On Ideal and Weakly-Ideal Access Structures

Reza Kaboli, Shahram Khazaei, Maghsoud Parviz

Sharif University of Technology
Department of Mathematical Sciences
{rezakaboli69,shahram.khazaei,maghsoud.parviz}@gmail.com

Abstract. For more than two decades, proving or refuting the following statement has remained a challenging open problem in the theory of secret sharing schemes (SSSs): *every ideal access structure admits an ideal perfect multi-linear SSS*. We consider a weaker statement in this paper asking if: *every ideal access structure admits an ideal perfect group-characterizable (GC) SSS*. Since the class of GC SSSs is known to include the multi-linear ones (as well as several classes of non-linear schemes), it might turn out that the second statement is not only true but also easier to tackle. Unfortunately, our understanding of GC SSSs is still too basic to tackle the weaker statement. As a first attempt, it is natural to ask if every ideal perfect SSS is equivalent to some GC scheme. The *main contribution* of this paper is to construct counterexamples using tools from theory of Latin squares and some recent results developed by the present authors for studying GC SSSs.

As a *minor contribution*, we also study the above two statements with respect to several variations of weakly-ideal access structures.

Key words: ideal secret sharing schemes, linear secret sharing, group-characterizable secret sharing, ideal access structure

1 Introduction

A *secret sharing scheme (SSS)* is used by a dealer to share a secret among a set of n participants by giving a share to each one. The dealer uses a fixed and publicly-known *sharing map* $\mu : \mathcal{S}_0 \times \mathcal{R} \to \mathcal{S}_1 \times \ldots, \mathcal{S}_n$, where $\mathcal{S}_0$ is the *secret space*, $\mathcal{S}_i$ is the *share space* of the i'th participant and $\mathcal{R}$ is the *randomness space*. Given a secret $s_0 \in \mathcal{S}_0$, the dealer chooses a randomness $r \in \mathcal{R}$, according to some known distribution (which might depend on s_0), and then computes the shares as $(s_1, \ldots, s_n) = \mu(s_0, r)$. The share s_i is then privately transferred to the i'th participant.

The most common notion of security for SSSs is *perfect* security. In a perfect SSS, it is required that every subset of participants either fully recover the secret, in which case the subset is called *qualified*, or gain no information about it. The set of all qualified subsets of participants is called an *access structure*.

The efficiency of a SSS is quantified using the notion of *information ratio*, defined to be the ratio between the largest share size and the secret size. The (perfect) information ratio of an access structure is the infimum of all information ratios of SSSs that perfectly realize it.

Linear and multi-linear SSS. The most well-studied type of SSS is the class of *multi-linear* schemes. In these schemes, the secret, share and randomness spaces are all *vector spaces* and the sharing map is linear. That is, the secret is composed of some finite field elements and the sharing is done by applying the sharing map on the secret elements and some randomly chosen elements from the finite field. When the secret is composed of a single field element, the scheme is called *linear*.

Group-characterizable SSS. Group-characterizable (GC) SSSs have recently been studied in a few works. We will review known results in Section 1.3. GC schemes are generalizations of several classes of SSSs, including multi-linear, abelian and homomorphic[1] schemes and probably a rich subclass of non-linear ones.

A GC scheme is defined by a finite group $(G, *)$, called the *main group*, and a collection $G_0, G_1, \ldots, G_n$ of its subgroups. The reader may refer to Appendix A for basics of abstract algebra. The secret space is the quotient set G/G_0 and the share space of the i'th participant is the quotient set G/G_i. To share a secret $s_0 \in G/G_0$, the dealer chooses a random $g \in G$ such that $s_0 = gG_0$ (there are $|G|/|G_0|$ such elements). The shares are then computed as $(s_1, \ldots, s_n) = (gG_1, \ldots, gG_n)$. That is, the i'th participant's share is the coset gG_i.

Non-perfect security notions. Several non-perfect security notions for SSSs have appeared in the literature, notably the following three ones (in decreasing level of security): *statistically-perfect* [8], *almost-perfect* [15] and *quasi-perfect* [25, Chapater 5]. Non-perfect SSSs allow some degree of imperfection in correctness and privacy, and they differ in how to quantize the amount of missed information by the qualified sets and leaked information to the unqualified ones. Non-perfect security notions have been recently studied in [22] and the following two main results have been proved. First, the information ratio of an access structure with respect to all non-perfect security notions coincides with perfect information ratio for the class of linear schemes. Second, for the general class of SSSs (i.e., non-linear), information ratio is invariant with respect to all non-perfect security notions, but it remains open whether it also coincides with perfect security.

1.1 Ideal SSS: an old problem and a new one

A SSS is said to be *ideal* if the secret size and all share sizes are equal. An access structure is called ideal if it is realizable by a perfect ideal SSS. Despite several notable results, characterization of ideal access structures is still an open problem. We will review the related literature in Section 1.3. All *known* ideal access structures are realizable by some ideal perfect multi-linear SSS. A long standing open problem in theory of SSSs (with consequences in matroid theory too, see Section 1.3) is to prove or refute the following statement, first raised by Simonis and Ashikhmin in [39].

[1] In a homomorphic scheme, multiplying the corresponding shares of two secrets results in valid shares for the product of the secrets.

Statement 1.1 (Multi-linear/Ideal) *Every ideal access structure admits an ideal perfect multi-linear SSS.*

It is known that SSSs whose secret spaces are of size two or three are linear [4]. Recently, Jafari and Khazaei [21] have shown that every ideal perfect homomorphic SSS can be transformed into an ideal perfect multi-linear scheme that realizes the same access structure. In another recent work [23], the present authors have shown that every homomorphic SSS is equivalent to some GC SSS with *normal* subgroups in the main group (i.e., $G_0, G_1, \ldots, G_n$ are all normal subgroups in G). Therefore Statement 1.1 is equivalent to the following: *every ideal access structure admits an ideal perfect GC SSS with normal subgroups.*

Since the original open problem has resisted all efforts for more than two decades, and GC SSSs are probably a much richer class than the GC schemes with normal subgroups, it makes sense to first try to prove or refute the following weaker statement.

Statement 1.2 (GC/Ideal) *Every ideal access structure admits an ideal perfect GC SSS.*

If Statement 1.2 turns out to be wrong, so does Statement 1.1. If Statement 1.2 turns out to be true, the next step would be—e.g., similar to the approach of [21]—to see if there exists a way to transform a perfect ideal GC SSS into a perfect ideal GC scheme with normal subgroups, that still realizes the same access structure.

1.2 Contributions

Unfortunately, our understanding of GC SSSs is still in its infancy state, and due to lack of enough tools and techniques we are not yet ready to prove or refute Statement 1.2. In this paper, we present the following results.

(I) **On group-characterizability of ideal SSSs.** The first natural attempt for proving Statement 1.2, if true, is *to see if every ideal perfect SSS is equivalent to some GC SSS*. Our main result in this paper is to show that this naive approach fails to work. That is, there exists ideal perfect SSSs which are not equivalent to any GC scheme. Therefore, more sophisticated methods are needed to prove the statement, if true. Again, a natural approach for doing so, is to find a generic method that transforms any ideal perfect SSS into an ideal perfect GC scheme, for the same access structure.

Challenges and tools. We remark that our result is not as trivial as it might seem at first. First, not many examples of non-linear SSSs are known in the literature. Second, assuming that one finds a candidate, how would one prove that it is not equivalent to any GC SSS?

Solution. We use the connection between Latin squares and ideal access structures for the (2,2)-threshold access structure, first realized by Seymour in [36]. Once we find such candidates, we use our recent result [23] which allows one to recognize if a SSS is equivalent to any GC one.

(II) **On weakly-ideal access structures.** Since proving or refuting both Statement 1.1 and Statement 1.2 remain challengingly open for ideal access structures, our next goal is to see if similar statements are satisfied for weaker notions of ideality.

Four weak variants. In [6], Beimel and Livne have named an access structure *nearly-ideal* if it admits a perfect SSS with information ratio arbitrarily close to one. Also, a nearly-ideal access structure which is not ideal was exhibited in [5]. Another approach to study other notions of weakly-ideal access structures is to work with non-perfect SSSs instead of perfect ones. Each non-perfect security notion mentioned earlier leads to a natural notion of weak ideality for access structures as follows: *quasi-ideal*, *almost-ideal* and *statistically-ideal*. The recent result of Jafari and Khazaei [22] shows that these three notions of ideality are equivalent.

Observations. One may wonder if Statement 1.1 or Statement 1.2 holds true for any of the mentioned variants of weakly-ideal access structures; but of course, the statements need to be slightly modified (see Questions 5.2 and 5.6). We show that none of the four variants of weakly ideal access structures mentioned above are realizable by "close-to-ideal" multi-linear SSSs. This result follows by two recent results by Jafari and Khazaei: 1) for the class of linear schemes, the information ratio of an access structure is invariant with respect to all non-perfect security notions as well as perfect security [22] and 2) there exists a nearly-deal access structure that does not admit a close-to-ideal perfect linear SSS [21]. Also, we show that quasi-ideal access structures are realizable by "close-to-ideal" GC SSSs, which follows by the following observations. GC random variables completely characterize the topological closure of the so-called *entropy region* [41] due to a remarkable result by Chan and Yeung [14]. A direct consequence of this result is that in the computation of information ratio of access structures with respect to quasi-perfect security, we can restrict ourselves to the class of GC SSSs. It is unknown if this is true for perfect or any other non-perfect security notion. In particular, it remains an open question if the other three variants of weakly-ideal access structures are realizable by "close-to-ideal" GC SSSs. A summary of these observations is given in Table 1 (Section 7).

(II) **Towards a weak characterization of ideal access structures.** Mejia and Montoya [33] have presented to some extent a characterization theorem for ideal access structures that admit ideal multi-linear SSSs. It is an interesting topic for research to see if their result can be extended to other classes of ideal access structures. Since in this paper we are focusing on ideal access structures that admit GC SSSs, we use this opportunity to provide some tools which might be useful for the study of such possible extensions to this class.

1.3 Related works

In this section, we review known and related results about ideal and GC SSSs.

Ideal SSSs. SSSs were introduced in two independent works by Shamir [37] and Blakely [9] for the case of *threshold access structures* (i.e., a set is qualified if and only if its size is larger than a certain threshold). Shamir's scheme was perfectly secure, but Blakely's was statistically secure. Secret sharing for *general access structures* was introduced by Ito, Saito and Nishizeki [20]. It was proved by Karnin et. al. [27] that perfect realization is not possible with share sizes smaller than the secret size. The notions of *ideal SSS* and *ideal access structure* were introduced in a remarkable work by Brickell and Davenport [10], in which they discovered that every ideal SSS is induced by a *matroid*. Seymour showed that the access structures induced by matroids are not necessarily ideal [36]. Matroids which correspond to ideal SSSs were subsequently called *entropic* (e.g., see [35]). Ideal SSSs are not only equivalent to entropic matroids, but also to *p-representable matroids* [30] and *almost affine codes* [39]. Despite several important works (e.g., see [1, 3, 7, 29–31, 38]), the characterization and classification of ideal SSSs is still an open problem. Simonis and Ashikhmin [39] proved that the class of ideal multi-linear SSSs is strictly larger than that of the linear ones (because, e.g., the non-Pappus matroid is not representable) and raised the question if every ideal access structure admits an ideal multi-linear SSS.

Recently, Jafari and Khazaei [21] showed that every ideal homomorphic SSS can be converted into an ideal multi-linear scheme, with the same access structure. This shows that in the case of ideal access structures, homomorphic and linear SSSs have the same power. But, for general access structures, Jafari and Khazaei [21] also showed that homomorphic SSSs outperform multi-linear ones.

Group-characterizable SSSs. The notion of GC random variables was introduced by Chan and Yeung in [14], where they proved that the GC random variables are rich enough to completely characterize the (topological) closure of the so-called *entropy region* [11] (defined to be the set of all entropic polymatroids). GC RVs include several classes of well-known RVs. Multi-linear, abelian and Homomorphic SSSs are all known to be GC. In particular in [23] it was shown that every homomorphic SSS is equivalent to some GC scheme with normal subgroups in the main group. Additionally, a necessary and sufficient condition was given for a SSS to be equivalent to some GC scheme (which will be recalled and used in this paper). In [23], it was also proved that for the class of GC SSSs whose secret subgroup (G_0) is normal in the main group (G), the almost-perfect, statistical and perfect security notions all coincide.

GC random variables have also been studied in other works (e.g., [12, 13, 18, 40]), which are not directly related to SSSs.

1.4 Paper structure

The paper is organized as follows. In Section 2, we present the notations and basic concepts. In Section 3, we review the results of [23], which is a necessary and sufficient condition for a SSS to be *inherently group-characterizable*. In Section 4, using the necessary condition mentioned in Section 3, we present ideal perfect SSSs which are not inherently GC. Weakly-ideal access structures are studied in

Section 5. In Section 6 we recall and study Mejia and Montoya's classification-like theorem of ideal access structures that admit ideal multi-linear schemes. The paper is concluded in Section 7.

2 Preliminaries and notation

In this section, we introduce our notation and basic concepts. We refer to [2] for a survey on SSSs. For the reader's convenience we review the basic concepts of abstract algebra in Appendix A.

Notation. We use boldface letters for random variables (RVs). For a positive integer n, $[n]$ stands for the set $\{1, 2, \ldots, n\}$. All RVs considered in this paper are discrete with finite supports. The support and Shannon entropy of a RV $\mathbf{x}$ are denoted by $\operatorname{supp}(\mathbf{x})$ and $\mathrm{H}(\mathbf{x})$, respectively. The mutual information of RVs $\mathbf{x}, \mathbf{y}$ is denoted by $\mathrm{I}(\mathbf{x} : \mathbf{y}) := \mathrm{H}(\mathbf{x}) + \mathrm{H}(\mathbf{y}) - \mathrm{H}(\mathbf{x}, \mathbf{y})$. Also, $\mathrm{H}(\mathbf{x}|\mathbf{y}) := \mathrm{H}(\mathbf{x}) - \mathrm{I}(\mathbf{x} : \mathbf{y})$.

2.1 Secret sharing schemes

A secret sharing scheme (SSS) is usually meant to be used by a *dealer* to share a secret among a set of participants as follows. The dealer chooses a randomness according to a pre-specified distribution and applies a fixed and public mapping on the secret and randomness to compute the share of each participant. This definition does not consider a priori a distribution on the secret space. In this paper, we use the following equivalent definition.

Definition 2.1 (Secret sharing scheme) *A secret sharing scheme (SSS), on participants set $[n]$, is a joint distribution $\Pi = (\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_n)$, where $\mathbf{x}_0$ is the secret RV with $\mathrm{H}(\mathbf{x}_0) > 0$ and $\mathbf{x}_i$ is the share RV of participant $i \in [n]$.*

A dealer samples $(x_0, x_1, \ldots, x_n)$ according to the joint distribution $\mathbf{x}$ and keeps x_0 as the secret for himself. He then privately transfers the share x_i to participant i. If the dealer wishes to share a given secret $x_0 \in \operatorname{supp}(\mathbf{x}_0)$, he samples from distribution $\mathbf{x}$ a tuple $(x_0, x_1, \ldots, x_n)$ conditioned on the event $[\mathbf{x}_0 = x_0]$. The shares are then determined by the sampled tuple.

Perfect security. The most common type of security notion for a SSS is that of *perfect* security. In a perfectly-secure SSS, the secret can be reconstructed only by qualified subsets and it must remain information-theoretically hidden from unqualified sets. This concept is formalized using the following two definitions.

Definition 2.2 (Access structure) *Let $[n]$ be a set of participants. We refer to a non-empty subset $\Gamma \subseteq 2^{[n]}$, with $\varnothing \notin \Gamma$, as an access structure if it is monotone; i.e., if $A \in \Gamma$ and $A \subseteq B \subseteq [n]$ then $B \in \Gamma$. The elements of Γ are called qualified and those of $2^{[n]} \backslash \Gamma$ are called unqualified.*

Definition 2.3 (Perfect realization) *We say that a SSS $(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_n)$ is a perfect scheme for an access structure Γ on participants set $[n]$ if the following two conditions hold:*

- *(***Correctness***)* $\mathrm{H}(\mathbf{x}_0|\mathbf{x}_A) = 0$*, for every qualified subset* $A \in \Gamma$*,*
- *(***Privacy***)* $\mathrm{I}(\mathbf{x}_0 : \mathbf{x}_A) = 0$*, for every unqualified subset* $A \in \Gamma^c$*,*

where for a subset $A \subseteq [n]$*,* $\mathbf{x}_A = (\mathbf{x}_i)_{i \in A}$ *denotes the marginal distribution on coordinates with elements in* A*.*

Perfect information ratio. There is a well-known parameter, called information ratio, for quantifying the efficiency of SSSs. The information ratio of participant i in the SSS $\Pi = (\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_n)$ is defined to be $\mathrm{H}(\mathbf{x}_i)/\mathrm{H}(\mathbf{x}_0)$. The information ratio of a SSS is the maximum of all participants' information ratios. The (perfect) information ratio of an access structure is defined as the infimum of the information ratios of all SSSs that perfectly realize it.

2.2 Multi-linear secret sharing schemes

The most common types of SSSs fall into the class of multi-linear schemes. In these schemes, the secret is composed of some finite field elements and sharing is done by applying some fixed linear mapping on the secret elements and some randomly chosen elements from the finite field. Several equivalent definitions exist for multi-linear schemes. Here, we present two definitions, which are known to be equivalent (e.g., see [23, Appendix C].

Definition 2.4 (Multi-linear SSS) *A multi-linear SSS can be defined in any of the following equivalent ways.*

I. **(linear maps)** *Let* $\mu_i : U \to U_i$ *be a linear map for every* $i \in \{0, 1, \dots, n\}$*, where* U *and* U_i*'s are all finite dimensional vector spaces on a finite field* $\mathbb{F}$*. We refer to* $(\mu_0(\mathbf{u}), \mu_1(\mathbf{u}), \dots, \mu_n(\mathbf{u}))$ *as a multi-linear SSS, where* $\mathbf{u}$ *is a uniform RV on* U*.*

II. **(affine subspaces)** *Let* V *be a finite-dimensional vector space on a finite field* $\mathbb{F}$ *and* $V_0, V_1, \dots, V_n$ *be subspaces of* V*. We refer to* $(\mathbf{v} + V_0, \mathbf{v} + V_1, \dots, \mathbf{v} + V_n)$ *as a multi-linear SSS, where* $\mathbf{v}$ *is a uniform RV on* V*. Here, the support of RV* $\mathbf{v} + V_i$ *is the set of all affine subspaces parallel to* V_i *(i.e.,* $\{v + V_i \mid v \in V\}$ *where* $v + V_i$ *is the translation of* V *by the vector* v*).*

III. **(Subspace collection)** *Let* T *be a finite-dimensional* $\mathbb{F}$*-vector space and* $T_0, T_1, \dots, T_n$ *be a collection of subspaces of* T*. Let* $\boldsymbol{\alpha}$ *be a uniform RV on* $T^* = \{\alpha \mid \alpha : T \to \mathbb{F}$ *is a linear functional*$\}$*, the dual space of* T*. We refer to* $(\boldsymbol{\alpha}|_{T_0}, \boldsymbol{\alpha}|_{T_1}, \dots, \boldsymbol{\alpha}|_{T_n})$ *as a multi-linear SSS. Here,* $\boldsymbol{\alpha}|_{T_i}$ *is the same mapping as* α *but its domain has been restricted to* T_i*.*

The first definition corresponds to the description which was given in the beginning of this subsection: simply let $\mathbf{u} = (\mathbf{s}, \mathbf{r})$ and $\mu_0(\mathbf{s}, \mathbf{r}) = \mathbf{s}$, where $\mathbf{s}$ is the secret and $\mathbf{r}$ is the randomness. The second definition is useful to view the multi-linear schemes as a subclass of group-characterizable SSSs, which is defined in next subsection. The third definition is closely related to definition of SSSs in terms of the so-called *(multi-target) monotone span programs* [3,26]. We refer to [22, Section 2.5] for an explanation of this connection.

2.3 Group-characterizable SSSs

The notion of GC RVs was introduced by Chan and Yeung in the information theory literature in 2002 [14]. Here we tailor the definition for SSSs. It can be viewed as a generalization of the second definition given above for multi-linear SSSs.

Definition 2.5 (GC scheme) *Let $(G, *)$ be a finite group, $G_0, G_1 \ldots, G_n$ be some subgroups of G and $\mathbf{g}$ be a uniform RV on G. We refer to the joint RV $(\mathbf{g}G_0, \mathbf{g}G_1, \ldots, \mathbf{g}G_n)$ as a* group-characterizable *(GC) SSS, induced by the tuple $[G : G_0, G_1, \cdots, G_n]$. Here, $\mathbf{g}G_i$ is a RV whose support is the left cosets of G_i in G.*

Group-characterizable SSSs generalize several classes of SSSs including multilinear ones, as discussed above, abelian ones [21] and homomorphic ones [23].

3 On inherently group-characterizable SSSs

In [23], SSSs which are "'equivalent" to some GC scheme have been called *inherently group-characterizable (IGC)*. The formal definition is given below.

Definition 3.1 (IGC scheme) *A SSS $\Pi = (\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_n)$ is called* inherently group-characterizable *(IGC) if there exist a GC SSS $\Pi' = (\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_n)$ and a tuple $(f_0, f_1, \ldots, f_n)$ of mappings $f_i : \text{supp } (\mathbf{x}_i) \to \text{supp}(\mathbf{y}_i)$ such that the random variable Π' is identically distributed as $(f_0(\mathbf{x}_0), f_1(\mathbf{x}_1), \ldots, f_n(\mathbf{x}_n))$.*

In this section, we recall a theorem proved in [23], which gives a necessary and sufficient condition for a RV to be IGC. We first present some definitions and then the theorem.

3.1 Some basic definitions

We recall two *group actions*[2] on matrices defined in [23]. The set of all permutations on $[m]$, called the *symmetric group* of order m is denoted by $\mathbb{S}_m$.

Definition 3.2 (Permutation action) *Let M be a matrix with m rows and $\sigma \in \mathbb{S}_m$. The action $\sigma \cdot M$ is defined to be a matrix with the same number of rows whose i'th row is the $\sigma(i)$'th row of M.*

Definition 3.3 (Reordering action) *Let $M = [m_{ij}]_{m\times n}$ be a matrix and denote its jth column by M^j. A* reordering *for M is a tuple $f = \left(f^1, f^2, \ldots, f^n\right)$ such that f^j, $j \in [n]$, is a permutation on the set of distinct elements of M^j. The action $f \cdot M$ is defined as follows, where f^j acts on the j'th column by $f^j \cdot M^j = [f^j(m_{ij})]_{m\times 1}$:*

$$f \cdot M = [f^1 \cdot M^1 | f^2 \cdot M^2 | \cdots | f^n \cdot M^n] \ .$$

[2] The action of a group G on a set X is a well-known concept in group theory, defined by a mapping $\cdot : G \times X \to X$, which has some specific properties. We do not need the complete definition in this paper.

Sometimes, reordering of a matrix behaves the same way as permuting the rows. This was a motivation for the following definition in [23].

Definition 3.4 (Automorphisms group of a matrix) *Let M be a matrix with m rows. The set of all automorphisms of M is defined as follows,*

$$\mathrm{Aut}(M) = \{\sigma \in \mathbb{S}_m : \sigma \cdot M = f \cdot M, \text{ for some reordering } f \text{ of } M\}.$$

Each element of $\mathrm{Aut}(M)$ *is called an* automorphism.

It turns out that $\mathrm{Aut}(M)$ is a subgroup of $\mathbb{S}_m$. Also, the reordering that corresponds to an automorphism σ is unique, which we denote by f_σ.

3.2 A necessary and sufficient condition for inherent group-characterizability

Theorem 3.5, proved in [23], provides a necessary and sufficient condition for a SSS to be IGC. First we need to define the matrix representation of a SSS.

Matrix representation of a SSS. A SSS on n participants can be represented by a matrix with $n + 1$ columns, by considering the distinct elements of the support of the SSS as the rows of the matrix. Of course, a non-zero probability needs to be assigned to each row to fully specify the scheme, but for uniform distributions it can be ignored. In particular, the following two classes of SSSs are known to be uniformly distributed on their supports: the GC class [11] and the ideal perfect class [38].

Theorem 3.5 ([23]) *Let Π be a SSS, with uniform distribution on its support. Let M be the matrix representation of Π with m rows. Then Π is IGC if and only if for every $i, j \in [m]$ there exists an automorphism $\sigma \in$* $\mathrm{Aut}(M)$ *such that $\sigma(i) = j$. Additionally, if Π is IGC, then m divides* $|\mathrm{Aut}(M)|$.

4 Ideal schemes which are not IGC

In this section, we show that there are ideal perfect SSSs which are not IGC. The motivation for studying this problem was discussed in the introduction.

We consider the $(2, 2)$-threshold access structure and use the connection between SSSs and Latin squares to show the existence of infinitely many non-IGC ideal SSSs for it. To warm up, we start by showing that a natural non-linear scheme for this access structure turns out to be IGC.

4.1 An unsuccessful attempt

Consider the $(2, 2)$-threshold access structure, defined on participants set $\{p_1, p_2\}$, whose only qualified subset is $\{p_1, p_2\}$. There is a simple linear scheme for this access structure. The secret and randomness spaces are both a finite field $\mathbb{F}$. To share a secret $s \in \mathbb{F}$, a randomness $r \in \mathbb{F}$ is chosen uniformly which will be the share of participant p_1. The share of p_2 is $s + r$.

One may consider the following more general variant of this scheme, with the hope to get a non-IGC scheme. The secret and randomness spaces are both a finite group $(H, *)$, which is not necessarily abelian. To share a secret $s \in H$, a randomness $r \in H$ is chosen uniformly which will be the share of participant p_1. The share of p_2 is $s * r$. Unfortunately, this scheme is IGC according to the following proposition, proved in Appendix B.

Proposition 4.1 *Let* $(H, *)$ *be a finite group and* $\mathbf{s}, \mathbf{r}$ *be independent and uniformly distributed RVs on* H*. Then, the joint distribution* $(\mathbf{s}, \mathbf{r}, \mathbf{s} * \mathbf{r})$ *is IGC.*

4.2 Schemes based on Latin squares

It was noticed by Seymour [36] that there exists a one-to-one correspondence between ideal SSSs for the $(2, 2)$-threshold access structure and Latin squares.

A Latin square of size n is an $n \times n$ matrix with elements in $\{1, \ldots, n\}$, in which none of the entries occur twice within any row or column.

A Latin square of size n can be used to construct a SSS for the $(2, 2)$-threshold access access structure. The secret space is the set $\{1, \ldots, n\}$. For sharing a secret s, chosen uniformly from the secret space, we select randomly an entry of the Latin square that is equal to s. Let i and j be the row and column indices of this entry, respectively. The index i (resp. j) is considered as the share of party p_1 (resp. p_2). Clearly, the parties together can reconstruct the secret using their shares, but they learn no information about the secret alone. Therefore, the scheme is perfect and ideal.

On the other hand, in a straightforward way, an ideal SSS for the $(2, 2)$-threshold access structures induces a Latin square. Hence, Latin squares and ideal SSSs for this access structure are equivalent.

The goal of the remaining two subsections is to show that there exist Latin squares which correspond to non-IGC SSSs.

4.3 Autotopism group of a Latin square

The *autotopism group* of a Latin square is a well-studied concept in Latin square literature (e.g., see [28]), which turns out to be closely related to automorphism group of its corresponding SSS. In this subsection, we explore this connection.

Isotope Latin squares. The autotopism group of a Latin square is defined via the following group action. Let $f = (f_0, f_1, f_2) \in \mathbb{S}_n^3$ be a triple of permutations on the set $[n]$ and $\mathcal{LS}$ be a Latin square of size n. We define the action $f \cdot \mathcal{LS}$ as follows:

- first, f_0 acts on the entries of $\mathcal{LS}$;
- then, f_1 permutes the rows of $\mathcal{LS}$;
- finally, f_2 permutes the columns of $\mathcal{LS}$.

Clearly, $f \cdot \mathcal{LS}$ remains a Latin square. We say that two Latin squares $\mathcal{LS}$ and $\mathcal{LS}'$ are *isotope* if there exists $f \in \mathbb{S}_n^3$ such that $f \cdot \mathcal{LS} = \mathcal{LS}'$. Now, we are ready to define the autotopism group of a Latin square.

Definition 4.2 (Autotopism group) *Let $\mathcal{LS}$ be a Latin square of size n. The following set is called the* autotopism group *of $\mathcal{LS}$:*

$$\mathrm{Atp}(\mathcal{LS}) := \{f \in \mathbb{S}_n^3 : \mathcal{LS} = f \cdot \mathcal{LS}\} \ .$$

The following easy-to-prove proposition relates group autotopism of a Latin square to the automorphism group of its corresponding SSS (recall Definition 3.4).

Proposition 4.3 (Relation between Atp and Aut) *Let M be the matrix representation of the SSS induced by a Latin square $\mathcal{LS}$. Then we have*

$$\mathrm{Atp}(\mathcal{LS}) = \{f_\sigma : \sigma \in \mathrm{Aut}(M)\} \ ,$$

where f_σ is the unique reordering that corresponds to the automorphism σ.

4.4 Counterexamples

We use the following theorem, proved by McKay and Wanless in [32], to show that there exists infinitely many ideal SSSs which are not IGC.

Theorem 4.4 (Informal [32]) *Almost all Latin squares have a trivial autotopism group.*

Let $\mathcal{LS}$ be a Latin square and M be the matrix representation of its corresponding SSS. If $\mathrm{Atp}(\mathcal{LS}) = \{e\}$, then by Proposition 4.3, the set $\{f_\sigma : \sigma \in \mathrm{Aut}(M)\}$ contains only the identity element (reordering). Since M has no repeated rows, if a permutation $\sigma \in \mathrm{Aut}(M)$ is non-trivial, then the reordering f_σ will be non-trivial. Therefore, $\mathrm{Atp}(\mathcal{LS}) = \{e\}$ implies that $\mathrm{Aut}(M) = \{e\}$. Hence, the matrix M is not IGC, because by Theorem 3.5, the row size of M must divide the size of the group $\mathrm{Aut}(M)$. Thus, we have the following corollary.

Corollary 4.5 *There are infinitely many ideal SSSs that are not IGC.*

Smallest concrete counterexample. Up to isotopy, the number of Latin squares of size $n = 1, 2, 3, 4, 5$ is equal to $1, 1, 1, 2, 2$, respectively. Clearly, inherent group-characterizability of schemes induced by Latin squares is invariant up to isotopy. It is possible to check that for $n \leqslant 4$, all schemes induced by non-isotope Latin squares of size n are IGC. Here is an example of a Latin square of size $n = 5$ which does not induce an IGC scheme.

$$\mathcal{LS} = \begin{array}{|c|c|c|c|c|}
\hline
1 & 2 & 3 & 5 & 4 \\
\hline
3 & 4 & 1 & 2 & 5 \\
\hline
2 & 1 & 5 & 4 & 3 \\
\hline
4 & 5 & 2 & 3 & 1 \\
\hline
5 & 3 & 4 & 1 & 2 \\
\hline
\end{array}$$

5 On weakly-ideal access structures

In this section, we first recall three well-known non-perfect security notions for SSSs. Then, we review four weak notions of ideality for access structures which have, explicitly or implicitly, appeared in the literature. In the last three subsections, we discuss the possibility of realization of weakly-ideal access structures by optimal schemes from three different classes of SSSs (multi-linear, GC and a subclass of GC schemes).

5.1 Non-perfect security notions and known results

In this subsection, we recall three well-known non-perfect security notions for SSSs. Statistical security is a standard relaxation of perfect security, probably first mentioned in [8]. Almost-perfect and quasi-perfect security notions have been introduced and studied in [15, 24, 25]. We refer to [22] for an extensive study of non-perfect security notions.

Family of schemes. Non-perfect security notions are defined with respect to a family $\{\Pi_k\}_{k\in\mathbb{N}}$ of SSSs, where k can be considered as a security parameter. We assume that the sequence of information ratios of the SSSs in our families is converging. We refer to the converged value as the *information ratio of the family.*

In the following, let Γ be an access structure on n participants and $\{\Pi_k\}_{k\in\mathbb{N}}$ be a family of SSSs, where $\Pi_k = (\mathbf{x}_0^k, \mathbf{x}_1^k, \dots, \mathbf{x}_n^k)$. We recall that a function $\varepsilon : \mathbb{N} \to \mathbb{R}$ is said to be negligible if $\varepsilon(k) = k^{-\omega(1)}$.

Statistical security. We say that $\{\Pi_k\}$ is a statistical family for Γ (or $\{\Pi_k\}$ statistically realizes Γ) if:

1. The secret length grows at most polynomially in k; that is, $\log_2 |\mathrm{supp}(\mathbf{x}_0^k)| = \mathrm{O}(k^c)$ for some $c > 0$.
2. For every qualified set $A \in \Gamma$, there exists a reconstruction function $\textsc{Recon}_A : \mathrm{supp}(\mathbf{x}_A^k) \to \mathrm{supp}(\mathbf{x}_0^k)$ such that for every secret s in the support of $\mathbf{x}_0^k$, the error probability $\Pr[\textsc{Recon}_A(\mathbf{x}_A^k) \neq s | \mathbf{x}_0^k = s]$ is negligible in k.
3. For every unqualified set $A \in \Gamma$ and every pair of secrets s, s' in the support of $\mathbf{x}_0^k$, the statistical distance $\frac{1}{2}\sum_x |\Pr[\mathbf{x}_A^k = x|\mathbf{x}_0^k = s] - \Pr[\mathbf{x}_A^k = x|\mathbf{x}_0^k = s']|$ is negligible in k.

Almost-perfect security. We say that $\{\Pi_k\}$ is an almost-perfect family for Γ (or $\{\Pi_k\}$ almost-perfectly realizes Γ) if:

1. $\lim\limits_{k\to\infty} \mathrm{H}(\mathbf{x}_0^k|\mathbf{x}_A^k) = 0$ for every qualified set $A \in \Gamma$, and
2. $\lim\limits_{k\to\infty} \mathrm{I}(\mathbf{x}_0^k : \mathbf{x}_B^k) = 0$ for every unqualified set $B \notin \Gamma$.

Quasi-perfect security. We say that $\{\Pi_k\}$ is a quasi-perfect family for Γ (or $\{\Pi_k\}$ quasi-perfectly realizes Γ) if:

- $\lim_{k\to\infty} \frac{\mathrm{H}(\mathbf{x}_0^k|\mathbf{x}_A^k)}{\mathrm{H}(\mathbf{x}_0^k)} = 0$ for every qualified set $A \in \Gamma$, and
- $\lim_{k\to\infty} \frac{\mathrm{I}(\mathbf{x}_0^k:\mathbf{x}_A^k)}{\mathrm{H}(\mathbf{x}_0^k)} = 0$ for every unqualified set $B \in \Gamma^c$.

Non-perfect information ratios. With respect to each security notion, a variant of information ratio for an access structure can be defined. For example, the *quasi-perfect information ratio* of an access structure is defined to be the infimum of the information ratios of all families of SSSs that quasi-perfectly realize it. Statistically-perfect and almost-perfect information ratios are defined similarly.

Known results about non-perfect SSSs. The following relation holds for the information ratios of an access structure with respect to the mentioned security notions and for every class of SSSs:

$$\begin{gathered}\text{quasi-perfect} \leqslant \text{almost-perfect} \leqslant \text{statistical} \leqslant \text{perfect} \\ \text{(for any class of schemes)}\ . \end{gathered} \tag{5.1}$$

For the GC SSSs whose secret subgroup (G_0) is normal in the main group (G), the following equivalence has been proved in [23]. That is, if $\{\Pi_k\}$ is an almost-perfect family for an access structure Γ, then for every sufficiently large k, Π_k is a perfect scheme for Γ. The equivalence for the multi-linear class has also been mentioned in [5].

$$\begin{gathered}\text{almost-perfect} \equiv \text{statistical} \equiv \text{perfect} \\ \text{(for GC schemes with normal secret subgroup)}\ . \end{gathered} \tag{5.2}$$

For multi-linear and general classes of SSSs, it has been proved in [22] that the following relations hold for the information ratios of an access structure with respect to different security notions:

$$\begin{gathered}\text{quasi-perfect} = \text{almost-perfect} = \text{statistical} \\ \text{(for general schemes),} \end{gathered} \tag{5.3}$$

$$\begin{gathered}\text{quasi-perfect} = \text{almost-perfect} = \text{statistical} = \text{perfect} \\ \text{(for multi-linear schemes).} \end{gathered} \tag{5.4}$$

An interesting property of quasi-perfect security is that GC SSSs are “complete” for computing the corresponding information ratio. It is an open problem if this is also true for other security notions. The following proposition has been implicitly mentioned in [25]. The proof follows from a well-known result by Chan and Yeung [14] stating that: for every scheme (random variable) $\Pi = (\mathbf{x}_i)_{i\in P\cup\{p_0\}}$, there exists a sequence $\{\Pi_k\}$ of GC schemes, with $\Pi_k = (\mathbf{x}_i^k)_{i\in P\cup\{p_0\}}$, such that for every $A \subseteq P \cup \{p_0\}$ it holds that $\lim_{k\to\infty} \frac{1}{k}\mathrm{H}(\mathbf{x}_A^k) = \mathrm{H}(\mathbf{x}_A)$.

Proposition 5.1 (Completeness of GC SSSs for quasi-perfect security) *The quasi-perfect information ratio of every access structure can be computed by restricting the computation to the class of GC schemes.*

5.2 Four variants of weakly-ideal access structures

Recall that an access structure is called ideal if it admits an ideal perfect SSS. One can consider weaker notions of ideality for access structures. In [6], an access structure has been called *nearly-ideal* if its (perfect) information ratio is one. Weaker variants can be defined with respect to the non-perfect security notions mentioned in the previous subsection. In [15], an access structure has been called *almost-ideal* if its almost-perfect information ratio is one. One can define *statistically-ideal* and *quasi-ideal* access structures similarly (we are not aware of any explicit mention of these notions in the literature).

The following relation holds between different notions of ideality:

$$\text{quasi-ideal} \Leftrightarrow \text{almost-ideal} \Leftrightarrow \text{statistically-ideal} \underset{\Rightarrow}{\overset{\Leftarrow}{?}} \text{nearly-ideal} \underset{\not\Rightarrow}{\overset{\Leftarrow}{}} \text{ideal} \tag{5.5}$$

The equivalence between quasi-ideal, almost-ideal and statistically-ideal access structures follows from relation (5.3). Notice that an ideal access structure is nearly-ideal too. However, the converse is not necessarily true. A notable counterexample, introduced by Beimel and Livne [6, page 2641], is a well-known 12-participant access structure, called $\mathcal{F} \wedge \overline{\mathcal{F}}$. It has both Fano an non-Fano access structures as minors. The (perfect) information ratio of this access structure is one but it does not admit an ideal perfect SSS.

It remains an open question whether statistically-ideal and nearly-ideal notions are equivalent. In [15], Csirmaz has presented an explicit almost-ideal (and hence statistically-ideal) access structure with 174 participants. Finding smaller such access structures is an interesting research problem that might lead to the resolution of this open question.

5.3 Impossibility of realization by multi-linear schemes

Recall that it is a long-standing open problem whether every ideal access structure admits an ideal multi-linear SSS [39]. It is then natural to ask a similar question about any of the four variants of weakly-ideal access structures.

Question 5.2 (Multi-linear/Weakly-ideal) *Is any variant of weakly-ideal access structures "optimally realizable" by multi-linear SSSs?*

Let us first present a formal definition of *optimal realizability* by a class of SSSs (e.g., multi-linear or GC).

Definition 5.3 (Optimal realizability) *Let $\mathcal{C}$ be a class of SSSs. We say that an <u>almost-ideal</u> access structure Γ is optimally realizable by class $\mathcal{C}$, if there exists a family of class-$\mathcal{C}$ SSSs that <u>almost-perfectly</u> realizes Γ and the sequence of their* *information ratios converges to one. A similar definition can be given for the case of nearly-ideal, statistically-ideal and quasi-ideal access structures, with respect to the perfect, statistically-perfect and quasi-prefect realizations, respectively.*

Claim 5.4 *The answer to Question 5.2 is negative for all four variants of weakly-ideal access structures.*

Proof. By relation (5.4), it is sufficient to prove the claim only for the case of nearly-ideal access structures. Recall that at the end of Section 5.2, we mentioned that Beimel and Livne have presented an example of a nearly-ideal access structure called $\mathcal{F} \wedge \overline{\mathcal{F}}$. Recently, Jafari and Khazaei [21] showed that the exact value of its information ratio is 4/3 for the class of multi-linear SSSs. Therefore, it is not optimally realizable by multi-linear schemes. This completes the proof of our claim. □

5.4 Possibility of realization by GC schemes

Recall that it also remains open if every ideal access structure admits an ideal GC SSS. Similar to Question 5.2, we can raise the following question.

Question 5.5 (GC/Weakly-ideal) *Is any variant of weakly-ideal access structures "optimally realizable" by GC SSSs?*

By Proposition 5.1, in the computation of information ratios of access structures with respect to quasi-perfect security, it is sufficient to restrict to the class of GC SSSs. Therefore, the answer to Question 5.6 is positive for quasi-ideal access structures. As we mentioned earlier, it is an open problem if GC SSSs are complete for perfect or any other non-perfect security notion. It also remains open if the the answer to Question 5.6 is positive for the other three variants of weakly-ideal access structures (which is a special case of the former open problem).

5.5 Possibility of realization by GC schemes with normal secret subgroup

Motivated by relation (5.2), one can raise the following question.

Question 5.6 (GC with normal secret group/Weakly-ideal) *Is any variant of weakly-ideal access structures "optimally realizable" by GC SSSs with normal secret subgroups?*

The problem remains open for all four variants. However, by (5.2) the answer for almost-ideal, statistically-ideal and nearly-ideal access structures are all the same.

6 Mejia and Montoya's characterization-like theorem for ideal access structures

In this section, we recall a result by Mejia and Montoya [33] for characterizing ideal access structures that admit ideal multi-linear schemes. It is an interesting research problem if their result can be extended to ideal access structures that admit ideal GC schemes. In this section, we present some notions which might be useful to explore this idea.

6.1 Matroids induced by ideal access structures

There are several equivalent definitons for matroids (e.g., see [34]). The following is suitable for the purpose of this paper.

Definition 6.1 *If Q is a finite set and $r : 2^Q \to \mathbb{Z}$ satisfies the following three conditions, then $M = (Q, r)$ is called a matroid on the ground set Q with rank function r:*

a) *If $A \subseteq Q$, then $0 \leqslant r(A) \leqslant |A|$.*
b) *If $A \subseteq B \subseteq Q$, then $r(A) \leqslant r(B)$.*
c) *If $A, B \subseteq Q$, then $r(A \cup B) + r(A \cap B) \leqslant r(A) + r(B)$.*

Independent sets and bases. For a matroid $M = (Q, r)$, a set $A \subseteq Q$ is called an independent set of M if $r(A) = |A|$. The maximal independent sets are called bases. It is easy to prove that all bases have the same cardinality.

Let Γ be an ideal access structure and $\mathbf{x} = (\mathbf{x}_i)_{i=0}^n$ be an ideal secret sharing scheme that realizes it. Define $Q = \{0, 1, \dots, n\}$ and the function $r : 2^Q \to \mathbb{R}$ as

$$r(A) = \mathrm{H}(\mathbf{x}_A)/\mathrm{H}(\mathbf{x}_0).$$

It can be shown [10] that the tuple (Q, r) is a matroid with rank function r and the ground set Q. This matroid is independent of the scheme and is uniquely determined by the access structure. We notate the matroid induced by an ideal access structure Γ by M_Γ.

We need the following definitions for this section.

Definition 6.2 (Matroid representation and entropic matroid) *Let Γ be an access structure and M_Γ be its induced matroid. Every ideal SSS for Γ is called a* representation *for M_Γ. Matroids that have such representations are called* entropic.

Definition 6.3 (Multi-linear/GC matroid) *We call a matroid multi-linear (resp. GC) if it is representable by an ideal multi-linear (resp. GC) SSS.*

Definition 6.4 (Multi-linear/GC ideal access structure) *We call an ideal access structure multi-linear (resp. GC) if it admits an ideal multi-linear (resp. GC) SSS.*

6.2 A characterization theorem for ideal multi-linear access structures

We recall that an access structure is called homogeneous if all its minimal qualified subsets have the same size. Related to a given matroid, Mejia and Montoya [33] define a homogeneous access structure as follows.

Definition 6.5 (Mejia-Montoya's access structure) *Let $M = (Q, r)$ be a matroid. Define the access structure* $\mathrm{Gen}(M)$ *as follows:*

$$\mathrm{Gen}(M) = \{A \subseteq Q : r(A) = r(Q)\}$$

Clearly, $\mathrm{Gen}(M) \subseteq 2^Q$ is an access structure on the participant set Q. Furthermore, the size of all its minimal qualified sets is $r(Q)$. Hence, $\mathrm{Gen}(M)$ is homogeneous.

Notice that by starting from an ideal access structure Γ on n participants, we end up with an access structure $\mathrm{Gen}(M_\Gamma)$ on $n+1$ participants. It is not directly clear if $\mathrm{Gen}(M_\Gamma)$ is ideal too. However, if Γ admits an ideal multi-linear scheme, the following theorem proved by Mejia and Montoya [33], shows that $\mathrm{Gen}(M_\Gamma)$ is also ideal and admits an ideal multi-linear scheme. The converse is also trivially true even when $\mathrm{Gen}(M_\Gamma)$ is only ideal (i.e., without requiring to be realizable by an ideal multi-linear scheme).

This theorem in some sense states that to characterize ideal multi-linear access structures, it is sufficient to characterize ideal multi-linear homogeneous ones. It remains open if a similar theorem holds for other classes of SSSs such as GC schemes. In later subsections, we provide some tools that might be useful to explore such extensions.

Theorem 6.6 (characterization theorem) *Let Γ be an access structure. Then Γ is ideal multi-linear if and only if* $\mathrm{Gen}(M_\Gamma)$ *is ideal multi-linear.*

6.3 Extended complementary information

Below, we introduce two notions called complementary information (CoI) and extended COI (ECoI). The former is defined for two jointly distributed RVs and the latter for a vector of jointly distributed RVs. In some sense, the CoI is similar to the common information property [16].

Definition 6.7 (CoI) *Let* $\mathbf{x}, \mathbf{y}$ *be two jointly distributed RVs such that* $\mathrm{H}(\mathbf{x}|\mathbf{y}) = 0$. *We say that* $(\mathbf{x}, \mathbf{y})$ *satisfies the complementary information property if there exists a RV* $\mathbf{z}$ *such that the following properties hold:*

1. $\mathrm{H}(\mathbf{z}|\mathbf{y}) = 0$
2. $\mathrm{I}(\mathbf{z} : \mathbf{x}) = 0$
3. $\mathrm{H}(\mathbf{y}) = \mathrm{H}(\mathbf{x}) + \mathrm{H}(\mathbf{z})$

Definition 6.8 (Extended CoI property) *Let $(\mathbf{y}, \mathbf{x}_1, \ldots, \mathbf{x}_n)$ be a vector of jointly distributed RVs such that*

$\mathrm{H}(\mathbf{x}_i|\mathbf{y}) = 0$ *and* $\mathrm{H}(\mathbf{x}_i) = \mathrm{H}(\mathbf{x}_j)$*, for all* $i, j \in [n]$*. We say that* $[\mathbf{y}; (\mathbf{x}_i)_{i\in[n]}]$ *satisfies the extended complementary information property (ECoI) if there exists a RV* $\mathbf{z}$ *such that the following conditions hold:*

1. $\mathrm{H}(\mathbf{z}|\mathbf{y}) = 0$,
2. $\mathrm{I}(\mathbf{z} : \mathbf{x}_1 \cdots \mathbf{x}_n) = 0$,
3. $\mathrm{H}(\mathbf{y}) = \mathrm{H}(\mathbf{z}) + \mathrm{H}(\mathbf{x}_i)$*, for all* $i \in [n]$.

It is easy to show that the multi-linear RVs satisfy the CoI property. Nevertheless, multi-linear RVs do not necessarily satisfy the CoI property. However, as we will see in the proof of Proposition 6.10, for a given multi-linear RV, it is possible to construct a "closely related" multi-linear RV that satisfies the ECoI property.

6.4 ECoI for matroids

In order to present the result of Mejia and Montoya in a way that one can think about its possible extensions (e.g., to GC schemes), we need to define the notion of ECoI for matroids as well.

Let $\mathbf{X} = (\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_n)$ be an ideal SSS for an access structure Γ. For a basis B of the induced matroid M_Γ and an element $b \in B$, notate $\mathbf{X}_{B,b} = (\mathbf{x}_i)_{i\in B\backslash b}$. Since the scheme is ideal, it then follows that $\mathrm{H}(\mathbf{X}_{B,b}) = (|B| - 1)\mathrm{H}(\mathbf{x}_0)$. The following definition is then meaningful, because all bases of a matroid have the same size.

Definition 6.9 *Let M be an entropic matroid and denote the set of its bases by $\mathcal{B}$. We say that M satisfies the ECoI property if there exists a representation* $\mathbf{X} = (\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_n)$ *for M such that* $[\mathbf{X}; (\mathbf{X}_{B,b})_{B\in\mathcal{B}, b\in B}]$ *satisfies the ECoI property.*

Proposition 6.10 *Any multi-linear matroid satisfies the ECoI property.*

Proof. Let M be a multi-linear matroid and $\mathbf{X} = (\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_n)$ be a representation for it, induced by a subspace collection $(T_0, T_1, \ldots, T_n)$ of a vector space T (see Definition 2.4–III). We show that $[\mathbf{X}; (\mathbf{X}_{B,b})_{B\in\mathcal{B}, b\in B}]$ satisfies the ECoI property. For any base B of M and $b \in B$ define $T_{B,b} = \sum_{i\in B\backslash b} T_i$.

It is possible to find a positive integer k such that the set $T^k \backslash \bigcup_{i=1}^n T_i^k$ has at least $k(\dim T - \dim T_1)$ linearly independent vectors. For this k, define the subspace W of T^k as the subspace generated by the obtained linearly independent vectors. Clearly, for all $i \in [n]$, it holds that $T^k = W \oplus T_i^k$. Let $\mathbf{X}' = (\mathbf{x}'_0, \mathbf{x}'_1, \ldots, \mathbf{x}'_n)$ be the multi-linear scheme induced by the vector space $\bigoplus_{i=1}^k T$ and its subspaces

$$(T'_0, T'_1, \ldots, T'_n) = (\bigoplus_{i=1}^k T_0, \bigoplus_{i=1}^k T_1, \ldots, \bigoplus_{i=1}^k T_n).$$

Clearly, $\mathbf{X}'$ is a multi-linear representation for the matroid M. Also, if $\mathbf{z}$ is the random variable induced by the subspace W, then according to the above discussion the tuple $[\mathbf{X}'; (\mathbf{X}'_{B,b})_{B\in\mathcal{B},b\in B}]$ satisfies the ECoI property with complementary information $\mathbf{z}$. Therefore, the matroid satisfies the ECoI property.

□

The following theorem is useful for thinking about generalization of Mejia and Montoya's result [33].

Theorem 6.11 *Let M be an entropic matroid which satisfies the ECoI property. Then the access structure* $\mathrm{Gen}(M)$ *is ideal.*

Proof. Let $\mathcal{B}$ be the set of bases for M. Since M satisfies the ECoI property, then there exists a representation $\mathbf{X} = (\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_n)$ for M such that $[\mathbf{X}; (\mathbf{X}_{B,b})_{B\in\mathcal{B},b\in B}]$ satisfy the ECoI property. Let $\mathbf{z}$ be the random variable that realizes it. Clearly, the tuple $\Pi = (\mathbf{z}, \mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_n)$ is an ideal secret sharing scheme for $\mathrm{Gen}(M)$ in which $\mathbf{z}$ is the secret RV and $\mathbf{x}_i$ is the i'th participant's share RV. □

Corollary 6.12 ([33]) *If M is a multi-linear matroid, then* $\mathrm{Gen}(M)$ *is an ideal multi-linear access structure.*

Corollary 6.13 *If Γ is an ideal multi-linear access structure, then* $\mathrm{Gen}(M_\Gamma)$ *is an ideal multi-linear access structure too.*

Since GC matroids are a natural generalization of the multi-linear ones, we may wonder if these matroid satisfy the ECoI property too. If so, one can then apply the above theorem to extend Mejia and Montoya's characterization theorem (Theorem 6.11).

Question 6.14 *Is it true that any GC matroid satisfies the ECoI property.*

We remark that unlike multi-linear random variables, the GC random variables do not necessarily satisfy the CoI property (Definition 6.7). The reason is that the notion of *complemented group* only exists for supersolvable groups with elementary abelian Sylow subgroups [19, Theorems 1& 2]. Nevertheless, this does not directly show that the answer to the above question is negative. For example if Statement 1.1 turns out to be true (i.e., every ideal access structure admits an ideal perfect multi-linear SSS), the answer to the above question is positive too.

7 Conclusion

It is a long standing open problem in secret sharing and matroid theory to prove or refute if every ideal access structure is realizable by an ideal multi-linear SSS.

In this paper, we first proposed to study a weaker statement asking if every ideal access structure is realizable by an ideal group-characterizable (GC) SSS. As a first step towards attacking this problem, we studied the easier problem if every ideal perfect SSS is GC, up to relabeling the secret and shares. Even though the answer turned out to be negative, the proof was not as trivial as it might look at a first glance.

Then, we studied four variants of weakly-ideal access structures; that is, nearly-ideal, statistically-ideal, almost-ideal and quasi-ideal. We then raised the same questions again; that is, whether every variant of weakly-ideal access structures is optimally realizable by a family of multi-linear or GC secret sharing schemes with information ratio one. For the class of multi-linear SSSs, the answer turned out to be negative for all variants. However, for the class of GC schemes, the answer was shown to be positive for the case of quasi-ideal access structures. The remaining cases were left open. Table 1 shows a summary of known results and open problems. The table also includes the possibility of optimal realization by GC SSSs with normal secret subgroups which was shortly discussed in the paper.

In the paper, we also explored a classification-like theorem by Mejia and Montoya for ideal access structures that admit ideal multi-linear schemes and suggested some tools for exploring its possible extensions for GC schemes.

		weakly-ideal			
	ideal	nearly-ideal	stat.-ideal	almost-ideal	quasi-ideal
multi-linear	?	✗	✗	✗	✗
GC with normal secret subgroup	?	?			?
GC	?	?	?	?	✓

Table 1: Optimal realizability of different types of ideal access structures by multi-linear and GC schemes

We hope that this paper incites motivation for researchers with interests in group-theory, combinatorics and matroid theory to study the GC random variables, introduced by Chan and Yeung in the context of information theory further. We believe that this may lead to the resolution of some long-standing open problems in the theory of secret sharing and matroid theory.

References

1. Michael Bamiloshin, Aner Ben-Efraim, Oriol Farràs, and Carles Padró. Common information, matroid representation, and secret sharing for matroid ports. *CoRR*, abs/2002.08108, 2020.
2. Amos Beimel. Secret-sharing schemes: a survey. In *International Conference on Coding and Cryptology*, pages 11–46. Springer, 2011.
3. Amos Beimel, Aner Ben-Efraim, Carles Padró, and Ilya Tyomkin. Multi-linear secret-sharing schemes. In *Theory of Cryptography Conference*, pages 394–418. Springer, 2014.
4. Amos Beimel and Benny Chor. Universally ideal secret-sharing schemes. *IEEE Transactions on Information Theory*, 40(3):786–794, 1994.

5. 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.
6. Amos Beimel and Noam Livne. On matroids and nonideal secret sharing. *IEEE Trans. Information Theory*, 54(6):2626–2643, 2008.
7. Amos Beimel and Noam Livne. On matroids and nonideal secret sharing. *IEEE Transactions on Information Theory*, 54(6):2626–2643, 2008.
8. Michael Bertilsson and Ingemar Ingemarsson. A construction of practical secret sharing schemes using linear block codes. In *Advances in Cryptology - AUSCRYPT '92, Workshop on the Theory and Application of Cryptographic Techniques, Gold Coast, Queensland, Australia, December 13-16, 1992, Proceedings*, pages 67–79, 1992.
9. George Robert Blakley. Safeguarding cryptographic keys. *Proc. of the National Computer Conference1979*, 48:313–317, 1979.
10. Ernest F. Brickell and Daniel M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology*, 4(2):123–134, 1991.
11. Ho-Leung Chan and Raymond W Yeung. A combinatorial approach to information inequalities. In *1999 Information Theory and Networking Workshop (Cat. No. 99EX371)*, page 63. IEEE, 1999.
12. Terence Chan and Alex J. Grant. Dualities between entropy functions and network codes. *IEEE Trans. Information Theory*, 54(10):4470–4487, 2008.
13. Terence H Chan, Alex Grant, and Thomas Britz. Properties of quasi-uniform codes. In *2010 IEEE International Symposium on Information Theory*, pages 1153–1157. IEEE, 2010.
14. 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.
15. László Csirmaz. Secret sharing and duality. *CoRR*, abs/1909.13663, 2019.
16. Peter Gács and János Körner. Common information is far less than mutual information. *Problems of Control and Information Theory*, 2(2):149–162, 1973.
17. Joseph Gallian. *Contemporary abstract algebra*. Nelson Education, 2012.
18. Laurent Guille, Terence Chan, and Alex J. Grant. The minimal set of ingleton inequalities. *IEEE Trans. Information Theory*, 57(4):1849–1864, 2011.
19. Philip Hall. Complemented groups. *Journal of the London Mathematical Society*, 1(3):201–204, 1937.
20. 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.
21. Amir Jafari and Shahram Khazaei. On abelian and homomorphic secret sharing schemes. Cryptology ePrint Archive, Report 2019/575, 2019. https://eprint.iacr.org/2019/575.
22. Amir Jafari and Shahram Khazaei. Partial secret sharing schemes. Cryptology ePrint Archive, Report 2020/448, 2020. https://eprint.iacr.org/2020/448.
23. Reza Kaboli, Shahram Khazaei, and Maghsoud Parviz. On group-characterizability of homomorphic secret sharing schemes. Cryptology ePrint Archive, Report 2019/576, 2019. https://eprint.iacr.org/2019/576.
24. Tarik Kaced. Almost-perfect secret sharing. In *2011 IEEE International Symposium on Information Theory Proceedings, ISIT 2011, St. Petersburg, Russia, July 31 - August 5, 2011*, pages 1603–1607, 2011.

25. Tarik Kaced. *Secret Sharing and Algorithmic Information Theory. (Partage de secret et the'orie algorithmique de l'information).* PhD thesis, Montpellier 2 University, France, 2012.
26. 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.
27. Ehud Karnin, Jonathan Greene, and Martin Hellman. On secret sharing systems. *IEEE Transactions on Information Theory*, 29(1):35–41, 1983.
28. A Donald Keedwell and József Dénes. *Latin squares and their applications.* Elsevier, 2015.
29. František Matúš. Algebraic matroids are almost entropic. *To appear in Proceedings of the AMS.*
30. František Matúš. Matroid representations by partitions. *Discrete Mathematics*, 203(1):169–194, 1999.
31. Frantisek Matús. Classes of matroids closed under minors and principal extensions. *Combinatorica*, 38(4):935–954, 2018.
32. Brendan D McKay and Ian M Wanless. On the number of latin squares. *Annals of combinatorics*, 9(3):335–344, 2005.
33. Carolina Mejia and J Andrés Montoya. On the information rates of homomorphic secret sharing schemes. *Journal of Information and Optimization Sciences*, 39(7):1463–1482, 2018.
34. James G Oxley. *Matroid theory*, volume 3. Oxford University Press, USA, 2006.
35. Carles Padró. Lecture notes in secret sharing. *IACR Cryptology ePrint Archive*, 2012:674, 2012.
36. Paul D. Seymour. On secret-sharing matroids. *J. Comb. Theory, Ser. B*, 56(1):69–73, 1992.
37. Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.
38. Juriaan Simonis and Alexei Ashikhmin. Almost affine codes. *Designs, Codes and Cryptography*, 14(2):179–197, 1998.
39. Juriaan Simonis and Alexei E. Ashikhmin. Almost affine codes. *Des. Codes Cryptogr.*, 14(2):179–197, 1998.
40. Fei Wei, Michael Langberg, and Michelle Effros. Towards an operational definition of group network codes. *CoRR*, abs/2002.00781, 2020.
41. Zhen Zhang and Raymond W. Yeung. On characterization of entropy function via information inequalities. *IEEE Trans. Information Theory*, 44(4):1440–1452, 1998.

A Basics of abstract algebra

For the 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 abstract algebra, e.g., [17].

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's 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.

B Proof of Proposition 4.1

One can use Theorem 3.5 to show that the scheme $(\mathbf{s}, \mathbf{r}, \mathbf{s} * \mathbf{r})$ is IGC. Here, we directly present a group characterization $[G : G_0, G_1, G_2]$ for it. Denote the trivial subgroup of H by 1 and let $(H^\circ, \cdot)$ be the opposite group of H, where it has the same elements and the product of $r, s \in H^\circ$ is defined to be $r \cdot s := s * r$. Let

$$\begin{aligned} G \ &= H \times H^\circ \ , \\ G_0 &= 1 \times H^\circ \ , \\ G_1 &= H \times 1 \ , \\ G_2 &= \{(x, x^{-1}) \mid x \in H\} \ . \end{aligned}$$

It is easy to check that the G_i's are subgroups of G. We show this only for G_2. Since G_2 is trivially closed under inversion, it is enough to show that it is closed under multiplication. Let $(x, x^{-1}), (y, y^{-1})$ be two elements of G_2 and notice that their product also belongs to G_2, since we have

$$(x, x^{-1}) \cdot (y, y^{-1}) = (x * y, x^{-1} \cdot y^{-1}) = (x * y, y^{-1} * x^{-1}) = (x * y, (x * y)^{-1}) \ .$$

Consider the GC scheme induced by $[G : G_0, G_1, G_2]$ and the relabeling (f_0, f_1, f_2) given by the isomorphisms $f_i : G/G_i \to H$, $i = 0, 1, 2$, defined as below:

$$\begin{cases} (s, r)G_0 \mapsto s & \text{if } \ i = 0 \\ (s, r)G_0 \mapsto r & \text{if } \ i = 1 \\ (s, r)G_0 \mapsto s * r & \text{if } \ i = 2 \end{cases}$$

The first two are trivially well-defined. To check that the last one is well-defined too, notice that $(s, r) \in G_2$ if and only if $s * r = 1$. It then follows that $[G : G_0, G_1, G_2]$ is a group characterization for the random variable $(\mathbf{s}, \mathbf{r}, \mathbf{s} * \mathbf{r})$.