowledge, there is not result in the literature proving superiority of general schemes to multi-linear ones.

Simonis and Ashikhmin [52] have shown that multi-linear secret sharing is more powerful than linear secret sharing by studying the access structure induced by the Non-Pappus matroid. The achieved gain was a constant factor and a super-constant gain has been quite recently achieved in [2] (see [1] for a follow-up).

The first indication of superiority of general schemes to linear schemes was provided by Beimel and Ishai [9] (see [55] for a follow-up) as their result was valid assuming some plausible number-theoretic (or complexity-theoretic) assumption holds true. Later, Beimel and Weinreb [13] proved the result without relying on any assumption. This result also follows by recent developments in secret sharing via the connection between the class of forbidden graph access structures and the CDS primitive [35], by Liu, Vaikuntanathan and Wee [46]. Applebaum and Arkis [1] have further discussed the power of amortization in secret sharing.

On homomorphic secret sharing. The notion of homomorphic secret sharing scheme was introduced by Benaloh [14]. Very little is known about homomorphic secret sharing schemes. Frankel, Desmedt and Burmester [30] have proved that the secret space of every homomorphic scheme is an abelian group. In a subsequent work, Frankel and Desmedt [29] have shown that, when the scheme is ideal, the share spaces are all isomorphic to the secret space, and hence abelian too. Additionally, they have proved that there exist infinitely many abelian groups over which there does not exist an ideal homomorphic scheme. In a recent work [42], it has been proved that homomorphic schemes are equivalent to group-characterizable schemes with normal subgroups.

1.4 Paper organization

In Section 2, we study the group-characterizable random variables, identify a subclass of them that satisfies the CI property, and provide equivalent definitions for abelian random variables. Basics of SSSs and simplified definitions for linear and abelian schemes are presented in Section 3. In Section 4, we introduce our new characteristic-dependent lower-bound technique and apply it to Fano and non-Fano access structures. In Section 5, we provide upper bounds

for Fano and non-Fano access structures by constructing optimal characteristic dependent schemes using the (λ, ω) decomposition method [56]. In Section 6, we prove superiority of abelian schemes to multi-linear ones. Section 7 studies the connection between convec sets and entropy regions. Section 8 presents the duality of abelian schemes. Section 9 presents our result on ideal homomorphic SSSs. Finally, we conclude the paper in Section 10.

2 Random variables based on groups

Since secret sharing schemes are equivalent to jointly distributed random variables (RVs), before formally introducing this primitive, we prefer to study RVs. In particular, we study the notion of group-characterizable random variables (GCRVs), introduced by Chan and Yeung in [20]. The reason for this is that some subclasses of GCRVs correspond to well-known classes of secret sharing schemes which will be studied in this paper.

Notation. We use the terminologies of RV and distributions interchangeably and use boldface characters for them. All RVs are discrete in this paper. The Shannon entropy of a RV $\boldsymbol{X}$ is denoted by $\mathrm{H}(\boldsymbol{X})$, and the mutual information of RVs $\boldsymbol{X}$ and $\boldsymbol{Y}$, is denoted by $\mathrm{I}(\boldsymbol{X} : \boldsymbol{Y})$.

2.1 Group-characterizable random variables

For reader's convenience we provide the necessary background on abstract algebra in Appendix A.

Definition 2.1 (GCRV [20]) *Let $G_1, \ldots, G_n$ be subgroups of a finite group $(G, *)$, called the* main group*, and let $\mathbf{g}$ be a uniform RV on G. We refer to the joint distribution $(\mathbf{g}G_1, \ldots, \mathbf{g}G_n)$ as a group-characterizable RV (GCRV), where $\mathbf{g}G_i$ is a RV whose support is the left cosets of G_i in G. We say that $[G : G_1, \ldots, G_n]$ is a group-characterization for the (induced) RV.*

Let $(\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n)$ be a GCRV induced by $[G : G_1, \ldots, G_n]$, and fix a subset $A \subseteq [n]$. It can be shown that the marginal RV $\boldsymbol{X}_A = (\boldsymbol{X}_i)_{i \in A}$ is uniform on its support $\Big\{ (gG_i)_{i \in A} \ : \ \ g \in G \Big\}$, which is a subset of the Cartesian product $\prod_{i \in A} \big(G/G_i\big)$. It is straightforward (e.g., see [20]) to show that $\mathrm{H}(\boldsymbol{X}_A) = \log \big(|G|/|G_A|\big)$.

Depending on the choice of main group or the subgroups, we will have different subclasses of GCRVs. We are interested in the following classes: 1) when the main group is a vector space, 2) when the main group is an abelian group, 3) when the subgroups are normal in the main group and, 4) when the subgroups are "globally permuting".

The first class is equivalent to the so called linear RVs [37] (which in the context of secret sharing it corresponds to multi-linear schemes). The second one is called abelian and, before our results, there has been almost no significant result

about them. By a recent result [42], the third class is equivalent to homomorphic secret sharing schemes. Regarding the fourth class, in Section 2.5, we will define the notion of globally permuting subgroups and show that GCRV in this class satisfy the common information property [31], which before were known to be satisfied by abelian schemes [28, Remark 3.7].

2.2 When the main group is abelian or a vector space

In this section, we provide an equivalent definition of GCRVs with abelian main groups. Our approach is a generalization of the approach taken in [37] for defining the notion of linear RVs. Therefore, we will not cover the case where the main group is a vector space and refer the reader to the original paper.

Let $(G,+)$ be a finite abelian group and $G_1,\dots,G_n$ be some subgroups of G. We associate a vector of jointly distributed RVs that we refer to as the RV induced by $(G;G_1,\dots,G_n)$. We call such a distribution an abelian RV. The approach in [37] employs the dual of a vector space. We use the notion of Pontryagin dual for abelian groups.

Definition 2.2 (Pontryagin dual) *The Pontryagin dual of an abelian group G, denoted by $\widehat{G}$, is the group of all homomorphism from G to $\mathbb{C}^*$, where $\mathbb{C}^*$ is the multiplicative group of non-zero complex numbers. In other words, $\widehat{G} = \mathrm{Hom}(G,\mathbb{C}^*) = \{\alpha : G \to \mathbb{C}^* | \alpha(0)=1, \alpha(a+b)=\alpha(a)\alpha(b)\}$.*

It can be verified that $|\widehat{G}| = |G|$ and in fact $\widehat{G} \cong G$, i.e., $\widehat{G}$ and G are isomorphic.

Let K_i be the kernel of the map $\widehat{G} \to \widehat{G_i}$ defined by $\alpha \to \alpha|_{G_i}$, where $\alpha|_{G_i}$ is the restriction map[4]; that is, $K_i = \{\alpha \in \widehat{G} : \alpha(x) = 1 \text{ for every } x \in G_i\}$. Now, the uniform probability distribution $\boldsymbol{\alpha}$ on $\widehat{G}$ and the maps $\mu_i : \widehat{G} \to \widehat{G}/K_i$ determine a joint distribution $(\boldsymbol{X}_i)_{i\in[n]} = \big(\mu_i(\boldsymbol{\alpha})\big)_{i\in[n]}$, which we call the distribution induced by $(G;G_1,\dots,G_n)$. Clearly, the induced distribution is GC since $[\widehat{G} : K_1,\dots,K_n]$ is a group-characterization for it whose main group is abelian. Since the same transformation takes $(\widehat{G};K_1,\dots,K_n)$ into $[G : G_1,\dots,G_n]$ isomorphically, we conclude that a GCRV with abelian main group is an abelian RV. That is, the two notions are equivalent.

Since the homomorphism $\widehat{G} \to \widehat{G_i}$ defined by $\alpha \to \alpha|_{G_i}$ is onto with kernel K_i, we get an isomorphism $\widehat{G}/K_i \cong \widehat{G_i} \cong G_i$. Therefore, $|\widehat{G}/K_i| = |G_i|$, implying that $\mathrm{H}(\boldsymbol{X}_i) = \log|\widehat{G}/K_i| = \log|G_i|$. More generally, for every subset $A \subseteq [n]$, we have $\mathrm{H}(\boldsymbol{X}_A) = \log|G_A|$ where $G_A = \sum_{i\in A} G_i$; because it can be shown in a straightforward way that $\widehat{G}/K_A \cong \widehat{G_A} \cong G_A$ where $K_A = \bigcap_{i\in A} K_i$. To summarize, we have the following proposition.

Proposition 2.3 (Abelian random variable) *Let $(G,+)$ be a finite abelian group and $G_1,\dots,G_n$ be some subgroups of G. Then, as discussed above, the tuple*

[4] For a function $f : D \to R$ and a sub-domain $A \subseteq D$, the restriction map $f|_A$ is the restriction of the map f to the subdomain A. That is, $f|_A : A \to R$ is defined by $f|_A(x) = f(x)$ for every $x \in A$.

$(G; G_1, \ldots, G_n)$ induces a RV $(\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n)$, called an abelian RV, which is GC with an abelian main group. Additionally, for every subset $A \subseteq [n]$, $\mathrm{H}(\boldsymbol{X}_A) = \log |G_A|$ where $G_A = \sum_{i \in A} G_i$.

2.3 When the subgroups are normal

We call a RV $\boldsymbol{X} = (\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n)$ homomorphic if i) the support of each marginal distribution $\boldsymbol{X}_i$ is a group, say X_i, ii) the support of $\boldsymbol{X}$ is a subgroup of the direct product group $X_1 \times \cdots \times X_n$, and iii) $\boldsymbol{X}$ is uniformly distributed on its support. This means that every $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ in the support of $\boldsymbol{X}$ are equiprobable and their product $(x_1 y_1, \ldots, x_n y_n)$ is also in the support of $\boldsymbol{X}$. The following result has been proved in [42], which provides an equivalent definition for homomorphic RVs in terms of GCRVs.

Theorem 2.4 *A vector of jointly distributed RVs is homomorphic if and only if it is, up to relabeling, group-characterizable with normal subgroups.*

The notion of relabeling has been defined in [42]. Two random variables $\boldsymbol{X}$ and $\boldsymbol{Y}$ are said to be relabeling of one another if there exists a mapping f from the support of $\boldsymbol{X}$ to the support of $\boldsymbol{Y}$ such that $f(\boldsymbol{X})$ and $\boldsymbol{Y}$ are identically distributed.

2.4 When the subgroups are globally permuting

In this section, we identify a subclass of GCRV that satisfies the common information (CI) property. We say that the pair $(\boldsymbol{X}, \boldsymbol{Y})$ of jointly distributed random variables satisfies the CI property if there exists a RV $\boldsymbol{Z}$ such that $\mathrm{H}(\boldsymbol{Z}|\boldsymbol{X}) = \mathrm{H}(\boldsymbol{Z}|\boldsymbol{Y}) = 0$ and $\mathrm{H}(\boldsymbol{Z}) = \mathrm{I}(\boldsymbol{X} : \boldsymbol{Y})$. We say that a vector $(\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n)$ of jointly distributed RVs satisfies the CI property if for every pair of (not necessarily disjoint) subsets $A, B \subseteq [n]$, $(\boldsymbol{X}_A, \boldsymbol{X}_B)$ satisfies the CI property.

In the original paper [31] that coined the term, it was shown that general RVs do not necessarily satisfy the CI property. It is known that linear and abelian RVs satisfy the CI property. In the remaining part of this section, we show that the CI property is satisfied by GCRVs when the subgroups are *globally permuting* (to be defined). This class includes the homomorphic RVs, which itself contains the linear and abelian RVs.

Let us recall the definition of product of two subgroups. For subgroups H, K of a group $(G, *)$, their product is defined to be $K * H = \{k * h : h \in K, h \in H\}$. Trivially, $K * H$ contains both K and H. The set $K * H$ is not necessarily a subgroup and its size is given by the *product formula*: $|K * H| = \frac{|K||H|}{|k \cap H|}$. The product of two subgroups H, K is a group if and only if they are *permuting*; that is, $H * K = K * H$.

Globally permuting subgroups. We say that a collection $G_1, \ldots, G_n$ of subgroups of a group $(G, *)$ are globally permuting if G_A and G_B are permuting subgroups for every $A, B \subseteq [n]$, where $G_A = \bigcap_{i \in A} G_i$.

Proposition 2.5 (GCRVs with CI) *Every group-characterizable random variable whose subgroups are globally permuting satisfies the CI property.*

Proof. Let $(\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n)$ be a GCRV induced by $[G : G_1, \ldots, G_n]$ and let $A, B \subseteq [n]$. By the product formula and definition of mutual information, we have $\mathrm{I}(\boldsymbol{X}_A : \boldsymbol{X}_B) = \log \frac{|G|}{|G_A * G_B|}$. Since G_A and G_B are permuting subgroups, their product is a subgroup, say G_0, which contains both G_A and G_B. Therefore, $\mathrm{I}(\boldsymbol{X}_A : \boldsymbol{X}_B) = \log \frac{|G|}{|G_0|}$. Now consider the GCRV $(\boldsymbol{X}_0, \boldsymbol{X}_A)$ induced by $[G : G_0, G_A]$. By definition of conditional entropy, we have $\mathrm{H}(\boldsymbol{X}_0|\boldsymbol{X}_A) = \log \frac{|G_A|}{|G_A \cap G_0|} = \log \frac{|G_A|}{|G_A|} = 0$. Similarly, $\mathrm{H}(\boldsymbol{X}_0|\boldsymbol{X}_B) = 0$. Also, $\mathrm{H}(\boldsymbol{X}_0) = \log \frac{|G|}{|G_0|}$. Therefore, $\boldsymbol{X}_0$ satisfies the required conditions of CI. □

The intersection of normal subgroups is normal. Also, normal subgroups are permuting. Therefore, a collection of normal subgroups are globally permuting. The following corollary then follows by Theorem 2.4.

Corollary 2.6 (CI for homomorphic RV) *Homomorphic random variables satisfy the common information property.*

3 Secret sharing schemes: basic definitions

In this section, we present the basic concepts in secret sharing. Throughout the paper, n stands for the number of participants, $P = [n] = \{1, \ldots, n\}$ is the participants set and $Q = P \cup \{0\}$, where 0 stands for the dealer.

Access structure. A non-empty subset $\mathcal{A} \subseteq 2^P$, with $\varnothing \notin \mathcal{A}$, is called an *access structure* on P if it is *monotone*; that is, $A \subseteq B \subseteq P$ and $A \in \mathcal{A}$ imply that that $B \in \mathcal{A}$. A subset $A \subseteq P$ is called *qualified* if $A \in \mathcal{A}$; otherwise, it is called *unqualified*. A qualified subset is called *minimal* if none of its proper subsets is qualified.

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

Linear, p-linear and abelian SSS. In the rest of paper *we do not distinguish between linear and multi-linear SSS* and simply call them linear. A SSS is said to be linear (resp. abelian), if as a RV it is linear (resp. abelian). It is called p-linear, for a prime p, if the characteristic of the underlying finite field is p. Based on our discussion in Section 2.2, we use the simplified notations $\Pi = (T; T_0, T_1, \ldots, T_n)$ and $\Pi = (G; G_0, G_1, \ldots, G_n)$ for a linear and an abelian scheme, respectively. Here, T is a finite dimensional vector space on a finite field and T_i's are subspaces of it. Similarly, G is a finite abelian group and G_i's are its subgroups. More

precisely, when we refer to a secret sharing scheme Π (linear or abelian), we are actually referring to the induced secret sharing scheme $\boldsymbol{S} = \left(\boldsymbol{S}_i\right)_{i\in Q}$. When there is no confusion, we omit T and G and simply write $\Pi = (T_i)_{i\in Q}$ and $\Pi = (G_i)_{i\in Q}$ for a linear and an abelian scheme, respectively.

Perfect security. We say that $\left(\boldsymbol{S}_i\right)_{i\in Q}$ is a *(perfect) SSS* for $\mathcal{A}$, or it *(perfectly) realizes* $\mathcal{A}$, if the following two conditions 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 $A \in \mathcal{A}$ and,
- *Privacy:* $\mathrm{I}(\boldsymbol{S}_0 : \boldsymbol{S}_B) = 0$ for every unqualified set $B \in \mathcal{A}^c$.

Convec of a SSS. The *convec* (short for contribution vector) of a secret sharing scheme $(\boldsymbol{S}_0, \boldsymbol{S}_1, \ldots, \boldsymbol{S}_n)$ is defined by the vector $\left(\frac{\mathrm{H}(\boldsymbol{S}_1)}{\mathrm{H}(\boldsymbol{S}_0)}, \ldots, \frac{\mathrm{H}(\boldsymbol{S}_n)}{\mathrm{H}(\boldsymbol{S}_0)}\right)$.

Information ratio. The *maximum* and *average* information ratios of a SSS on n participants with convec $(\sigma_1, \ldots, \sigma_n)$ are defined to be $\max\{\sigma_1, \ldots, \sigma_n\}$ and $(\sigma_1 + \ldots + \sigma_n)/n$, respectively. The maximum/average information ratio of an access structure is defined to be the infimum of all maximum/average information ratios of all SSSs that realize it.

Linear, p-linear and abelian information ratio. In the computation of (max/average) information ratio, if we restrict ourselves to the class of linear (resp. p-linear or abelian) schemes, we refer to it as the linear (resp. p-linear or abelian) information ratio.

4 A new lower bound technique

In this section, we introduce our new technique for finding a lower bound on the characteristic-dependent linear information ratio of an access structure. We then apply our method to determine the exact value of the maximum/average linear information ratio of the Fano and non-Fano access structures on odd and even characteristics, respectively. Both access structures are ideal for the opposite characteristic.

Recap on linear SSS. As we mentioned in Section 3, we use the notation $\Pi = (T_i)_{i\in Q}$ for a linear SSS. It is easy to verify that the convec of Π is simply given by $\left(\frac{\dim T_i}{\dim T_0}\right)_{i\in P}$. Also, the correctness and privacy conditions for realization of an access structure $\mathcal{A}$ by Π are simplified as follows, where $T_A = \sum_{i\in A} T_i$:

- *Correctness:* $T_0 \cap T_A = T_0$ for $A \in \mathcal{A}$,
- *Privacy:* $T_0 \cap T_A = \{0\}$ for $A \notin \mathcal{A}$.

These relations follow by properties of entropy function and the product formula (which was mentioned in Section 2.4) for vector spaces (i.e., $|V + W| = \frac{|V||W|}{|V\cap W|}$, or equivalently $\dim(V + W) = \dim V + \dim W - \dim(V \cap W)$).

4.1 Two useful lemmas

Two linear algebraic lemmas, that we call the *minimal subspace lemma* and the *kernel lemma*, in companion with other concepts from linear algebra lie at the heart of our method.

Lemma 4.1 (Minimal subspace lemma) *Let $(T_0, T_1, \ldots, T_n)$ be a linear SSS for an access structure $\mathcal{A}$ and $A \in \mathcal{A}$ be a minimal qualified set. Then, there exists a subspace collection $\{V_i\}_{i\in A}$, where $V_i \subseteq T_i$ for each $i \in A$, such that:*

(i) $\dim V_i = \dim T_0$ *for every* $i \in A$,
(ii) $V_k \cap \sum_{i\in A\setminus\{k\}} T_i = \{0\}$ *for every* $k \in A$,
(iii) $T_0 \subseteq \bigoplus_{i\in A} V_i$ *(i.e., every* $s \in T_0$ *can be uniquely written as* $s = \sum_{i\in A} a_i$ *where* $a_i \in V_i$*)*,
(iv) the projection of T_0 *onto* V_i *is surjective and injective for every* $i \in A$.

Proof. Let $e_1, \ldots, e_z$ be a basis for T_0. Since $T_0 \subseteq \sum_{i\in A} T_i$, one can write $e_j = \sum_{i\in A} e_{ij}$ for $e_{ij} \in T_i$. We define V_i as the linear span of $e_{i1}, \ldots, e_{iz}$. These vectors are independent because a linear relation $\sum_{j=1}^{z} \lambda_j e_{ij} = 0$ implies that $\sum_{j=1}^{z} \lambda_j e_j$ is expressed inside $\sum_{k\in A\setminus\{i\}} T_k$. But since $A\setminus\{i\}$ is unqualified, it must hold that $\sum_{j=1}^{z} \lambda_j e_j = 0$; i.e., λ_j's are all zero. Hence, $\dim V_i = \dim T_0 = z$ that proves (i). To prove (ii), let $a \in V_k \cap \sum_{i\in A\setminus\{k\}} T_i$. We show that $a = 0$. Write $a = \sum_{j=1}^{z} \lambda_j e_{kj}$ and notice that $\sum_{j=1}^{z} \lambda_j e_j = \sum_{j=1}^{z} \sum_{i\in A} \lambda_j e_{ij} = a + \sum_{j=1}^{z} \sum_{i\in A\setminus\{k\}} \lambda_j e_{ij}$.

Since both a and $\sum_{j=1}^{z} \sum_{i\in A\setminus\{k\}} \lambda_j e_{ij}$ belong to $\sum_{i\in A\setminus\{k\}} T_i$, so is $\sum_{j=1}^{z} \lambda_j e_j$. But $A\setminus\{k\}$ is not qualified and hence $\sum_{j=1}^{z} \lambda_j e_j = 0$. So λ_j's are all zero and hence $a = 0$. To prove (iii), it is clear that $T_0 \subseteq \sum_{i\in A} V_i$. But this sum is indeed a direct sum; i.e., $V_k \cap \sum_{i\in A\setminus\{k\}} V_i = \{0\}$ for every $k \in A$, since a stronger statement was proved in (ii). To prove the last statement, since $\dim T_0 = \dim V_i$, we only need to prove that projecting T_0 onto V_i is surjective. Suppose $a \in V_i$ and write $a = \sum_{j=1}^{z} \lambda_j e_{ij}$. Then, the V_i component of $\sum_{j=1}^{z} \lambda_j e_j$ is a, and therefore, its projection onto V_i is a. □

The following corollary can be proved using Shannon inequalities (e.g., refer to [22, Proposition 2.3 (i)]). Here, we present an alternative proof using the minimal subspace lemma (MSL).

Corollary 4.2 *Let $(T_0, T_1, \ldots, T_n)$ be a linear SSS for the access structure $\mathcal{A}$. Then, for every minimal qualified set $A \in \mathcal{A}$ and every participant $k \in A$, we have* $\dim T_k \geqslant \dim T_0 + \dim \left(T_k \cap \sum_{i\in A\setminus\{k\}} T_i\right)$.

Proof. Let $\{V_i\}_{i\in A}$ be a minimal subspace collection. Clearly, $T_k \cap \sum_{i\in A\setminus\{k\}} T_i$ is a subspace of T_k and so is V_k by the lemma. By Lemma 4.1 (ii), these subspaces are independent. It then follows that $\dim T_k \geqslant \dim V_k + \dim \left(T_k \cap \sum_{i\in A\setminus\{k\}} T_i\right)$. This completes the proof since $\dim V_k = \dim T_0$ by Lemma 4.1 (i). □

Lemma 4.3 (Kernel lemma) *Let $(T_0, T_1, \ldots, T_n)$ be a linear SSS for an access structure $\mathcal{A}$ on n participants. Let $A \in \mathcal{A}$ be a minimal qualified subset and*

for every participant $i \in A$ let A_i (not necessarily different from A) be a minimal qualified subset that includes i. For the minimal qualified subsets A and A_i, $i \in A$, consider minimal subspace collections $\{V_j\}_{j\in A}$ and $\{V_j^i\}_{j\in A_i}$, respectively. Define the linear map $\phi : T_0 \to \bigoplus_{i\in A} \frac{V_i}{V_i \cap V_i^i}$, by sending $s \in T_0$ to its projections on V_i and taking it modulo $V_i \cap V_i^i$ for $i \in A$. That is, if $s = \sum_{i\in A} a_i$ for $a_i \in V_i$, we define $\phi(s) = \big([a_i]\big)_{i\in A}$, where $[\cdot]$ stands for the class in the corresponding quotient space. Then, $\sum_{i\in A} \dim T_i \geqslant (|A|+1)\dim T_0 - \dim\ker\phi$.

Proof. The linear map ϕ induces a 1-1 linear map $\bar{\phi} : \frac{T_0}{\ker\phi} \to \bigoplus_{i\in A} \frac{V_i}{V_i\cap V_i^i}$. Hence, $\sum_{i\in A} \dim \frac{V_i}{V_i\cap V_i^i} \geqslant \dim \frac{T_0}{\ker\phi}$, or equivalently, $\sum_{i\in A} \big(\dim V_i - \dim(V_i \cap V_i^i)\big) \geqslant \dim T_0 - \dim\ker\phi$. Add $\sum_{i\in A}\dim(V_i^i) = |A|\dim T_0$ —see Lemma 4.1 (i)— to the both sides of this inequality and simplify to get $\sum_{i\in A}\dim(V_i + V_i^i) \geqslant (|A|+1)\dim T_0 - \dim\ker\phi$. The claim then follows due to $V_i + V_i^i \subseteq T_i$, which implies $\sum_{i\in A}\dim T_i \geqslant \sum_{i\in A}\dim(V_i+V_i^i)$. □

4.2 Application to Fano

The Fano access structure, denoted by $\mathcal{F}$, is the port of the Fano matroid, with the following representation[5]: $\mathcal{F} = 14 + 25 + 36 + 123 + 156 + 246 + 345$. It is ideal on finite fields with even characteristics but it does not admit an ideal scheme if the secret space size is odd [47]. We employ our method to determine the exact value of its maximum and average p-linear information ratios for every odd prime p, which turns out to be independent of p. The Fano access structure enjoys a high degree of symmetry[6] which is useful for both finding lower bounds and upper bounds.

Proposition 4.4 (Fano with odd characteristics) *For an odd prime p and every p-linear SSS $(T_0, T_1, \ldots, T_6)$ for Fano access structure, we have:*

(I) $\dim T_i \geqslant \dim T_0$, *for every* $i \in \{1,\ldots,6\}$,
(II) $\dim T_i + \dim T_j + \dim T_k \geqslant 4\dim T_0$, *for every size-3 minimal qualified set* $\{i,j,k\}$.

Additionally, the maximum and average p-linear information ratios are both $\frac{4}{3}$ for every odd prime prime p.

Proof. The first inequality is trivial and follows by Corollary 4.2. To prove (II), by symmetry, we only prove the inequality for the qualified set $\{1,2,3\}$. Let ϕ be the linear map defined in Lemma 4.3 by the minimal qualified sets $A = \{1,2,3\}$, $A_1 =$

[5] A subset $A = \{i_1,\ldots,i_k\} \subseteq [n]$ is represented by $i_1\cdots i_k$; e.g., 14 for the set $\{1,4\}$. An access structure with minimal qualified subsets $\{A_1,\ldots,A_k\}$ is represented by $A_1 + \ldots + A_k$.

[6] We call a permutation ϕ on the participants set of an access structure $\mathcal{A}$ a symmetry of $\mathcal{A}$, if $\phi(\mathcal{A})$ is isomorphic to $\mathcal{A}$, where $\sigma(\mathcal{A})$ is an access structure which is achieved by replacing participant i with $\phi(i)$.

$\{1,4\}$, $A_2 = \{2,5\}$ and $A_3 = \{3,6\}$ with the corresponding minimal subspace collections $\{V_1, V_2, V_3\}$, $\{V_1', V_4'\}$, $\{V_2', V_5'\}$ and $\{V_3', V_6'\}$. The claim follows if we show that $\ker \phi$ is zero, since $\dim T_1 + \dim T_2 + \dim T_3 \geqslant 4 \dim T_0 - \dim \ker \phi$.

Suppose $s = a_1 + a_2 + a_3 \in T_0$, where $a_i \in V_i$ for $i = 1, 2, 3$, maps to zero by ϕ; i.e., $\phi(s) = ([a_1], [a_2], [a_3]) = 0$, or equivalently, $a_i \in V_i \cap V_i'$, for $i = 1, 2, 3$.

There are $a_4' \in V_4'$, $a_5' \in V_5'$ and $a_6 \in V_6'$ such that $a_1 + a_4' \in T_0$, $a_2 + a_5' \in T_0$ and $a_3 + a_6' \in T_0$. By subtracting each vector from $s = a_1 + a_2 + a_3 \in T_0$, it then follows that $a_2 + a_3 - a_4' \in T_0$, $a_1 + a_3 - a_5' \in T_0$ and $a_1 + a_2 - a_6' \in T_0$. But since $\{2,3,4\}$, $\{1,3,5\}$ and $\{1,2,6\}$ are unqualified sets, all these vectors must be zero; i.e., $a_4' = a_2 + a_3$, $a_5' = a_1 + a_3$ and $a_6' = a_1 + a_2$. Since the characteristic of the underlying finite field is odd, we have $s = (a_4' + a_5' + a_6')/2$. Since $\{4,5,6\}$ is unqualified, it implies that $s = 0$. This shows that $\ker \phi = \{0\}$.

Proof of claim on information ratio: By adding up inequality (II) for every size-3 minimal qualified set $\{i,j,k\}$, we get $2 \sum_{i=1}^{6} \dim T_i \geqslant 16$. It then follows that the maxim and average p-linear information ratios are both at least $4/3$. In Section 5.3, we will show that, for every odd prime p, it admits a p-linear SSS with convec $(\frac{4}{3}, \frac{4}{3}, \frac{4}{3}, \frac{4}{3}, \frac{4}{3}, \frac{4}{3})$, showing that the max and average lower bounds are both tight (see Corollary 5.5). □

4.3 Application to non-Fano

The non-Fano access structure, denoted by $\mathcal{N}$, is the port of the non-Fano matroid, with the following representation: $\mathcal{N} = 14 + 25 + 36 + 123 + 156 + 246 + 345 + 456$; that is, $\mathcal{N} = \mathcal{F} + 456$ (see Footnote 5). It is ideal on finite fields with odd characteristics but it does not admit an ideal scheme if the secret space size is even [47]. We apply our technique to find the exact value of its maximum and average 2-linear information ratios. Similar to Fano, the non-Fano access structure also enjoys a high degree of symmetry (see Footnote 6).

Proposition 4.5 (Non-Fano with even characteristic) *For every 2-linear SSS $(T_0, T_1, \ldots, T_6)$ for the non-Fano access structure, we have:*

(I) $\dim T_i \geqslant \dim T_0$, *for every* $i \in \{1, \ldots, 6\}$,
(II) $\dim T_1 + \dim T_2 + \dim T_3 + \dim T_i \geqslant 5 \dim T_0$, *for every* $i = 4, 5, 6$,
(III) $\dim T_4 + \dim T_5 + \dim T_6 \geqslant 4 \dim T_0$,
(IV) $\dim T_i + 2 \dim T_j + \dim T_k \geqslant 5 \dim T_0$, *for every triple* $(i,j,k) = (1,5,6)$, $(1,6,5)$, $(2,4,6)$, $(2,6,4)$, $(3,4,5)$, $(3,5,4)$.

Additionally, the maximum and average 2-linear information ratios are $\frac{4}{3}$ *and* $\frac{23}{18}$, *respectively.*

Proof. The first inequality is trivial and follows by Corollary 4.2. Proofs of (II)-(IV) are based on the kernel lemma (Lemma 4.3).

Proof of (II). By symmetry, we prove the inequality for $i = 4$. Let ϕ be the linear map defined in Lemma 4.3 by the minimal qualified sets $A =$

$\{1,2,3\}$, $A_1 = \{1,4\}$, $A_2 = \{2,5\}$ and $A_3 = \{3,6\}$ with the corresponding subspace collections $\{V_1, V_2, V_3\}$, $\{V_1', V_4'\}$, $\{V_2', V_5'\}$ and $\{V_3', V_6'\}$. Since the inequality $\dim T_1 + \dim T_2 + \dim T_3 \geqslant 4\dim T_0 - \dim\ker\phi$ holds, it is enough to show that $\dim T_4 \geqslant \dim T_0 + \dim\ker\phi$. By Corollary 4.2, for the minimal qualified set $\{4,5,6\}$, we have $\dim T_4 \geqslant \dim T_0 + \dim(T_4 \cap (T_5 + T_6))$. Therefore, it is enough to construct a 1-1 map from $\ker\phi$ into $T_4 \cap (T_5 + T_6)$. This implies that $\dim(T_4 \cap (T_5 + T_6) \geqslant \dim\ker\phi$, which completes the proof.

We construct the 1-1 map from $\ker\phi$ into $T_4 \cap (T_5 + T_6)$ by associating a unique $a_4' \in T_4 \cap (T_5 + T_6)$ to every $s \in \ker\phi$. Suppose $s = a_1 + a_2 + a_3 \in T_0$, where $a_i \in V_i$ for $i = 1,2,3$, maps to zero by ϕ; i.e.; $a_i \in V_i \cap V_i'$ for $i = 1,2,3$. Therefore, one can find $a_4' \in V_4'$, $a_5' \in V_5'$ and $a_6' \in V_6'$ such that $a_1 + a_4' \in T_0$, $a_2 + a_5' \in T_0$ and $a_3 + a_6' \in T_0$. If we add each of these three vectors separately to $s = a_1 + a_2 + a_3 \in T_0$, we get $a_2 + a_3 + a_4' \in T_0$, $a_1 + a_3 + a_5' \in T_0$ and $a_1 + a_2 + a_6' \in T_0$ (recall the characteristic is even). Now all these vectors need to be zero since $\{2,3,4\}$, $\{1,3,5\}$ and $\{1,2,6\}$ are unqualified sets; hence, $a_4' = a_2 + a_3$, $a_5' = a_1 + a_3$ and $a_6' = a_1 + a_2$. It follows that $a_4' = a_5' + a_6'$ and, hence, it belongs to $T_4 \cap (T_5 + T_6)$. So we have defined a 1-1 map from $\ker\phi$ into $T_4 \cap (T_5 + T_6)$ by sending s to a_4'. The 1-1 ness of this map follows from the uniqueness of $a_4' \in V_4'$ such that $a_1 + a_4' \in T_0$; see Lemma 4.1 (iv).

Proof of (III). The proof is similar to that of Proposition 4.4. Let ϕ be the linear map defined in Lemma 4.3 by the minimal qualified sets $A = \{4,5,6\}$, $A_4 = \{1,4\}$, $A_5 = \{2,5\}$ and $A_6 = \{3,6\}$ with the corresponding subspace collections $\{V_4, V_5, V_6\}$, $\{V_1', V_4'\}$, $\{V_2', V_5'\}$ and $\{V_3', V_6'\}$. It is enough to show that $\ker\phi$ is zero because $\dim T_3 + \dim T_4 + \dim T_5 \geqslant 4\dim T_0 - \dim\ker\phi$. Suppose $s = a_4 + a_5 + a_6 \in T_0$, where $a_i \in V_i$ for $i = 4,5,6$, is in the kernel of ϕ; i.e.; $a_i \in V_i \cap V_i'$ for $i = 4,5,6$. We can find $a_i' \in V_i'$, for $i = 1,2,3$, such that $a_1' + a_4 \in T_0$, $a_2' + a_5 \in T_0$ and $a_3' + a_6 \in T_0$. By adding the sum of the first two vectors to $s = a_4 + a_5 + a_6 \in T_0$, it follows that $a_1' + a_2' + a_6 \in T_0$ (characteristic is even). But since $\{1,2,6\}$ is unqualified, the resulting vector must be zero; i.e., $a_6 = a_1' + a_2'$. Similarly, $a_4 = a_2' + a_3'$ and $a_5 = a_1' + a_3'$. Hence $s = a_4 + a_5 + a_6 = 0$. This shows that $\ker\phi = \{0\}$.

Proof of (IV). By symmetry, we prove the inequality only for the triple $(i,j,k) = (1,5,6)$. Let ϕ be the linear map defined in Lemma 4.3 by the minimal qualified sets $A = \{1,5,6\}$, $A_1 = \{1,4\}$, $A_5 = \{2,5\}$ and $A_6 = \{3,6\}$ with the corresponding minimal subspace collections $\{V_1, V_5, V_6\}$, $\{V_1', V_4'\}$, $\{V_2', V_5'\}$ and $\{V_3', V_6'\}$. The proof continues similar to that of (I). It is enough to show that $\dim T_5 \geqslant \dim T_0 + \dim\ker\phi$, because $\dim T_1 + \dim T_5 + \dim T_6 \geqslant 4\dim T_0 - \dim\ker\phi$. Since $\{4,5,6\}$ is a minimal qualified set, by Corollary 4.2, we have $\dim T_5 \geqslant \dim T_0 + \dim(T_5 \cap (T_4 + T_6))$. Therefore, to complete the proof, it is enough to construct a 1-1 map from $\ker\phi$ into $T_5 \cap (T_4 + T_6)$. Suppose $s = a_1 + a_5 + a_6 \in T_0$ for $i = 1,5,6$, where $a_i \in V_i$, maps to zero by ϕ; i.e.; $a_i \in V_i \cap V_i'$ for $i = 1,5,6$. Our map sends s to a_5. The uniqueness of this choice follows from Lemma 4.1 (iv). It remains to prove that $a_5 \in T_5 \cap (T_4 + T_6)$. It is enough to show that $a_5 \in T_4 + T_6$ since clearly $a_5 \in T_5$. Find $a_i' \in V_i'$, for $i = 2,3,4$ such that $a_1 + a_4' \in T_0$, $a_2' + a_5 \in T_0$ and $a_3' + a_6 \in T_0$. By adding the second vector, the

third one and the sum of the three vectors to $s = a_1 + a_5 + a_6 \in T_0$, it respectively follows that $a_1 + a_2' + a_6 \in T_0$, $a_1 + a_3' + a_5 \in T_0$ and $a_2' + a_3' + a_4' \in T_0$ (characteristic is even). But all these vectors must be zero since $\{1, 2, 6\}$, $\{1, 3, 5\}$ and $\{2, 3, 4\}$ are unqualified sets. Hence $a_5 = a_1 + a_3' = (a_2' + a_6) + (a_2' + a_4') = a_4' + a_6 \in T_4 + T_6$.
Proof of claim on information ratio: By inequality (III), the maxim 2-linear information ratio is at least $\frac{4}{3}$. By multiplying inequality (III) by two and adding it up with inequality (II) for every $i = 4, 5, 6$, we get $3\sum_{i=1}^{6} \dim T_i \geqslant 23$, which show that the average 2-linear information ratio is at least $\frac{23}{18}$. In Section 5.4, we will construct a 2-linear scheme with convec $(\frac{4}{3}, \frac{4}{3}, 1, \frac{4}{3}, \frac{4}{3}, \frac{4}{3})$, showing that both lower bounds are tight. □

5 Upper bounds for Fano and non-Fano

In this section, we construct characteristic-dependent SSSs for Fano and non-Fano access structures that match the lower bounds on the information ratios stated in Proposition 4.4 and Proposition 4.5, respectively. We use the (λ, ω)-decomposition technique [56] for constructing our schemes.

Even though the exact value of information ratios are determined, we try to determine their convec sets, where convec set is a parameter more general than information ratio. Our motivation for the study of convec sets will be discussed in Section 7.

The p-linear convec set of Fano is completely determined for every odd prime p. But, for the 2-linear convec set of non-Fano, an almost matching upper-bound is found.

5.1 Convec set

Before presenting the definition of a convec set, we present some basic definitions from topology which are useful for their understanding.

Definition 5.1 *A subset $\mathcal{X} \subseteq \mathbb{R}^n$ is said to be* convex *if for every pair of points $x, y \in \mathcal{X}$ and for every real number $\alpha \in [0, 1]$, the point $\alpha x + (1 - \alpha)y$, called a* convex combination *of x and y, is also in the set. The intersection of finitely many half-spaces is called a* convex polytope. *The* closure *of a set $\mathcal{X}$ is denoted by $\overline{\mathcal{X}}$, defined as the union of $\mathcal{X}$ with all its limit points. A point of a convex set $\mathcal{X}$ is said to be an* extreme point *if it does not lie in any line segment with endpoints in $\mathcal{X}$.*

We refer to [36] for background on convex sets. A convex set can be described either in terms of the intersection of a collection of half-spaces or in terms of its extreme points (together with some extra information called rays, which are redundant for convec sets).

Definition 5.2 (Convec set) *The convec set of an access structure $\mathcal{A}$, denoted by $\Sigma(\mathcal{A})$, is defined as the set of all convecs of all SSSs that realize $\mathcal{A}$. When we restrict to the class* C *of SSSs, we use the notation $\Sigma^{\mathrm{C}}(\mathcal{A})$.*

In particular, for the class of abelian (resp. p-linear/linear/homomorphic) SSSs, we use the notation Σ^{Abl} *(resp.* $\Sigma^{p}/\Sigma^{\text{Lin}}//\Sigma^{\text{Hom}}$*) and call it the abelian (resp. p-linear/linear/homomorphic) convec set.*

Similar to the convec sets, the abelian, p-linear and homomorphic convec sets all have convex closures (this claims follows by Lemma 6.2 and Remark 6.3, which will be stated in next section). However, as we will see in Section 6, the closure of a linear convec set is not necessarily convex, but union of convex sets, due to the following relation $\overline{\Sigma^{\text{Lin}}}(\mathcal{A}) = \bigcup_{p:\text{prime}} \overline{\Sigma^{p}}(\mathcal{A})$. In fact, our result on superiority of abelian schemes to linear schemes stems from this intuition.

It is clear that convec set is a more general parameter than information ratio. In particular, the maximum and average information ratios of an access structure $\mathcal{A}$ on n participants, with respect to the class C of schemes, can equivalently be defined as $\min\{\max(x) : x \in \overline{\Sigma^{\text{C}}}(\mathcal{A})\}$ and $\frac{1}{n}\min\{\sum_{i=1}^{n} x_i : (x_1, \ldots, x_n) \in \overline{\Sigma^{\text{C}}}(\mathcal{A})\}$, respectively.

We remark that there exist examples of access structures such that the extreme points of their convec sets are not realizable (e.g., the nearly-ideal access structures [11], which are non-ideal but their information ratio is one, do not contain the all-one vector in their convec sets). It is an open problem if there exists an access structure whose convec set is not a convex polytope (i.e., it has infinity many extreme points) and we conjecture that such access structures exist. Nevertheless, we conjecture that (1) the p-linear convec set of every access structure is a convex polytope, and (2) all its extreme points are realizable.

5.2 The (λ, ω)-decomposition technique

In this subsection, we review the (λ, ω)-decomposition technique from [56], which is a generalization of λ-decomposition, first proposed by Stinson [53]. It is used for constructing a SSS given a collection of SSSs, satisfying some particular conditions.

Definition 5.3 ((λ, ω)-decomposition) *Let* $\lambda > \omega \geqslant 0$ *be integers and* $\mathcal{A}$ *be an access structure. A* (λ, ω)-decomposition *for* $\mathcal{A}$ *consists of a collection* $\mathcal{A}_1, \ldots, \mathcal{A}_m$ *of access structures on the same set of participants as* $\mathcal{A}$ *such that the following requirements are satisfied: (1) if* $A \in \mathcal{A}$*, then* $A \in \mathcal{A}_j$ *for at least* λ *distinct values of* $j \in [m]$*, and (2) if* $A \in \mathcal{A}$*, then* $A \in \mathcal{A}_j$ *for at most* ω *distinct values of* $j \in [m]$*.*

Theorem 5.4 *Let* p *be a prime and* $\mathcal{A}_1, \ldots, \mathcal{A}_m$ *be a* (λ, ω)*-decomposition for* $\mathcal{A}$*. If for every* $j \in [m]$ *there exists a* p*-linear SSS for* $\mathcal{A}_j$ *with convec* σ_j*, then there exists a* p*-linear SSS for* $\mathcal{A}$ *with convec* $\frac{1}{\lambda-\omega}\sum_{j=1}^{m}\sigma_j$*.*

5.3 Matching upper-bound for Fano (odd characteristic)

We have used a computer to determine the extreme points of the polytope described by the 10 half-spaces mentioned in Proposition 4.4 (a normalization to

$\dim T_0$ is considered). It has the following 7 extreme points, which due to symmetries of Fano (see Footnote 6), they have been grouped in two columns:

$$\begin{array}{ll} (2,1,1,2,1,1) & (2,2,2,1,1,1) \\ (1,2,1,1,2,1) & (1,2,1,2,1,2) \\ (1,1,2,1,1,2) & (2,1,1,1,2,2) \\ & (1,1,2,2,2,1) \end{array} \tag{5.1}$$

Table 1: (λ,ω) decompositions for Fano (odd).

$\mathcal{A}_j$	convec	F_1	F_2
14	$(1,0,0,1,0,0)$	✓	
$\mathcal{F}_{14}$	$(1,1,1,1,1,1)$	✓	
$1+2+3$	$(1,1,1,0,0,0)$		✓
$\mathcal{N}$	$(1,1,1,1,1,1)$		✓
(λ,ω)		$(1,0)$	$(2,1)$

Table 2: Convec names.

#	Convec
F_1	$(2,\ 1,\ 1,\ 2,\ 1,\ 1)$
F_2	$(2,\ 2,\ 2,\ 1,\ 1,\ 1)$
N_1	$(1,\ 1,\ 1,\ 2,\ 2,\ 2)$
N_2	$(2,\ 1,\ 1,\ 2,\ 1,\ 1)$
N_3	$(2,\ 1,\ 1,\ 1,\ 2,\ 2)$
N_4	$(\frac{3}{2},\ 1,\ 1,\ \frac{3}{2},\ \frac{3}{2},\ \frac{3}{2})$
N_5	$(\frac{4}{3},\ \frac{4}{3},\ 1,\ \frac{4}{3},\ \frac{4}{3},\ \frac{4}{3})$
N_6	$(\frac{7}{5},\ \frac{6}{5},\ \frac{6}{5},\ \frac{6}{5},\ \frac{7}{5},\ \frac{7}{5})$

Table 3: (λ,ω) decompositions for non-Fano (even).

$\mathcal{A}_j$	Convec	N_1	N_2	N_3	N_4	N_5	N_6
14	$(1,0,0,1,0,0)$		✓				
456	$(0,0,0,1,1,1)$	✓					
1+5+6	$(1,0,0,0,1,1)$			✓			
14+456	$(1,0,0,1,1,1)$				✓		
123+36+25	$(1,1,1,0,1,1)$						✓
14+36+156 +345+456	$(1,0,1,1,1,1)$					✓	✓
14+25+156 +246+456	$(1,1,0,1,1,1)$						✓
$\mathcal{N}_{14}$	$(1,1,1,1,1,1)$		✓		✓	✓	✓
$\mathcal{N}_{25}$	$(1,1,1,1,1,1)$					✓	✓
$\mathcal{N}_{36}$	$(1,1,1,1,1,1)$						✓
$\mathcal{F}$	$(1,1,1,1,1,1)$	✓			✓	✓	✓
$\mathcal{N}$+234	$(1,1,1,1,1,1)$			✓			
(λ,ω)		$(1,0)$	$(1,0)$	$(2,1)$	$(2,0)$	$(3,0)$	$(5,0)$

Refer to Footnote 5 for representation of access structures. The minimal qualified subsets of the access structure $\mathcal{F}_{14}$ is the same as $\mathcal{F}$ except that 14 is excluded and $124, 134, 145, 146$ are all added. The access structure $\mathcal{N}_{14}$ is defined similarly; i.e., 14 is excluded from $\mathcal{N}$ and $124, 134, 145, 146$ are all added. For, $\mathcal{N}_{25}$ (resp. $\mathcal{N}_{36}$), the set 25 (resp. 36) is excluded from $\mathcal{N}$ and the sets $125, 235, 245, 256$ (resp. $136, 236, 346, 356$) are all added. A check mark (✓) indicates that the corresponding access structure appears in the desired (λ,ω)-decomposition. All sub-access structures, i.e., $\mathcal{A}_j$'s, in Table 1 are ideal on every odd prime characteristic. Those in Table 3 are ideal on even characteristic.

Using the (λ,ω)-decomposition, we show that for every prime p, all 7 points (convecs) are realizable for Fano by some p-linear scheme. Since the convecs of each column are symmetries of each other, it is enough to realize one from

each group. Table 1 presents a (λ, ω)-decomposition for the first convec of each column.

To summarize, we have determined the linear convec set of Fano for every odd prime, which is the convex polytope described by the 10 half-spaces mentioned in Proposition 4.4 with the 7 vectors in (5.1) as its extreme points.

Since the collection $\mathcal{F}, \mathcal{F}, \mathcal{F}$ is a $(3, 0)$-decomposition for $\mathcal{F}$, by taking the average of the convecs in the first column, we have the following corollary.

Corollary 5.5 *For every prime p, there exists a p-linear scheme for Fano with convec* $(\frac{4}{3}, \frac{4}{3}, \frac{4}{3}, \frac{4}{3}, \frac{4}{3}, \frac{4}{3})$. *In particular, this convec is optimal with respect to both maximum and average information ratios.*

5.4 An almost matching upper-bound for non-Fano (even characteristic)

The convex polytope described by the 16 half-spaces mentioned in Proposition 4.5 (after a normalization to $\dim T_0$), has the following set of 13 extreme points. Again, this has been verified using a computer. Note that due to symmetries of non-Fano (see Footnote 6), they have been grouped in five columns.

$$\begin{array}{rcccc}
 & (2,1,1,2,1,1) & (2,1,1,1,2,2) & (\frac{3}{2},1,1,\frac{3}{2},\frac{3}{2},\frac{3}{2}) & (\frac{5}{3},1,1,\frac{4}{3},\frac{4}{3},\frac{4}{3}) \\
(1,1,1,2,2,2) & (1,2,1,1,2,1) & (1,2,1,2,1,2) & (1,\frac{3}{2},1,\frac{3}{2},\frac{3}{2},\frac{3}{2}) & (1,\frac{5}{3},1,\frac{4}{3},\frac{4}{3},\frac{4}{3}) \\
 & (1,1,2,1,1,2) & (1,1,2,2,2,1) & (1,1,\frac{3}{2},\frac{3}{2},\frac{3}{2},\frac{3}{2}) & (1,1,\frac{5}{3},\frac{4}{3},\frac{4}{3},\frac{4}{3})
\end{array}$$

We have been able to realize all, except those in the last column, with a 2-linear scheme. In particular, using the (λ, ω)-decomposition, we show that the following 16 extreme points can be realized by a 2-linear scheme. Table 3 presents a (λ, ω)-decomposition for the first convec from each column.

$$\begin{array}{rcccc}
 & (2,1,1,2,1,1) & (2,1,1,1,2,2) & (\frac{3}{2},1,1,\frac{3}{2},\frac{3}{2},\frac{3}{2}) & (\frac{4}{3},\frac{4}{3},1,\frac{4}{3},\frac{4}{3},\frac{4}{3}) & (\frac{7}{5},\frac{6}{5},\frac{6}{5},\frac{6}{5},\frac{7}{5},\frac{7}{5}) \\
(1,1,1,2,2,2) & (1,2,1,1,2,1) & (1,2,1,2,1,2) & (1,\frac{3}{2},1,\frac{3}{2},\frac{3}{2},\frac{3}{2}) & (\frac{4}{3},1,\frac{4}{3},\frac{4}{3},\frac{4}{3},\frac{4}{3}) & (\frac{6}{5},\frac{7}{5},\frac{6}{5},\frac{7}{5},\frac{6}{5},\frac{7}{5}) \\
 & (1,1,2,1,1,2) & (1,1,2,2,2,1) & (1,1,\frac{3}{2},\frac{3}{2},\frac{3}{2},\frac{3}{2}) & (1,\frac{4}{3},\frac{4}{3},\frac{4}{3},\frac{4}{3},\frac{4}{3}) & (\frac{6}{5},\frac{6}{5},\frac{7}{5},\frac{7}{5},\frac{7}{5},\frac{6}{5})
\end{array}$$

The convex polytope which has the above set of vectors as its extreme points can be described by 22 half-spaces, 16 of which are those of Proposition 4.5. The additional 6 half-spaces are given by inequality $\dim T_i + \dim T_j + \dim T_k + \dim T_\ell \geqslant 5 \dim T_0$, for every $(i, j, k, \ell) = (1, 5, 6, 2), (1, 5, 6, 3), (2, 4, 6, 1), (2, 4, 6, 3), (3, 4, 5, 1), (3, 4, 5, 2)$.

To summarize, if one construct a 2-linear scheme with convec $(\frac{5}{3}, 1, 1, \frac{4}{3}, \frac{4}{3}, \frac{4}{3})$ for non-Fano, then the lower bound given by Proposition 4.5 is tight. On the other hand, if one derives the above 6 additional inequalities (by symmetry only one), it proves that our upper-bound (that corresponds to the last set of 16 extreme points) is tight.

6 Power of abelian schemes

In this section, we prove that abelian SSSs are more powerful than the linear schemes. To this end, we study the access structure $\mathcal{F}+\mathcal{N}$ [11,47], to be described below. In Section 6.1, we compute the exact value of its maximum and average linear information ratios. In Section 6.2, we provide an upper bound on its maximum and average abelian information ratios. It turns out that our upper-bound on the maximum abelian information ratio (7/6) is smaller that the exact value of the maximum linear information ratio (4/3). In Section 6.3, we will see that the lower bound technique of [28] (FKMP) fails to determine the exact value of linear information ratio of access structures. Two open problems are also presented and discussed in Section 6.4.

The $\mathcal{F}+\mathcal{N}$ access structure. For the purpose of this section, we assume that the participants sets of $\mathcal{F}$ and $\mathcal{N}$ access structures are $\{1,\ldots,6\}$ and $\{7,\ldots,12\}$, respectively. The access structure $\mathcal{F}+\mathcal{N}$, with participants set $\{1,\ldots,12\}$, is then defined to be the union of $\mathcal{F}$ and $\mathcal{N}$. This access structure is non-ideal but its information ratio is one, and hence called nearly-ideal [11].

6.1 Optimal linear schemes for $\mathcal{F}+\mathcal{N}$

Let p be an arbitrary prime (odd or even). Given a p-linear scheme for $\mathcal{F}$ with convec $\sigma_{\mathcal{F}}$ and a p-linear scheme for $\mathcal{N}$ with convec $\sigma_{\mathcal{N}}$, we can combine them in a straightforward way to construct a p-linear SSS for $\mathcal{F}+\mathcal{N}$ with convec $(\sigma_{\mathcal{F}},\sigma_{\mathcal{N}})$. The converse is also true (technically because Fano and non-Fano are minors of $\mathcal{F}+\mathcal{N}$).

Therefore, for every odd prime p, every extreme point of $\Sigma^p(\mathcal{F}+\mathcal{N})$ is of the form $(x,\mathbf{1})$, where x is an extreme point of $\Sigma^p(\mathcal{F})$ and $\mathbf{1}$ is an all-1 vector of length six. Consequently, by Proposition 4.4, the maximum p-linear information ratio of $\mathcal{F}+\mathcal{N}$ is $\frac{4}{3}$. Also, the average p-linear information ratio is $(\frac{4}{3}*6+6)/12 = 7/6$. By Corollary 5.5, there exists a p-linear scheme with convec $\sigma_{\text{odd}} = (\frac{4}{3},\frac{4}{3},\frac{4}{3},\frac{4}{3},\frac{4}{3},\frac{4}{3},1,1,1,1,1,1)$ that meets these optimal values.

Similarly, every extreme point of $\Sigma^2(\mathcal{F}+\mathcal{N})$ is of the form $(\mathbf{1},y)$, where y is an extreme point of $\Sigma^2(\mathcal{N})$. Therefore, by Proposition 4.5, the maximum 2-linear information ratio of $\mathcal{F}+\mathcal{N}$ is $\frac{4}{3}$. Additionally, the average 2-linear information ratio is $(6+\frac{23}{18}*6)/12 = \frac{41}{36}$. By our results in Section 5.4, there exists a 2-linear scheme with convec $\sigma_{\text{even}} = (1,1,1,1,1,1,\frac{4}{3},\frac{4}{3},1,\frac{4}{3},\frac{4}{3},\frac{4}{3})$ that meets these optimal values.

We conclude that the maximum and average linear information ratios of $\mathcal{F}+\mathcal{N}$ are 4/3 and 41/36, respectively.

6.2 An abelian (mixed-linear) scheme for $\mathcal{F}+\mathcal{N}$

We will work with a special type of abelian schemes that we call *mixed-linear*. Let Π_k's be linear SSSs for $k=1,\ldots,m$ and let $\Pi_k = (T_0^k, T_1^k, \ldots, T_n^k)$. We refer to the abelian schemes $\Pi_1 \oplus \cdots \oplus \Pi_m = (G_0, G_1, \ldots, G_n)$ as a mixed-linear

scheme where $G_i = T_i^1 \oplus \cdots \oplus T_i^m$. If the characteristics corresponding to the underlying finite fields are different, $\Pi_1 \oplus \cdots \oplus \Pi_m$ is non-linear. Informally, the secret space of $\Pi_1 \oplus \cdots \oplus \Pi_m$ is the Cartesian product of the secret spaces of Π_k's. To share a secret $(s_1, \ldots, s_m)$ using $\Pi_1 \oplus \cdots \oplus \Pi_m$, where s_k is in the secret space of Π_k, for each $k \in [m]$, we share s_k using Π_k with an independent randomness. Each participant in $\Pi_1 \oplus \cdots \oplus \Pi_m$ receives m shares, one from each Π_k, $k \in [m]$.

The following proposition follows from Lemma 6.2.

Proposition 6.1 (Mixed-linear convec set) *Denote the convec set of an access structure $\mathcal{A}$ with respect to the class of mixed-linear schemes by $\Sigma^{\text{MixL}}(\mathcal{A})$. Then, $\overline{\Sigma^{\text{MixL}}}(\mathcal{A}) = \text{convh}\left(\overline{\Sigma^{\text{LIN}}}(\mathcal{A})\right)$, where $\text{convh}(\mathcal{X})$, the convex hull of $\mathcal{X}$, is the set of all convex combinations of vectors in the subset $\mathcal{X} \subseteq \mathbb{R}^n$.*

Proof. Let $\Pi = (T_i)_{i \in Q}$ and $\Pi' = (T'_i)_{i \in Q}$ be two linear secret sharing schemes for $\mathcal{A}$, and denote their convecs with σ and σ', respectively. We need to show that for every real number $0 \leqslant x \leqslant 1$, there exists a sequence $\{\Pi''_j\}$ of mixed-linear scheme for $\mathcal{A}$ such that the sequence $\{\text{cv}(\Pi''_j)\}$ converges to $x\sigma + (1-x)\sigma'$.

Let $y = \log|T_0| / \log|T'_0|$ and $\{x_j\}, \{y_j\}$ be two sequences of non-negative rational numbers respectively converging to x and y, respectively. Let $x_j = c_j/d_j$ and $y_j = e_j/f_j$ where c_j, d_j, e_j, f_j are non-negative integers. The secret sharing scheme Π''_j is constructed as follows:

$$\Pi''_j = \underbrace{\Pi \oplus \ldots \oplus \Pi}_{f_j c_j \text{ times}} \oplus \underbrace{\Pi' \oplus \ldots \oplus \Pi'}_{e_j(d_j - c_j) \text{ times}} ,$$

where the notation $\oplus$ similarly defined as in the beginning of this subsection. Informally, the scheme works as follows. The secret space of Π''_j is $T_0^\ell \times T_0'^k$ where $\ell = f_j c_j$ and $k = e_j(d_j - c_j)$. To share a secret $(s_1, \ldots, s_\ell, s'_1, \ldots, s'_k)$, we share each s_i using an independent instance of Π and each s'_i using an independent instance of Π'. That is, each participant receives $\ell + k$ total pieces of shares.

It is easy to see that Π''_j is mixed-linear and it realizes $\mathcal{A}$. We continue to show that the sequence of convecs of Π''_j, $\{\text{cv}(\Pi''_j)\}$, converges to $x\sigma + (1-x)\sigma'$. We have

$$\begin{aligned}
\text{cv}(\Pi''_j) &= \frac{\log\left(|T_i|^\ell \cdot |T'_i|^k\right)}{\log\left(|T_0|^\ell \cdot |T'_0|^k\right)} \\
&= \frac{f_j c_j \log|T_i| + e_j(d_j - c_j)\log|T'_i|}{f_j c_j \log|T_0| + e_j(d_j - c_j)\log|T'_0|} \\
&= \frac{x_j}{x_j + (1-x_j)y_j/y} \frac{\log|T_i|}{\log|T_0|} + \frac{(1-x_j)}{x_j y/y_j + (1-x_j)} \frac{\log|T'_i|}{\log|T'_0|} ,
\end{aligned}$$

or more compactly,

$$\text{cv}(\Pi''_j) = \frac{x_j}{x_j + (1-x_j)y_j/y}\sigma + \frac{(1-x_j)}{x_j y/y_j + (1-x_j)}\sigma' ,$$

which clearly converges to $x\sigma + (1-x)\sigma'$, concluding the claim. □

Lemma 6.2 (Convex combination lemma) *Let Π and Π' be two mixed-linear SSSs for an access structure $\mathcal{A}$ with convecs σ and σ'. Then for every real number $x \in [0,1]$, there exists a family $\{\Pi''_j\}$ of mixed-linear schemes such that: 1) each Π''_j realizes $\mathcal{A}$, 2) the sequence of convecs of Π''_j's converges to $x\sigma + (1-x)\sigma'$.*

Remark 6.3 *Lemma 6.2 remains true even if we replace "mixed-linear" in the statement of lemma with p-linear, abelian or homomorphic; or if we remove it. That is, the lemma is not only true for the general schemes but also for p-linear, mixed-linear, abelian and homomorphic schemes.*

By our discussion in Section 6.1, $\mathcal{F} + \mathcal{N}$ has a p-linear scheme with convec σ_{odd} for every odd prime p and a 2-linear scheme with convec σ_{even}. Therefore, by letting $x = \frac{1}{2}$ in above lemma, it follows that $\mathcal{F}+\mathcal{N}$ has a family of mixed-linear (and hence abelian) schemes such that the sequence of their convecs converges to $\frac{1}{2}\sigma_{\text{odd}} + \frac{1}{2}\sigma_{\text{odd}} = (\frac{7}{6}, \frac{7}{6}, \frac{7}{6}, \frac{7}{6}, \frac{7}{6}, \frac{7}{6}, \frac{7}{6}, \frac{7}{6}, 1, \frac{7}{6}, \frac{7}{6}, \frac{7}{6})$. Consequently, the maximum and average mixed-linear (and hence abelian) information ratios of $\mathcal{F}+\mathcal{N}$ are at most 7/6 and 41/36, respectively. Using Proposition 6.1 and our lower-bounds for Fano and non-Fano (Proposition 4.4 and Proposition 4.5), we have verified by a computer that these values are tight for mixed-linear schemes. We refer the reader to Appendix B for further details. It remains open if these bounds are optimal for abelian schemes (this will be further discussed in Section 6.4).

We remark that similar to the nearly-ideal schemes, we do not have an abelian (mixed-linear) scheme for $\mathcal{F}+\mathcal{N}$ with maximum information ratio 7/6. Instead, for every $\epsilon > 0$, we have an abelian (mixed-linear) scheme with maximum information ratio $7/6 + \epsilon$.

6.3 On incompleteness of FKMP lower bound method

Farràs, Kaced, Molleví and Padró [28] introduced a new method (FKMP for short) for computing a lower bound on the information ratio of access structures. It integrates the common information (CI) property of random variables (which was studied in Section 2.4) in a linear programing by adding extra variables and extra constraints due to CI conditions. The method was implemented and successfully applied to several small access structures. Since linear, mixed-linear, abelian and homomorphic random variables all satisfy the CI property (Corollary 2.6), the FKMP lower bound applies not only to linear schemes but also to other three classes. Our result on superiority of abelian schemes to linear schemes implies that the FKMP method is "incomplete" for determining the optimal linear information ratio of access structures.

It remains open if the method is "incomplete" for determining the optimal mixed-linear, abelian or homomorphic information ratios of access structures too. In particular, it is an interesting problem to apply the FKMP method to see if a non-trivial lower bound for $\mathcal{F}+\mathcal{N}$ can be found. We remark that any new result in this direction should probably be achieved analytically; because the size of the corresponding linear programing is out of reach for nowadays computers.

6.4 Two open problems about abelian and homomorphic SSSs

By our previous discussions, the maximum information ratio and maximum mixed-linear information ratio of $\mathcal{F} + \mathcal{N}$ are respectively 1 and 4/3. Therefore, general secret sharing outperforms mixed-linear secret sharing. It remains open if general SSSs can outperform abelian ones too. Also, it remains open if (1) abelian schemes are superior to mixed-linear schemes, or (2) homomorphic schemes are superior to abelian schemes.

Probelm 6.4 (Abelian/Homomorphic convec set problems) *Is any of the following relations true for every access structure $\mathcal{A}$?*

- **(Abelian)** $\overline{\Sigma^{\text{Abl}}}(\mathcal{A}) = \overline{\Sigma^{\text{MixL}}}(\mathcal{A})$.
- **(Homomorphic)** $\overline{\Sigma^{\text{Hom}}}(\mathcal{A}) = \overline{\Sigma^{\text{Abl}}}(\mathcal{A})$.

If the answer to abelian convec set problem is positive, it shows that general SSSs are superior to abelian schemes. Nevertheless, one might be to prove superiority of general schemes to abelian schemes without solving the abelian convec set problem.

If the answer to abelian convec set problem is negative, it shows that abelian schemes are superior to mixed-linear (and in particular linear) schemes. Similarly, if the answer to the homomorphic convec set problem is negative, it shows that homomorphic (and hence general) schemes are superior to abelian schemes schemes.

In Section 7, we will talk more about consequences of negative answers to any of these problems; see Corollary 7.3.

7 On relation between convec sets and entropy regions

The motivations behind working with convec sets are three folds.

First, the extreme points of convec sets play an important role in constructing (optimal) secret sharing schemes via decomposition methods such as the (λ, ω)-decomposition discussed in Section 5.2. Second, it helps us to understand the limits of techniques for lower bounding information ratio of access structures better. A technique might be good enough to derive an inequality to determine the optimal information ratio, but it might fail to derive all inequalities necessary to describe the convec set completely. (The reader may refer to Appendix C for further discussions on these two motivations).

The rest of this section is devoted to discuss our third motivation, which is the following. Convec sets can help us to understand the structure of the so-called *entropy region*, introduced by Zhang and Yeung in [57]. In this section, we review the notion of entropy region and study its relation with convec sets.

7.1 Entropy region

The purpose of this subsection is to introduce the notations $\tilde{\Gamma}_n$, $\tilde{\Gamma}_n^{\text{Lin}}$, Γ_n^p, $\tilde{\Gamma}_n^{\text{MixL}}$, $\tilde{\Gamma}_n^{\text{Abl}}$, $\tilde{\Gamma}_n^{\text{Hom}}$ which will be used in the subsequent subsections. As we will see in

Section 7.2, in the context of secret sharing, they are related to the closures of the following sets Σ, Σ^{Lin}, Σ^{p}, Σ^{MixL}, Σ^{Abl} and Σ^{Hom}.

A point $h \in \mathbb{R}^{2^n-1}$, whose indices are indexed by non-empty subsets of $[n] = \{1, \ldots, n\}$, is said to be *entropic* if there exists a RV $(\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n)$ such that $h_A = \mathrm{H}(\boldsymbol{X}_A)$ for every non-empty $A \subseteq [n]$. If the RV is group-characterizable, h is said to be a group-characterizable entropic point. Similarly, p-linear, linear, mixed-linear, abelian and homomorphic entropic points are defined.

The set of all entropic points in $\mathbb{R}^{2^n-1}$ is called the *entropy region* on n RVs and is denoted by Γ_n. When we restrict to the class of group-characterizable (resp. p-linear/mixed-linear/abelian/homomorphic) entropic points, we use the notation Γ_n^{GC} (resp. $\Gamma_n^{p}, \Gamma_n^{\text{MixL}}, \Gamma_n^{\text{Abl}}, \Gamma_n^{\text{Hom}}$); notice that we have deliberately excluded the case of "linear" which will be handled separately. The closure of the entropy region is a convex set. Chan and Yeung [20] have proved that the closure of the entropy region is equal to the closure of the cone of all group-characterizable entropic points; that is, $\overline{\Gamma_n} = \overline{\text{cone}}\big(\Gamma_n^{\text{GC}}\big)$, where the cone of a set $\mathcal{X} \subseteq \mathbb{R}^n$ is defined to be $\text{cone}(\mathcal{X}) = \{\alpha x : x \in \mathcal{X}, \alpha \geqslant 0\}$. We refer to $\overline{\text{cone}}(\Gamma_n^{p})$ as the p-linear region and denote it by $\tilde{\Gamma}^{p}$. The mixed-linear, abelian and homomorphic regions are similarly defined and denoted by $\tilde{\Gamma}_n^{\text{MixL}}$, $\tilde{\Gamma}_n^{\text{Abl}}$ and $\tilde{\Gamma}_n^{\text{Hom}}$, respectively. To have a consistent notation, we denote the closure of the entropy region, i.e., $\overline{\Gamma_n}$, also by $\tilde{\Gamma}_n$, and also call it the entropy region which will be clear from the context. We let $\tilde{\Gamma}_n^{\text{Lin}} := \bigcup_{p:\text{prime}} \tilde{\Gamma}^{p}$ and and call it the linear regions. Notice that the relation $\tilde{\Gamma}_n^{\text{MixL}} = \text{convh}(\tilde{\Gamma}^{Lin})$ holds (see Definition 6.1 for definition of convex hull).

Similar to the closure of the entropy region, the p-linear, mixed-linear, abelian and homomorphic entropy regions are all convex sets. Although the linear entropy region is known to be convex for $n \leqslant 5$ [25], it is not the case for $n \geqslant 7$ [16, 26]. The situation is unknown for $n = 6$ [24].

Notice that the relation $\tilde{\Gamma}_n^{\text{Lin}} \subseteq \tilde{\Gamma}_n^{\text{MixL}} \subseteq \tilde{\Gamma}_n^{\text{Abl}} \subseteq \tilde{\Gamma}_n^{\text{Hom}}$ trivially holds true. Except for the first inclusion, which is known to be proper for $n \geqslant 7$ by [16], it remains open if the other inclusions are proper for any n. It remains open if $\tilde{\Gamma}_n^{\text{MixL}}$, $\tilde{\Gamma}_n^{\text{Abl}}$ and $\tilde{\Gamma}_n^{\text{Hom}}$ all coincide, which as we will see in next subsection, if this turns out to be the case, it shows that the answer to the abelian and homomorphic convec set problems (Problem 6.4) are both positive.

7.2 Entropy region and convec set

Next, we discuss the relation between different types of entropy regions and their corresponding convec sets. We explain the relation between $\tilde{\Gamma}_{n+1}$ and $\overline{\Sigma}(\mathcal{A})$, where $\mathcal{A}$ is an access structure on n participants (the extra variable corresponds to the secret). The other cases are similar.

We first remark that the correctness and privacy conditions in the definition of perfect realization for an access structure on n participants correspond to hyperplanes in $\mathbb{R}^{2^{n+1}-1}$. The set $\overline{\Sigma}(\mathcal{A})$ can equivalently be computed by the following steps. The intersection of the entropy region $\tilde{\Gamma}_{n+1}$ and the hyperplanes that describe the correctness and privacy conditions for the access structure

is computed. Each point of the resulting area is then scaled by dividing all coordinates to the entry that corresponds to the secret entropy. The obtained region, which is a (convex) subsets of $\mathbb{R}^{2^{n+1}-1}$, is then projected on the n entries that correspond to the participants share entropies. It can easily be seen that what we get is essentially $\overline{\Sigma}(\mathcal{A})$. Based on above discussion, we have the following proposition.

Proposition 7.1 *Let $\mathcal{A}$ be an access structure on n participants.*

- *If $\overline{\Sigma^{\text{MIXL}}}(\mathcal{A}) \subsetneq \overline{\Sigma^{\text{ABL}}}(\mathcal{A})$, then $\tilde{\Gamma}_{n+1}^{\text{MIXL}} \subsetneq \tilde{\Gamma}_{n+1}^{\text{ABL}}$.*
- *If $\overline{\Sigma^{\text{ABL}}}(\mathcal{A}) \subsetneq \overline{\Sigma^{\text{HOM}}}(\mathcal{A})$, then $\tilde{\Gamma}_{n+1}^{\text{ABL}} \subsetneq \tilde{\Gamma}_{n+1}^{\text{HOM}}$.*

Therefore, by studying SSSs one may gain some information about the structure of the entropy region with respect to different classes of RVs.

Here we discuss one such application. Recall that in Section 6.1 we almost determined the linear convec set of the 12-participant access structure $\mathcal{F} + \mathcal{N}$. Our almost matching lower and upper bounds for $\overline{\Sigma^{\text{LIN}}}(\mathcal{F} + \mathcal{N})$ is enough to deduce that it is a non-convex set. Consequently, the same thing holds for $\tilde{\Gamma}_n^{\text{LIN}}$ for any $n \geqslant 13$. This proves the existence of characteristic-dependent linear rank inequalities on at most 13 variables. The first examples of such inequalities were found in [16] which are on seven variables.

7.3 On completeness of the DFZ method

Recall that we index the indices of vectors in $\mathbb{R}^{2^n-1}$ with non-empty subsets of $[n]$. A vector $c \in \mathbb{R}^{2^n-1}$ is called a (linear) information inequality on n variables if for every entropic vector $h \in \Gamma_n$ it holds that $\langle c, h\rangle := \sum_{\varnothing \neq A \subseteq [n]} c_A h_A \geqslant 0$.

We call $c \in \mathbb{R}^{2^n-1}$ a rank inequality if $\langle c, h\rangle \geqslant 0$ for every linear entropic point $h \in \tilde{\Gamma}_n^{\text{LIN}}$ (this is equivalent to say for every $h \in \text{convh}\left(\tilde{\Gamma}_n^{\text{LIN}}\right) = \tilde{\Gamma}_n^{\text{MIXL}}$).

In [25], Dougherty, Freiling and Zeger have presented a method (called DFZ for short), using which they have been able to derive all rank inequalities on at most five variable. In particular, all known rank inequalities, including millions on six variables [24], have been derived using the DFZ method. The method employs the common information (CI) property of RVs which was defined in Section 2.5. In [25], it has been explicitly asked if the DFZ method is complete for determining all rank inequalities. Here is a formal description of completeness.

Completeness of the DFZ method. Let $\mathcal{I}_n$ denote the set of all rank inequalities on n variables derived using the DFZ method. We say that the DFZ method is complete for the (mixed-)linear region with n variables if and only if $\tilde{\Gamma}_n^{\text{MIXL}} = \bigcap_{c \in \mathcal{I}_n} \{h \in \mathbb{R}^{2^n-1} : \langle c, h\rangle \geqslant 0\}$. The completeness of the DFZ method can similarly be defined with respect to the abelian and homomorphic regions.

It is known that the DFZ method is complete for linear region for every $n \leqslant 5$ variables. In particular, for $n \leqslant 5$, the linear entropy region is a convex polytope; that is, it can be described as an intersection of finitely many half-spaces.

Recall that by Corollary 2.6, the CI property holds for homomorphic RVs and consequently abelian ones too. Therefore, for every $c \in \mathcal{I}_n$ and every homomorphic (and hence abelian) entropic point $h \in \mathbb{R}^{2^n}$, we have $\langle c, h\rangle \geqslant 0$. The following proposition then follows.

Proposition 7.2 *If the DFZ method is complete for the mixed-linear region with n variables, then $\tilde{\Gamma}_n^{\text{Hom}} = \tilde{\Gamma}_n^{\text{Abl}} = \tilde{\Gamma}_n^{\text{MixL}}$.*

We remark that the converse might not be true because, as we saw in Section 2.4, the CI property holds for a larger class of RVs (see Proposition 2.5).

By Proposition 7.1, we then have the following corollary.

Corollary 7.3 *If the DFZ method is complete for the mixed-linear region with $n+1$ variables, then for every access structure $\mathcal{A}$ on n participants, we have $\overline{\Sigma^{\text{Hom}}}(\mathcal{A}) = \overline{\Sigma^{\text{Abl}}}(\mathcal{A}) = \overline{\Sigma^{\text{MixL}}}(\mathcal{A})$. In particular, if the answer to abelian (resp. homomorphic) convec set problem (Problem 6.4) is not true, then for some n, the DFZ method is not complete for the mixed-linear (resp. abelian) region with n variables.*

We remark that even if the answer to both abelian and homomorphic convect set problems both turn out to be positive, we do not interpret it as a strong indication of completeness of the CI method in determining all linear rank inequalities. The reason is that, as we saw earlier, the CI property holds for a larger class of random variables (see Proposition 2.5).

8 Duality of abelian secret sharing schemes

In this section, we generalize the well-known result of [27,40] on duality of linear schemes to the class of abelian schemes. We first present the definition of access function [27] and dual of an access function. Access function is a generalization of the notion of access structure to allow non-perfect realization (with a control on the amount of information gained by every subset of participants on the secret). The dual of an access function is a natural generalization of dual of an access structure [40]. The dual of an access structure $\mathcal{A}$ on a participant set P is an access structure $\mathcal{A}^*$, on the same set of participants, defined as follows: $A \in \mathcal{A}^*$ if and only if $(P \backslash A) \notin \mathcal{A}$.

Definition 8.1 (Access function and its dual) *A mapping $\Phi : 2^P \to [0,1]$ is called an* access function *if $\Phi(\varnothing) = 0$, $\Phi(P) = 1$ and it is monotone; i.e., $A \subseteq B \subseteq P$ implies that $\Phi(A) \leqslant \Phi(B)$. The dual of Φ, denoted by Φ^*, is defined by $\Phi^*(A) = 1 - \Phi(P \backslash A)$, for every $A \subseteq P$.*

The access function of a secret sharing scheme $\Pi = (\boldsymbol{S}_i)_{i \in P}$ is defined by $\Phi_\Pi(A) = \frac{\mathrm{I}(\boldsymbol{S}_0 : \boldsymbol{S}_A)}{\mathrm{H}(\boldsymbol{S}_0)}$. The access function of an abelian scheme $\Pi = (G_i)_{i \in Q}$ can be computed by the simplified relation $\Phi_\Pi(A) = \frac{\log |G_0 \cap G_A|}{\log |G_0|}$, where $G_A = \sum_{i \in A} G_i$. This relation follows by properties of entropy function and the product formula

(which was mentioned in Section 2.4) for abelian groups (i.e., $|K+H| = \frac{|K||H|}{|K\cap H|}$). Also, its convec is simply given by $\mathrm{cv}(\Pi) = \left(\frac{\log|G_i|}{\log|G_0|}\right)_{i\in P}$.

Proposition 8.2 (Duality) *Let $\Pi = (G; G_0, G_1, \ldots, G_n)$ be an abelian scheme that satisfies $G_0 \subseteq \sum_{i=1}^n G_i$ (so that $\Phi_\Pi([n]) = 1$). Then, there exists an abelian scheme Π^* such that $\Phi_{\Pi^*} = \Phi^*_\Pi$ and $\mathrm{cv}(\Pi^*) \leqslant \mathrm{cv}(\Pi)$.*

Proof. Let $P = [n]$. We construct an abelian scheme $\Pi^* = (G^*; G_0^*, G_1^*, \ldots, G_n^*)$ such that $|G_0^*| = |G_0|$ and $|G_i^*| \leqslant |G_i|$. This proves the relation between the convecs. For proving the the relation between the access functions, since $|G_0^*| = |G_0|$, we essentially need to show that for every $A \subseteq P$, we have $\log|G_0^* \cap G_A^*| = \log|G| - \log|G_0 \cap G_{P\setminus A}|$, where $G_A = \sum_{i\in A} G_i$ and similarly $G_A^* := \sum_{i\in A} G_i^*$. Equivalently, we will prove the following equality:

$$|G_0^* \cap G_A^*| = \frac{|G|}{|G_0 \cap G_{P\setminus A}|} \ . \tag{8.1}$$

The dual construction. Consider the subgroup $C \subseteq \prod_{i\in Q} G_i$ whose elements are the vectors $(x_i)_{i\in Q} \in \prod_{i\in Q} G_i$ satisfying $\sum_{i\in Q} x_i = 0$. For every $i \in P$, let C_i be the subgroup of C whose projection on the ith component is zero. To define our dual abelian scheme Π^*, we let $G^* = \widehat{C}$ and $G_i^* = \{\alpha \in \widehat{C} | \alpha(C_i) = \{1\}\}$. The reader may recall the definition of Pontryagin dual given in Section 2.2.

The claim on convec. It is clear that $G_i^* = \widehat{(C/C_i)}$ since, in general, the subgroup of $\widehat{G}$ that vanishes on a subgroup $H \leqslant G$ is isomorphic to $\widehat{(G/H)}$. Note that the projection $C \to G_i$ that sends $(x_i)_{i\in Q}$ to x_i is onto for $i = 0$ (since $G_0 \subseteq \sum_{i=1}^n G_i$) and its kernel is C_0. So $G_0 \cong C/C_0$. Therefore, $|G_0^*| = \left|\widehat{(C/C_0)}\right| = |C/C_0| = |G_0|$. Also the projection $C \to G_i$ has kernel C_i so C/C_i is a subgroup of G_i; hence, $|G_i^*| = \left|\widehat{(C/C_i)}\right| = |C/C_i| \leqslant |G_i|$. The claim on convec then follows.

The claim on access function. To prove (8.1), we define $C_A = \bigcap_{i\in A} C_i$ for $A \subseteq P$ and prove two relations: (I) $G_0^* \cap G_A^* \cong \frac{C}{C_0+C_A}$ and (II) $\frac{C_0+C_A}{C_0} \cong G_0 \cap G_{P\setminus A}$. Equation (8.1) then follows because in the above we proved that $G_0 \cong C/C_0$.

Proof of (I). We claim that $G_A^* = \{\alpha \in \widehat{C} | \alpha(C_A) = \{1\}\}$. Notice that $C_A \subseteq C_i$ for all $i \in A$. Therefore, if $\alpha(C_i) = \{1\}$ then $\alpha(C_A) = \{1\}$. So $G_i^* \subseteq \{\alpha \in C^* | \alpha(C_A) = \{1\}\}$ and hence $\sum_{i\in A} G_i^* \subseteq \{\alpha \in C^* | \alpha(C_A) = \{1\}\}$. Conversely, if $\alpha \in \widehat{C}$ and $\alpha(C_A) = \{1\}$, then α, on input $(x_i)_{i\in Q}$, depends only on variables x_i for $i \in A$, i.e., $\alpha(x_0, x_1, \ldots, x_n) = \alpha(y_0, y_1, \ldots, y_n)$, where $y_i = 0$ for $i \notin A$ and $y_i = x_i$ for $i \in A$. Now we have $\alpha(y_1, \ldots, y_n) = \sum_{i\in A} \alpha(0, \ldots, 0, y_i, 0, \ldots, 0)$ and $\alpha(0, \ldots, 0, y_i, 0, \ldots, 0)$ is an element of G_i^* for $i \in A$. Therefore, $\alpha \in \sum_{i\in A} G_i^*$. It is easy to see that $G_0^* \cap G_A^* = \{\alpha \in \widehat{C} | \alpha(C_0 + C_A) = \{1\}\} \cong \left(\widehat{\frac{C}{C_0+C_A}}\right) \cong \frac{C}{C_0+C_A}$.

Proof of (II). Let $C_0 + C_A \to G_0$ be the projection onto the 0-th component. Then its kernel is C_0 and its image is $G_0 \cap G_{P\setminus A}$; because if $(x_i)_{i\in A} \in C_A$, then

$\sum_{i\in A} x_i = 0$ and for every $i \in A$, $x_i = 0$. Therefore $x_0 = -\sum_{i\in P\setminus A} x_i$ and hence $x_0 \in G_{P\setminus A}$. Therefore, $\frac{C_0+C_A}{C_0} \cong G_0 \cap G_{P\setminus A}$. □

9 On ideal homomorphic secret sharing schemes

The main goal of this section is to prove that every ideal homomorphic SSS can be converted to an ideal linear scheme, without changing its access structure.

Notation. We say that a SSS is homomorphic if, as a random variable, it is homomorphic (see Definition 2.3 for definition of homomorphic RVs). In this section, we simply refer to a subgroup Ω of a product group $\prod_{i\in Q} \Omega_i$ as a homomorphic secret sharing scheme; because, a uniform distribution on Ω induces a random variable $(\boldsymbol{S}_i)_{i\in Q}$, i.e., a secret sharing schemes. We assume that the projection of Ω on its i'th component is onto such that Ω_i is the support of Ω_i. For $x \in \Omega$, we denote the projection on entires with indices in a subset $A \subseteq Q$ by x_A; we use x_i for $i \in Q$.

Secret sharing with weak privacy. It is easier to prove our result for a security notion with a weaker privacy requirement for SSSs, introduced by Brickell and Davenport in [18]. They have proved that for ideal schemes, the two notions coincide. We show that the two notions coincide for general homomorphic schemes (Lemma 9.1 Part I).

Instead of requiring that unqualified subsets gain no information about the secret, the *weak privacy* requires that unqualified subsets must not be able to rule out any possibility for the secret. That is, for an unqualified subset $A \subseteq P$, we require the following holds: for any x (in the support of the secret sharing) and for any secret s, there exists some y (in the support of the secret sharing) such that $x_A = y_A$ and $y_0 = s$.

A key lemma. We need the following lemma for proving our main result of this section. Part (II) has been proved by Frankel, Desmedt and Burmester in [30] and Part (III) was proved in a subsequent work by Frankel and Desmedt in [29]. For completeness, we provide a simple and clean proof. In the remaining part of this section, we assume that our access structures have at least one minimal qualified subset of size at least two.

Lemma 9.1 (Homomorphic SSS) *Let $\Omega \subseteq \prod_{i\in Q} \Omega_i$ be a homomorphic SSS with weak privacy for an access structure $\mathcal{A}$. Then,*

(I) Ω is a perfect scheme for $\mathcal{A}$.
(II) the secret space, Ω_0, is an abelian group.
(III) if Ω is ideal, then $\Omega_0 \cong \Omega_i$.

Proof. For a subset $A \subseteq Q$, we have a projection map π_A from $\prod_{i=0}^{n} \Omega_i$ onto $\prod_{i\in A} \Omega_i$ and we use the notation Ω_A to denote the projection of the group Ω onto its A component $\prod_{i\in A} \Omega_i$ i.e., $\pi_A(\Omega)$.

(I) Since Ω is a SSS for $\mathcal{A}$ with weak privacy, for any $B \notin \mathcal{A}$, any $x \in \Omega$ and any $s \in \Omega_0$, one may find $y \in \Omega$ such that $y_B = x_B$ and $y_0 = s$. This is equivalent to the statement that the projection $\Omega \to \Omega_0 \times \Omega_B$ is onto. Since the pre-image of any point of an onto homomorphism of groups have exactly as many elements as the number of the elements of the kernel of that homomorphism, it follows that the number of $y \in \Omega$ with $y_B = x_B$ and $y_0 = s$ is independent of the choice of $s \in \Omega_0$. Hence Ω is a prefect SSS for $\mathcal{A}$.

(II) We need to show that for all $s_1, s_2 \in \Omega_0$, $s_1 \cdot s_2 = s_2 \cdot s_1$. Let $e \in \Omega$ be the identity element, that is, an element whose i component is the identity elements of the corresponding groups Ω_i. Let $A = \{j_1, j_2, \ldots, j_k\}$ be a minimal set in $\mathcal{A}$ of size at least 2 and, for $i = 1, 2$, let $A_i = A \backslash \{j_i\}$. Since $A_i \notin \mathcal{A}$ and $e \in \Omega$, there are $x(i) \in \Omega$ such that $x(i)_{A_i} = e_{A_i}$ and $x(i)_0 = s_i$. Then since any element in a group commutes with the identity element, we have $(x(1) \cdot x(2))_A = (x(2) \cdot x(1))_A$, and since $A \in \mathcal{A}$, we must have $(x(1) \cdot x(2))_0 = (x(2) \cdot x(1))_0$, that is $s_1 \cdot s_2 = s_2 \cdot s_1$.

(III) We first show that for a general homomorphic scheme Ω and for every $i \in Q$, the secret group Ω_0 is a sub-quotient of Ω_i; that is, there is an into group homomorphism from a subgroup of Ω_i to Ω_0. Let $A \in \mathcal{A}$ be a minimal set of size at least two that contains i and $A_1 = A \backslash \{i\}$. Let Ω_i' be the kernel of the projection $\pi_{A_1} : \Omega_A \to \Omega_{A_1}$. Then Ω_i' can be identified with a subgroup of Ω_i. We show that the restriction of the reconstruction homomorphism R_A to Ω_i' is an onto homomorphism to Ω_0. For any $s \in \Omega_0$ we need to find an element $y \in \Omega$ such that $y_{A_1} = e_{A_1}$ and $y_0 = s$, since then $y_A \in \Omega_i'$ and $R_A(y_A) = s$. This follows from the fact that $A_1 \notin \mathcal{A}$.
Therefore, there is an onto homomorphism from a subgroup Ω_i' of Ω_i onto Ω_0. But for an ideal Ω, since $|\Omega_i| = |\Omega_0|$, we must have $\Omega_i' = \Omega_i$ and the homomorphism must be an isomorphism; because an onto map between sets of the same size is also one to one. So all Ω_i's are isomorphic to Ω_0.

□

Now we provide two proofs for the main result of this section.

Theorem 9.2 *If an access structure admits an ideal homomorphic SSS, then it also admits an ideal linear SSS.*

Notation. For an integer m and an abelian group G, we use $m : G \to G$ for the homomorphism that sends x to $mx := x + \ldots + x$ (m times). We also use mG for the image of this map, which is a subgroup of G.

Proof. **(First)** Let Ω be an ideal homomorphic SSS for an access structure $\mathcal{A}$. By Lemma 9.1, without loss of generality, we can consider Ω as a subgroup of G^{n+1}, where G is a finite abelian group. Let p be a prime factor of $|G|$ and let Ω' be the image of Ω inside $\frac{G}{pG} \times \frac{G}{pG} \times \cdots \times \frac{G}{pG}$. We claim that Ω' is an ideal linear SSS for $\mathcal{A}$ which proves the theorem. A vector space over $\mathbb{F}_p$ is an abelian group V such that $pV = 0$. Therefore $\frac{G}{pG}$ is a vector space over $\mathbb{F}_p$ and Ω' is a subspace. To prove the claim, it is enough to show that for

every $A \in \mathcal{A}$, if for $x, y \in \Omega$ we have $x_A \equiv y_A \mod p$, then $x_0 \equiv y_0 \mod p$. Let $R_A : G^{|A|} \to G$ be the reconstruction function for the qualified subset A, where by definition it a homomorphism. It follows that R_A maps $pG^{|A|}$ to pG. Therefore, if $x_A - y_A \in pG^{|A|}$ then $x_0 - y_0 \in pG$. For $A \notin \mathcal{A}$, if $x \in \Omega$ and $s \in G$, we know that there is $y \in \Omega$ such that $x_A = y_A$ and $y_0 = s$. If we take everything modulo p, we get the required element in Ω' that verifies the condition of weak privacy for Ω'. □

Proof. **(Second)** Let Ω be an ideal homomorphic SSS for an access structure $\mathcal{A}$. By Lemma 9.1, without loss of generality, we can consider Ω as a subgroup of G^{n+1}, where G is a finite abelian group. Let r be the exponent of the group Ω inside $G \times \cdots \times G$. This is the smallest integer that $r\Omega = 0$. Choose a prime factor p of $|G|$. Since G has elements of order p, hence Ω that projects onto G surjectively has elements of order p; therefore $p|r$. Let $m = \frac{r}{p}$. We claim that $m\Omega$, as a subgroup of $mG \times \cdots \times mG$, is an ideal linear SSS for $\mathcal{A}$ which proves the theorem. Note that mG is a non-trivial abelian group such that $pmG = 0$. Hence, it is a vector space over $\mathbb{F}_p$ and $m\Omega$ is a subspace of $mG \times \cdots \times mG$. To prove the claim, we need to show that for every $A \in \mathcal{A}$, if $x, y \in m\Omega$ and $x_A = y_A$, then $x_0 = y_0$. But this is true for any $x, y \in \Omega$ and, therefore, it is true for $x, y \in m\Omega$. We need also to show that for every $A \notin \mathcal{A}$, if $x \in m\Omega$ and $s \in mG$, then there is $y \in m\Omega$ such that $x_A = y_A$ and $y_0 = s$. Let $x = mx'$ and $k = ms'$ for $x' \in \Omega$ and $s' \in G$. Since Ω is a SSS fo $\mathcal{A}$, there is $y' \in \Omega$ such that $x'_A = y'_A$ and $y'_0 = s'$. It follows that if we let $y = my' \in m\Omega$, we have found the required element. □

Discussion. Here we mention two consequences of the result of this section.

- We remark that we do not know if our result on duality of abelian secret sharing can be extended to homomorphic schemes, in general. However, by our third result, and the result on duality of multi-linear schemes, it can be concluded that the result on duality holds true for ideal homomorphic schemes. This consequence is particularly interesting since it is an open problem if the duality result holds for ideal secret sharing schemes or if it holds for the homomorphic secret sharing schemes. In next section, we discuss a more interesting consequence of this result.
- A well-known open problem in secret sharing is to prove or refute the following statement [52]: every ideal access structure admits an ideal multi-linear secret sharing scheme. Our result bring us one step closer to solving this problem since its is enough to prove or refute the following equivalent statement: every ideal access structure admits an ideal homomorphic secret sharing scheme.

10 Conclusion

We introduced the notion of mixed-linear secret sharing and presented some results about abelian and homomorphic secret sharing schemes. On of our main

goals was to understand the completeness of the following two methods, which both use the common information property of random variables: *DFZ* [25], a method for deriving linear rank inequalities, and *FKMP* [28], a method for deriving lower bounds on the multi-linear information ratio of access structures.

We showed that mixed-linear schemes are superior to multi-linear schemes, which proves the incompleteness of the FKMP method. The completeness or incompleteness of the DFZ method remains open. Solving the abelian and homomorphic open problems (Problem 6.4). Also, extending the duality of abelian schemes—proved in this paper and before only known to hold for multi-linear schemes—to the class of homomorphic schemes sounds challenging (we managed to handle the ideal case). If this extension fails to hold, it justifies the misbehavior of the lower bound obtained by the FKMP method with respect to duality, which was observed in [28].

References

1. Benny Applebaum and Barak Arkis. 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*, pages 317–344, 2018.
2. Benny Applebaum, Barak Arkis, Pavel Raykov, and Prashant Nalini Vasudevan. Conditional disclosure of secrets: Amplification, closure, amortization, lower-bounds, and separations. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, pages 727–757, 2017.
3. Benny Applebaum, Amos Beimel, Oriol Farràs, Oded Nir, and Naty Peter. Secret-sharing schemes for general and uniform access structures. *IACR Cryptology ePrint Archive*, 2019:231, 2019.
4. László Babai, Anna Gál, János Kollár, Lajos Rónyai, Tibor Szabó, and Avi Wigderson. Extremal bipartite graphs and superpolynomial lower bounds for monotone span programs. In *STOC*, pages 603–611, 1996.
5. László Babai, Anna Gál, and Avi Wigderson. Superpolynomial lower bounds for monotone span programs. *Combinatorica*, 19(3):301–319, 1999.
6. Amos Beimel, Aner Ben-Efraim, Carles Padró, and Ilya Tyomkin. Multi-linear secret-sharing schemes. In *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings*, pages 394–418, 2014.
7. Amos Beimel, Oriol Farràs, Yuval Mintz, and Naty Peter. Linear secret-sharing schemes for forbidden graph access structures. In *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part II*, pages 394–423, 2017.
8. Amos Beimel, Anna Gál, and Mike Paterson. Lower bounds for monotone span programs. *Computational Complexity*, 6(1):29–45, 1997.
9. Amos Beimel and Yuval Ishai. 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*, pages 188–202, 2001.
10. Amos Beimel, Eyal Kushilevitz, and Pnina Nissim. The complexity of multiparty PSM protocols and related models. 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 II, pages 287–318, 2018.
11. Amos Beimel and Noam Livne. On matroids and nonideal secret sharing. *IEEE Trans. Information Theory*, 54(6):2626–2643, 2008.
12. Amos Beimel, Noam Livne, and Carles Padró. 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.*, pages 194–212, 2008.
13. Amos Beimel and Enav Weinreb. Separating the power of monotone span programs over different fields. *SIAM J. Comput.*, 34(5):1196–1215, 2005.
14. Josh Cohen Benaloh. Secret sharing homomorphisms: Keeping shares of a secret secret. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 251–260. Springer, 1986.
15. George Robert Blakley. Safeguarding cryptographic keys. *Proc. of the National Computer Conference1979*, 48:313–317, 1979.
16. Anna Blasiak, Robert Kleinberg, and Eyal Lubetzky. Lexicographic products and the power of non-linear network coding. In *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*, pages 609–618, 2011.
17. Ernest F. Brickell. Some ideal secret sharing schemes. In *Advances in Cryptology - EUROCRYPT '89, Workshop on the Theory and Application of of Cryptographic Techniques, Houthalen, Belgium, April 10-13, 1989, Proceedings*, pages 468–475, 1989.
18. Ernest F. Brickell and Daniel M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology*, 4(2):123–134, 1991.
19. Renato M. Capocelli, Alfredo De Santis, Luisa Gargano, and Ugo Vaccaro. On the size of shares for secret sharing schemes. *J. Cryptology*, 6(3):157–167, 1993.
20. Terence H. Chan and Raymond W. Yeung. On a relation between information inequalities and group theory. *IEEE Trans. Information Theory*, 48(7):1992–1995, 2002.
21. László Csirmaz. The size of a share must be large. In *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, pages 13–22, 1994.
22. László Csirmaz. The size of a share must be large. *J. Cryptology*, 10(4):223–231, 1997.
23. Imre Csiszar and János Körner. *Information theory: coding theorems for discrete memoryless systems*. Cambridge University Press, 2011.
24. Randall Dougherty. Computations of linear rank inequalities on six variables. In *2014 IEEE International Symposium on Information Theory, Honolulu, HI, USA, June 29 - July 4, 2014*, pages 2819–2823, 2014.
25. Randall Dougherty, Christopher F. Freiling, and Kenneth Zeger. Linear rank inequalities on five or more variables. *CoRR*, abs/0910.0284, 2009.
26. Randall Dougherty, Eric Freiling, and Kenneth Zeger. Characteristic-dependent linear rank inequalities with applications to network coding. *IEEE Trans. Information Theory*, 61(5):2510–2530, 2015.
27. Oriol Farràs, Torben Brandt Hansen, Tarik Kaced, and Carles Padró. On the information ratio of non-perfect secret sharing schemes. *Algorithmica*, 79(4):987–1013, 2017.
28. Oriol Farràs, Tarik Kaced, Sebastià Martín Molleví, and Carles Padró. 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, pages 597–621, 2018.
29. Yair Frankel and Yvo Desmedt. Classification of ideal homomorphic threshold schemes over finite abelian groups (extended abstract). In *EUROCRYPT*, 1992.
30. Yair Frankel, Yvo Desmedt, and Mike Burmester. Non-existence of homomorphic general sharing schemes for some key spaces (extended abstract). In *CRYPTO*, 1992.
31. Peter Gács and János Körner. Common information is far less than mutual information. *Problems of Control and Information Theory*, 2(2):149–162, 1973.
32. Anna Gál. A characterization of span program size and improved lower bounds for monotone span programs. In *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23-26, 1998*, pages 429–437, 1998.
33. Anna Gál and Pavel Pudlák. A note on monotone complexity and the rank of matrices. *Inf. Process. Lett.*, 87(6):321–326, 2003.
34. Joseph Gallian. *Contemporary abstract algebra*. Nelson Education, 2012.
35. Yael Gertner, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. Protecting data privacy in private information retrieval schemes. *J. Comput. Syst. Sci.*, 60(3):592–629, 2000.
36. Branko Grünbaum, Victor Klee, Micha A Perles, and Geoffrey Colin Shephard. Convex polytopes. 1967.
37. Daniel Hammer, Andrei E. Romashchenko, Alexander Shen, and Nikolai K. Vereshchagin. Inequalities for shannon entropy and kolmogorov complexity. *J. Comput. Syst. Sci.*, 60(2):442–464, 2000.
38. Aubrey W Ingleton. Representation of matroids. *Combinatorial mathematics and its applications*, 23, 1971.
39. Mitsuru Ito, Akira Saito, and Takao Nishizeki. Secret sharing scheme realizing general access structure. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 72(9):56–64, 1989.
40. Wen-Ai Jackson and Keith M. Martin. Geometric secret sharing schemes and their duals. *Des. Codes Cryptography*, 4(1):83–95, 1994.
41. Wen-Ai Jackson and Keith M Martin. Perfect secret sharing schemes on five participants. *Designs, Codes and Cryptography*, 9(3):267–286, 1996.
42. Reza Kaboli, Shahram Khazaei, and Maghsoud Parviz. Group-homomorphic secret sharing schemes are group-characterizable with normal subgroups. *IACR Cryptology ePrint Archive*, 2019:576, 2019.
43. Mauricio Karchmer and Avi Wigderson. On span programs. In *Proceedings of the Eigth Annual Structure in Complexity Theory Conference, San Diego, CA, USA, May 18-21, 1993*, pages 102–111, 1993.
44. Ehud D. Karnin, J. W. Greene, and Martin E. Hellman. On secret sharing systems. *IEEE Trans. Information Theory*, 29(1):35–41, 1983.
45. Tianren Liu and Vinod Vaikuntanathan. Breaking the circuit-size barrier in secret sharing. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 699–708, 2018.
46. Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Conditional disclosure of secrets via non-linear reconstruction. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, pages 758–790, 2017.
47. Frantisek Matús. Two constructions on limits of entropy functions. *IEEE Trans. Information Theory*, 53(1):320–330, 2007.

48. Toniann Pitassi and Robert Robere. Lifting nullstellensatz to monotone span programs over any field. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 1207–1219, 2018.
49. Alexander A. Razborov. Applications of matrix methods to the theory of lower bounds in computational complexity. *Combinatorica*, 10(1):81–93, 1990.
50. Paul D. Seymour. On secret-sharing matroids. *J. Comb. Theory, Ser. B*, 56(1):69–73, 1992.
51. Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.
52. Juriaan Simonis and Alexei E. Ashikhmin. Almost affine codes. *Des. Codes Cryptography*, 14(2):179–197, 1998.
53. Douglas R Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Transactions on Information Theory*, 40(1):118–125, 1994.
54. Hung-Min Sun and Shiuh-Pyng Shieh. Secret sharing in graph-based prohibited structures. In *Proceedings IEEE INFOCOM '97, The Conference on Computer Communications, Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies, Driving the Information Revolution, Kobe, Japan, April 7-12, 1997*, pages 718–724, 1997.
55. Vinod Vaikuntanathan and Prashant Nalini Vasudevan. Secret sharing and statistical zero knowledge. In *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I*, pages 656–680, 2015.
56. Marten Van Dijk, Wen-Ai Jackson, and Keith M Martin. A general decomposition construction for incomplete secret sharing schemes. *Designs, Codes and Cryptography*, 15(3):301–321, 1998.
57. Zhen Zhang and Raymond W. Yeung. A non-shannon-type conditional inequality of information quantities. *IEEE Trans. Information Theory*, 43(6):1982–1986, 1997.

A Basics of group theory

For reader's convenience, we recall the basic concepts from group theory which are used in this paper. They can be found in any standard textbook in algebra, e.g., [34].

Group. A *group* is a tuple $(G, *)$ where G is a set and $*$ is a binary operation on G that satisfies the group axioms: *closure* (i.e., $a * b \in G$ for every $a, b \in G$), *associativity* (i.e., $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$), *identity* (i.e., there exists an element $e \in G$ called the identity such that $a * e = e * a = a$ for every $a \in G$) and *invertibility* (i.e., for every $a \in G$ there exists an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$).

Subgroup. A subset H of a group G is called a *subgroup* of G if it satisfies the group axioms under the operation of G. By Lagrange theorem, the order of a subgroup H of group G divides the order of G; i.e., $|H| \mid |G|$.

Coset and quotient set. Given a group G and a subgroup H, and an element $g \in G$, one can consider the corresponding left coset: $aH := \{ah : h \in H\}$. The set of all left cosets of a subgroup H in a group G is called the *quotient set*, denoted by G/H. In particular, $|G/H| = |G|/|H|$. The left cosets of a subgroup partition the group.

Normal subgroup and quotient group. A subgroup N of a group G is called *normal* if it is invariant under conjugation by members of G; that is, $gNg^{-1} = N$ for all $g \in G$. Indeed, for a normal subgroup N of G, the quotient set G/N admits a natural group structure, called the *quotient group*. The group operation is defined by $(aN) * (bN) = (a * b)N$ which can be shown to be well-defined.

Group homomorphism/isomorphism. Given two groups $(G, *)$ and $(H, \cdot)$, a *group homomorphism* from G to H is a mapping $\phi : G \to H$ such that for all $a, b \in G$ it holds that $\phi(a * b) = \phi(a) \cdot \phi(b)$. A bijective group homomorphism is called an *isomorphism*.

Kernel. The kernel of a group homomorphism $\phi : G \to H$ is the set of all elements of G that maps to e_H, the identity of H; i.e., $\ker \phi = \{g \in H : \phi(g) = e_H\}$. The kernel of ϕ is a normal subgroup of G.

The first isomorphism theorem. The image of any group G under a homomorphism is always isomorphic to a quotient of G. In particular, the image of G under a homomorphism $\phi : G \to H$ is isomorphic to $G/\ker(\phi)$.

Direct product group. The direct product of groups $(G, \bullet)$ and $(H, \cdot)$, denoted by $G \times H$, is a group defined on the set $G \times H$ by the natural group operation $(g_1, h_1) * (g_2, h_2) = (g_1 \bullet g_2, c_1 \cdot h_2)$.

B Lower and upper bounds for $\Sigma^{\mathrm{MixL}}(\mathcal{F} + \mathcal{N})$

Let $\mathbf{1}$ denote an all-1 vector of length six. For the purpose of this section let $p = 3$. Also, ignore to take the set closures into account.

Recall that in Section 4 we found lower bounds for $\Sigma^p(\mathcal{F})$ and $\Sigma^2(\mathcal{N})$. Also, in Section 5 we found upper bounds for them. Our lower and upper bounds where matching for $\Sigma^p(\mathcal{F})$, which determined its closure. Let $\Sigma^2_{\mathrm{lb}}(\mathcal{N})$ and $\Sigma^2_{\mathrm{ub}}(\mathcal{N})$ denote our lower and upper bounds for $\Sigma^2(\mathcal{N})$, respectively. It is easy to see that we have the following lower and upper bounds for $\Sigma^{\mathrm{MixL}}(\mathcal{F} + \mathcal{N})$.

$$\Sigma^{\mathrm{MixL}}_{\mathrm{lb}}(\mathcal{F} + \mathcal{N}) = \mathrm{convh}\Big\{ \{(\mathbf{1}, x) : x \in \Sigma^2_{\mathrm{lb}}(\mathcal{N})\} \cup \{(x, \mathbf{1}) : x \in \Sigma^p(\mathcal{F})\} \Big\} ,$$

$$\Sigma^{\mathrm{MixL}}_{\mathrm{ub}}(\mathcal{F} + \mathcal{N}) = \mathrm{convh}\Big\{ \{(\mathbf{1}, x) : x \in \Sigma^2_{\mathrm{ub}}(\mathcal{N})\} \cup \{(x, \mathbf{1}) : x \in \Sigma^p(\mathcal{F})\} \Big\} .$$

Using a computer, we have computed the half-space descriptions of the above sets which are given below:

$$\Sigma_{\mathrm{lb}}^{\mathrm{MixL}}(\mathcal{F}+\mathcal{N}): \begin{cases} x_i \geqslant 1, \\ i \in \{1,\ldots,12\} \\ \\ x_i + x_j + x_k + x_{10} + x_{11} + x_{12} \geqslant 7, \\ (i,j,k) \in \{(1,2,3),(1,5,6),(2,4,6),(3,4,5)\} \\ \\ x_i + x_j + x_k + x_\ell + x_7 + x_8 + x_9 \geqslant 7, \\ \ell \in \{10,11,12\} \\ (i,j,k) \in \{(1,2,3),(1,5,6),(2,4,6),(3,4,5)\} \\ \\ x_i + x_j + x_k + x_\ell + x_m + x_m + 2x_n \geqslant 8, \\ (\ell,m,n) \in \{(9,10,11),(9,11,10),(8,10,12), \\ (8,12,10),(7,11,12),(7,12,11)\} \\ (i,j,k) \in \{(1,2,3),(1,5,6),(2,4,6),(3,4,5)\} \end{cases}$$

$$\Sigma_{\mathrm{ub}}^{\mathrm{MixL}}(\mathcal{F}+\mathcal{N}): \begin{cases} x_i \geqslant 1, \\ i \in \{1,\ldots,12\} \\ \\ x_i + x_j + x_k + x_{10} + x_{11} + x_{12} \geqslant 7, \\ (i,j,k) \in \{(1,2,3),(1,5,6),(2,4,6),(3,4,5)\} \\ \\ x_i + x_j + x_k + x_\ell + x_7 + x_8 + x_9 \geqslant 7, \\ \ell \in \{10,11,12\} \\ (i,j,k) \in \{(1,2,3),(1,5,6),(2,4,6),(3,4,5)\} \\ \\ x_i + x_j + x_k + x_\ell + x_m + x_m + 2x_n \geqslant 8, \\ (\ell,m,n) \in \{(9,10,11),(9,11,10),(8,10,12), \\ (8,12,10),(7,11,12),(7,12,11)\} \\ (i,j,k) \in \{(1,2,3),(1,5,6),(2,4,6),(3,4,5)\} \\ \\ x_i + x_j + x_k + x_\ell + x_m + x_m + x_n + x_p \geqslant 8, \\ (\ell,m,n,p) \in \{(7,9,11,12),(7,9,11,10),(7,8,11,12), \\ (7,8,10,12)(8,9,10,5)(8,9,10,12)\} \\ (i,j,k) \in \{(1,2,3),(1,5,6),(2,4,6),(3,4,5)\} \end{cases}$$

Even though, the lower and upper bounds on $\Sigma^{\mathrm{MixL}}(\mathcal{F}+\mathcal{N})$ do not match, they are sufficient to determine the exact value of the maximum and average mixed-linear information ratios of $\mathcal{F}+\mathcal{N}$.

C On usefulness of convec sets

In an unpublished work, we have shown that, using the (λ,ω)-decomposition, almost all extreme convecs of all linear convec sets of access structures on five

participants can recursively be constructed. We start from an initial collection of convecs and take the duality of linear schemes into account. That is, when a new scheme with convec σ is constructed for an access structure $\mathcal{A}$, the dual pairs $(\mathcal{A}, \sigma)$ and $(\mathcal{A}^*, \sigma)$ are added to the collection. Our initial collection includes all extreme convecs of access structures on at most four participants and all ideal access structures on five participants. The initial collection were all known by 1996 [41], however, the linear optimal schemes for some access structures on five participants were only determined in 2018 [28], by direct construction.

Our method constructs all extreme convecs of all linear convec sets of access structures on five participants, except 7 convecs. By duality and symmetry, essentially 3 convecs can not be constructed (which fortunately they have very simple constructions). Our results show that the (λ, ω)-decomposition is not a complete method for construing every secret sharing scheme with an extreme convec, even if we assume that all ideal access structures are known.

We have also tried to use the FKMP method [28] to determine the linear convec set of small access structures. We have been able to find the optimal linear convec set for all access structures on five participants. For graph access structures on six participants, we have been able to find the optimal linear convec set of almost all access structures. We have not been able to determine the linear convec set of a few graph access structures on six participants. It is not clear to us yet, if this is a computational imitation, or if it is an inherent weakness of the FKMP method in determining the exact linear convec set of access structures.