On Group-Characterizability of Homomorphic Secret Sharing Schemes

Reza Kaboli, Shahram Khazaei, Maghsoud Parviz

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

Abstract. A group-characterizable (GC) random variable is induced by a finite group, called main group, and a collection of its subgroups [Chan and Yeung 2002]. The notion extends directly to secret sharing schemes (SSS). It is known that multi-linear SSSs can be equivalently described in terms of GC ones. The proof extends to abelian SSSs, a more powerful generalization of multi-linear schemes, in a straightforward way. Both proofs are fairly easy considering the notion of dual for vector spaces and Pontryagin dual for abelian groups. However, group-characterizability of homomorphic SSSs (HSSSs), which are generalizations of abelian schemes, is non-trivial, and thus the main focus of this paper.

We present a *necessary and sufficient* condition for a SSS to be equivalent to a GC one. Then, we use this result to show that HSSSs satisfy the sufficient condition, and consequently they are GC. Then, we strengthen this result by showing that a group-characterization can be found in which the subgroups are all normal in the main group. On the other hand, GC SSSs whose subgroups are normal in the main group can easily be shown to be homomorphic. Therefore, we essentially provide an *equivalent characterization of HSSSs* in terms of GC schemes.

We also present two *applications* of our equivalent definition for HSSSs. One concerns lower bounding the information ratio of access structures for the class of HSSSs, and the other is about the coincidence between statistical, almost-perfect and perfect security notions for the same class.

Key words: homomorphic secret sharing, access structure, information theory, group theory, group-characterizable random variable

1 Introduction

A *secret sharing scheme (SSS)* [9,26,36] allows a dealer to share a secret among a set of participants. The dealer applies a publicly-known probabilistic method to compute a share for each participant, which is then privately transferred to him/her. In a *perfect* SSS, it is required that only certain pre-specified subsets of participants, called *qualified*, be able to recover the secret, and others must gain no information about the secret. The collection of all qualified subsets is called an *access structure*.

The efficiency of a SSS is quantified using a parameter called *information ratio*, defined to be the ratio between the largest share size and the secret size. The information ratio of an access structure is defined as the infimum of the information ratios of all SSSs for it.

The most common type of SSSs is the class of *multi-linear* schemes, which we simply call *linear* in this paper. 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. A more powerful generalization of linear schemes, called *abelian*, has recently been studied in the literature [20, 29].

The notion of *homomorphic* SSS (HSSS), introduced by Benaloh [7] in 1986, plays a central role in several applications of secret sharing in cryptography (e.g., secure multi-party computation [6]). A SSS is called homomorphic if multiplication of the corresponding shares of two secrets results in valid shares for the product of the secrets. Every abelian (and consequently linear) scheme is homomorphic, but it is an open problem if homomorphic SSSs are stronger than the abelian schemes. This paper has been mainly motivated by our narrow knowledge and lack of understanding surrounding HSSSs, as it will be discussed next.

1.1 Known results about HSSSs

Very little is known about HSSSs. In 1992, Frankel, Desmedt and Burmester [22] proved that in perfect HSSSs, the secret space is an abelian group. In a subsequent work, Frankel and Desmedt [21] showed that when the scheme is *ideal* (i.e., all share sizes are the same as the secret size), the share spaces are all isomorphic to the secret space, and hence abelian too. Despite several subsequent attempts [14,17,35,38], characterization of ideal perfect HSSSs remained an open problem for a long time. Recently, Jafari and Khazaei [29] have shown that any ideal HSSS can be converted into an ideal 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. However, for general access structures, Jafari and Khazaei [29] also showed that HSSSs outperform linear ones [29] (in terms of the best achievable information ratio). In particular, it was shown in [29] that a subclass of abelian schemes, called *mixed-linear*, which are constructed by combing linear schemes with possibly different underlying finite fields, outperform linear ones. It remains an open question whether HSSSs can outperform abelian or even mixed-linear schemes.

1.2 An equivalent definition for HSSSs

As it was mentioned above, classification of HSSSs has remained a long-standing open problem. In this paper, we present an equivalent definition in terms of *group-characterizable* (GC) SSSs along with two applications.

GC SSSs can be defined in terms of the so-called *group-characterizable random variables* (GCRVs), defined by Chan and Yeung in 2002 [13]. We remark that RVs and SSSs are essentially equivalent notions (e.g., see [1]). Here we

present a definition of GC SSS based on the description that was given at the beginning of the introduction (i.e., as a probabilistic sharing method). In the following, we use some basic concepts of abstract algebra, which are recalled in Appendix A.

GC secret sharing. A *GC SSS* is defined by a finite group $(G, *)$, called the *main group*, along with a collection $G_0, G_1, \ldots, G_n$ of its subgroups, as follows. 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 $(s_1, \ldots, s_n) = (gG_1, \ldots, gG_n)$; i.e., the i'th participant's share is the coset $s_i = gG_i$.

Main result. As we mentioned earlier, the class of HSSSs includes the linear and abelian schemes, which are both GC (we will return to this fact at the end of this subsection). On the other hand, a GC SSS induced by a main group G and *normal* subgroups $G_0, \ldots, G_n$ in G can easily be shown to be homomorphic. It is not directly obvious whether HSSSs are GC, and if so, it is not clear if there are HSSSs that do not have a group characterization with normal subgroups. The main result of this paper is to show that the two classes are equal; that is, *every HSSS is GC with normal subgroups in the main group.*

Our approach. We call two vectors of jointly distributed RVs *equivalent* if they differ up to relabeling of the elements of the supports of their marginal distributions. We refer to RVs which are equivalent to some GCRV as *inherently GC*. One of the main contributions of this paper is a *key theorem* which essentially provides a *necessary and sufficient condition* for a RV to be inherently GC.

We take the following steps to prove our key theorem. We represent a vector of jointly distributed RVs by a *matrix*. Its rows are the elements of the support of the RV (a distribution on the rows is sufficient to fully describe the RV). We then associate a group to a matrix, called the *automorphism group* of that matrix. It is defined to be the set of all permutations on the rows of the matrix which result in the same matrix, up to relabeling of the entries of each column. Our key theorem is then stated as follows (the notions of *group action* and *transitivity* of a group action are standard definitions in abstract algebra and will be recalled in Appendix B).

Key Theorem: *A vector of jointly distributed RVs is inherently GC if and only if the automorphism group of its matrix representation acts transitively on the set of its rows.*

As an application of the sufficiency condition of the key theorem, we then show that HSSSs satisfy the mentioned condition. If a RV is inherently GC, the proof of our key theorem also *constructively* provides a group-characterization for it (which might be different from the original one). Some extra effort is required to show that HSSSs are IGC with normal subgroups (see Section 4.2 for further details).

Technicality comparison with linear and abelian RVs. As we mentioned earlier, linear and abelian SSSs (or equivalently RVs) are GC too. The group-characterizability of linear RVs was shown by Chan in [12], based on an equivalent definition of linear RVs by Hammer et. al. [25] (Definition 2.1–ii.). In fact, it can be shown that linear RVs are equivalent to GCRVs whose main groups are vector spaces. The proof is fairly easy considering the notion of duality for vector spaces. The abelian RVs were defined by Jafari and Khazaei [29] as a generalization of Hammer et. al.'s definition of linear RVs (Definition 2.2–ii.). The generalization relies on the notion of Pontryagin dual for abelian groups. We will show that abelian RVs are equivalent to GCRVs whose main groups are abelian. The proof uses the properties of Pontryagin duality and is very similar to the linear case, without any particular complexity. The complexity for the homomorphic case is essentially due to lack of proper notions of duality for general (i.e., non-abelian) groups.

1.3 Applications of our equivalent definition

Unlike linear SSSs, which have been very well studied in the literature, our understanding of HSSSs is very limited, as we discussed earlier. Here, we mention some further motivations for studying HSSSs, which turn out easy to answer thanks to our equivalent definition for HSSSs in terms of GC ones.

- **Lower-bounds.** A notable approach for finding a lower bound on the information ratio of access structures is to use the so-called Shannon-type or non-Shanon-type information inequalities (e.g., see [4, 10, 15]). Recently, Farràs et al. [20] have proposed an improved method using the *common information* property of random variables. In [20], it was mentioned that the obtained lower bound applies not only to linear SSSs but also to abelian ones because both classes are known to satisfy the common information property. It is a natural question to ask if their method also applies to any larger class. We will show that the common information property is satisfied for a subclass of GC SSSs whose subgroups have some specific property, which we show to be satisfied by normal subgroups. Consequently, the obtained lower bound using the common information method also applies to HSSSs (and even a larger class).
- **Non-perfect SSS.** The most common security notion for SSSs is perfect security. The following relaxations, in increasing level of security, have been presented in the literature: partial [30], quasi-perfect [32, Chapter 5], almost-perfect [16,33] and statistical (a well-known and standard relaxation, probably first mentioned in [8]). Recently, these security notions were extensively studied in [30] and two main results were presented. First, the information ratio of an access structure with respect to all non-perfect security notions coincides with perfect security 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 remained open whether it also coincides with perfect security.

For the class of linear SSSs, it is easy to argue that almost-perfect (and consequently statistical) security coincides with perfect security. This observation has already been made for statistical security by Beimel and Ishai [3, right after Definition 2.3]. We will show that the notion of almost-perfect (and consequently statistical) security also coincides with perfect security for a subclass of GC SSSs whose secret subgroups are normal in their main groups, which clearly includes homomorphic ones.

1.4 Paper organization

The paper is organized as follows. The required concepts about RVs and SSSs are presented in Section 2. In Section 3, we introduce the notion of inherent group-characterizability of RVs. In Section 4, our key theorem (i.e., the necessary and sufficient condition for inherent group-characterizability of RVs) is presented and proved; some applications of the necessary condition are also discussed. Our equivalent definition for HSSSs in terms of GC SSSs is introduced in Section 5. Applications of our equivalent definition is given in Section 6. The paper is concluded in Section 7.

2 Random variables and secret sharing

In this section, we introduce our notation and some basic concepts. For the reader's convenience we review the basic definitions of abstract algebra in Appendix A. We refer to [1] for a survey on the theory of secret sharing.

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

2.1 Linear, abelian and group-characterizable RVs

The notion of linear RVs is widely used in the literature and several equivalent definitions exist for them. Here, we present three such definitions. The equivalence of these definitions is well-known, but for completeness, we present a proof in Appendix C.

Definition 2.1 (Linear RV) *Let $\mathbb{F}$ be a finite field. A linear RV can be defined in any of the following equivalent ways.*

i. **(Linear maps)** *For every $i \in [n]$, let $\mu_i : S \to S_i$ be a linear map, where S and S_i's are all finite-dimensional $\mathbb{F}$-vector spaces. We refer to the joint RV $(\mu_1(\mathbf{s}), \ldots, \mu_n(\mathbf{s}))$ as a linear RV, where $\mathbf{s}$ is a uniform RV on S.*

ii. **(Dual space [25])** *Let T be a finite-dimensional $\mathbb{F}$-vector space and $T_1, \ldots, T_n$ be a collection of subspaces of T. Let $\boldsymbol{\alpha}$ be a uniform RV on*

$$T^* = \{\alpha \mid \alpha : T \to \mathbb{F} \text{ is a linear functional}\},$$

i.e., the dual space of T. We refer to $(\boldsymbol{\alpha}|_{T_1}, \ldots, \boldsymbol{\alpha}|_{T_n})$ as a linear RV. Here, $\boldsymbol{\alpha}|_{T_i}$ is the same mapping as α but its domain has been restricted to T_i.

iii. **(Affine subspaces)** *Let U be a finite-dimensional $\mathbb{F}$-vector space, $U_1, \ldots, U_n$ be a collection of subspaces of U and $\mathbf{u}$ be a uniform RV on U. We refer to $(\mathbf{u} + U_1, \ldots, \mathbf{u} + U_n)$ as a linear RV. Here, the support of RV $\mathbf{u} + U_i$ is the set of all affine subspaces parallel to U_i (i.e., $\{u + U_i \mid u \in U\}$ where $u + U_i$ is the translation of U by the vector u).*

The first definition is usually used in the secret sharing literature for defining linear SSSs (similar to the definition given in the third paragraph of the introduction). The second definition was introduced by Hammer et. al. [25] and has been widely used in the information theory literature, specifically in the search for the so-called *linear rank inequalities* (e.g., see [18]). Interestingly, this definition is closely related to definition of SSSs in terms of the so-called *(multi-target) monotone span programs* [2,34]. We refer to [30, Section 2.5] for an explanation of this connection. Also, this definition has been a source of motivation in [29] for defining abelian RVs. As we will see, the third definition is useful to view the linear RVs as a subclass of group-characterizable RVs, introduced by Chan and Yeung in [13].

Abelian RVs in the context of secret sharing has recently emerged in [20, 29]. Similar to the linear case, here we provide three definitions. The proof of equivalence is very similar to that of the linear case (see Appendix C).

Definition 2.2 (Abelian RVs) *Abelian RVs can be defined in the following equivalent ways.*

i. **(Abelian homomorphisms)** *For every $i \in [n]$, let $\mu_i : S \to S_i$ be a group homomorphism, where S and S_i's are all finite abelian groups. We refer to the joint RV $(\mu_1(\mathbf{s}), \ldots, \mu_n(\mathbf{s}))$ as an abelian RV, where $\mathbf{s}$ is a uniform RV on S.*

ii. **(Pontryagin dual [29])** *Let $(H, +)$ be a finite abelian group and $H_1 \ldots, H_n$ be a collection of its subgroups. Let $\boldsymbol{\alpha}$ be a uniform RV on*

$$\widehat{H} = \{\alpha \mid \alpha : H \to \mathbb{C}^* \text{ is a homomorphism}\},$$

called the Pontryagin dual of H, where $\mathbb{C}^*$ is the multiplicative group of non-zero complex numbers. We refer to $(\boldsymbol{\alpha}|_{H_1}, \ldots, \boldsymbol{\alpha}|_{H_n})$ as an abelian RV. Again, $\boldsymbol{\alpha}|_{H_i}$ is the same mapping as α, but with domain restricted to H_i.

iii. **(Cosets)** *Let $(G, +)$ be a finite abelian group and $G_1 \ldots, G_n$ be a collection of its subgroups. We refer to the RV $(\mathbf{g} + G_1, \ldots, \mathbf{g} + G_n)$ as an abelian RV, where $\mathbf{g}$ is a uniform RV on G. Here, the support of RV $\mathbf{g} + G_i$ is the set of all cosets of G_i in G (i.e., $\{g + G_i \mid g \in G\}$, where $g + G_i = \{g + h \mid h \in G_i\}$).*

Group-characterizable random variables (GCRVs) can be considered a generalization of the third definition for both linear and abelian RVs.

Definition 2.3 (Group-characterizable RV [13]) *Let $(G, *)$ be a finite group, $G_1 \ldots, G_n$ be a collection of its subgroups and $\mathbf{g}$ be a uniform RV on G. We refer to the RV $\mathbf{x} = (\mathbf{g}G_1, \ldots, \mathbf{g}G_n)$ as a* group-characterizable random variable *(GCRV), induced by $\pi = [G : G_1, \cdots, G_n]$. Here, $\mathbf{g}G_i$ is a RV whose support is the left cosets of G_i in G. We call G the* main group *and say that π is a* group-characterization *for $\mathbf{x}$.*

Let $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_n)$ be a GCRV induced by $[G : G_1, \cdots, G_n]$ and fix a subset $A \subseteq [n]$. The support of the RV $\mathbf{x}_A = (\mathbf{x}_i)_{i \in A}$ is $\left\{ (gG_i)_{i \in A} : \ g \in G \right\}$, which is a subset of the Cartesian product $\prod_{i \in A} \left(G/G_i \right)$. Equivalently, it can be viewed as the induced random variable $f(\mathbf{g})$, where $f : G \to \prod_{i \in A} (G/G_i)$ is defined by $g \mapsto (gG_i)_{i \in A}$. Let $G_A = \bigcap_{i \in A} G_i$. Since $(gG_i)_{i \in A} = (hG_i)_{i \in A}$ if and only if $g^{-1}h \in G_A$, it follows that $|\mathrm{supp}(\mathbf{x}_A)| = |G/G_A|$.

2.2 Secret sharing schemes

A secret sharing scheme (SSS) is a method by which a distinguished participant, called the *dealer*, shares a secret among a set of n participants. Given a secret x_0, the dealer first samples a randomness r according to some pre-specified distribution. He then employs a fixed and publicly-known mapping μ that takes the secret and randomness and computes the shares as $(x_1, \ldots, x_n) = \mu(x_0, r)$, where x_i is the share of ith participant. This definition does not assume a priori a distribution on the secret space. By considering a probability distribution on the secret space, a SSS can equivalently be defined as follows.

Definition 2.4 (Secret sharing scheme) *A secret sharing scheme (SSS) on participants set $[n]$ is a joint distribution $\mathbf{x} = (\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_n)$, 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 $i \in [n]$.*

Given a SSS $\mathbf{x} = (\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_n)$, the dealer can share a secret $x_0 \in \mathrm{supp}(\mathbf{x}_0)$ as follows. He samples a tuple $(x_0, x_1, \ldots, x_n)$ according to the distribution $\mathbf{x}$, conditioned on the event $[\mathbf{x}_0 = x_0]$. The shares are then determined by the sampled tuple.

A SSS by itself does not convey any notion of security. The most well-known security notion is that of *perfect* security, in which the goal of the dealer is to allow some pre-specified subsets of participants to recover the secret. The secret must remain information-theoretically hidden from all other subsets of participants. To formalize this intuition we present the notion of *access structure* first.

Definition 2.5 (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 2.6 (Perfect realization) *We say that a secret sharing scheme* $(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_n)$ *is a perfect scheme for an access structure* Γ *if the following two conditions hold:*

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

where $\mathbf{x}_A = (\mathbf{x}_i)_{i\in A}$ *for every* $A \subseteq [n]$*.*

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 $\mathbf{x} = (\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_n)$ is defined to be $\mathrm{H}(\mathbf{x}_i)/\mathrm{H}(\mathbf{x}_0)$. The information ratio of a SSS is the maximum (or sometimes the average) of all participants' information ratios. The information ratio of an access structure is defined as the infimum of the information ratios of all SSSs that perfectly realize it. Computing the information ratio of access structures is a challenging problem.

Linear, abelian and GC SSSs. Every class of RVs gives rise to a class of secret sharing schemes. A SSS $\mathbf{x} = (\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_n)$ on n participants is called GC (resp. linear or abelian) if the RV $\mathbf{x}$ is GC (resp. linear or abelian).

3 Inherently group-characterizable random variables

In this section, we introduce the notion of *inherently* group-characterizable (IGC) RVs. We use *matrix representation* of RVs and introduce the concept of *relabeling* for defining inherent group-characterizability of RVs.

Matrix representation of RVs. A RV with finite support can be represented by a matrix by considering the elements in the support of the RV as the rows of the matrix. We are not concerned about the order of rows. A non-zero probability must also be assigned to each row, based on the distribution of the RV. We usually ignore the distribution on the rows and focus on the matrix itself.

Example 3.1 *Consider a GCRV induced by* $[G : G_1, \cdots, G_n]$*. Clearly, its matrix representation is of the form*

$$\begin{bmatrix} g_1G_1 & g_1G_2 & \cdots & g_1G_n \\ g_2G_1 & g_2G_2 & \cdots & g_2G_n \\ \vdots & \vdots & & \vdots \\ g_mG_1 & g_mG_2 & \cdots & g_mG_n \end{bmatrix},$$

where all the rows are distinct and $\{g_1, g_2, \ldots, g_m\}$ *is some (possibly proper) subset of* G*, where* $m = |G|/|\bigcap_{i=1}^n G_i|$*. Because, as we mentioned earlier, a tuple* $(gG_1, \ldots, gG_n)$ *is equal to* $(hG_1, \ldots, hG_n)$ *if and only if* $g^{-1}h \in \bigcap_{i=1}^n G_i$*.*

From a secret sharing point of view, we do not distinguish between two jointly distributed RVs whose all marginal distributions are identical up to a relabeling of the elements of their supports. To capture this notion, we propose the following definition.

Definition 3.2 (Relabeling) *Let $M = [m_{ij}]_{m\times n}$ be a matrix and denote its j'th column by M^j. A* relabeling *for M is a tuple $f = \left(f^1, f^2, \ldots, f^n\right)$ such that f^j, $j \in [n]$, is an injection from the set of distinct elements in M^j, to an arbitrary set. The action $f \cdot M$ is defined by*

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

where f^j acts on the j'th column as $f^j \cdot M^j = [f^j(m_{ij})]_{m\times 1}$.

Example 3.3 *The following matrices are relabelings of each other:*

$$M = \begin{bmatrix} a & b & a \\ a & a & b \\ b & b & b \\ b & a & a \end{bmatrix} \quad , \quad M' = \begin{bmatrix} \# & \% & \$ \\ \# & * & \& \\ * & \% & \& \\ * & * & \$ \end{bmatrix} .$$

In order to work with RVs or SSSs that are essentially GC but do not have a built-in group-characterization, we present the following definition.

Definition 3.4 (Inherent group-characterizability) *A matrix M is called* inherently group-characterizable (IGC) *if there exists a relabeling f such that $f \cdot M$ is the matrix representation of a GCRV.*

The above definition was given for matrices, but it clearly can be extended to RVs and SSSs, which are *uniformly distributed on their supports*. Therefore, we can refer to RVs or SSSs as being IGC.

Remark 3.5 (On uniformity) *We would like to highlight the following points concerning the "uniform distribution assumption" that we need on the support of RVs and SSSs to call them IGC.*

- *RVs which are not uniformly distributed on their supports cannot be GC. One can extend the notion of GCRVs by allowing the RV $\mathbf{g}$ in Definition 2.3 to have an arbitrary distribution on G but with full support. Equivalently, the new definition calls a RV GC if its matrix representation is GC (even if the probabilities that are assigned to each row are not all the same).*
- *To the best of our knowledge, all known optimal perfect SSSs are uniform (and even* strongly-uniform *which is a more demanding property, see Section 4.3). Here, a SSS for an access structure is called optimal if there is no other SSS for the same access structure which decreases the information ratio of some participant without increasing it for the others. In particular, all well-known classes of SSSs (e.g., linear, abelian and homomorphic), are usually defined to be uniform by default. It is an open problem if non-uniform SSSs can outperform the uniform ones with respect to information ratio.*

4 A necessary and sufficient condition for inherent group-characterizability

In this section, we present a *key theorem* which provides a necessary and sufficient condition for a matrix to be IGC. First, we introduce the required tools and definitions in Section 4.1. Then, we present our key theorem and its proof in Section 4.2. Some applications of the key theorem are discussed in Section 4.3.

4.1 Automorphisms group of a matrix and its properties

Our main tool for determining the inherent group-characterizability of a given matrix is the notion of group automorphism of a matrix. To define this notion, we need to define two actions on matrices. The reader may recall the notion of group action, given in Appendix B.

Definition 4.1 (Permutation action) *Let M be a matrix with m rows and $\sigma \in S_m$, where S_m is the symmetric group of order m. The action $\sigma \cdot M$ is defined to be a matrix with m rows whose i'th row is the $\sigma(i)$'th row of M.*

Definition 4.2 (Reordering action) *A relabeling $\left(f^1, f^2, \ldots, f^n\right)$ of a matrix M is called a* reordering *if each f^j is a permutation on the set of distinct elements of M^j, the j'th column of M.*

Notice that a reordering of a matrix does not introduce new entries and only exchanges entries of each column. Sometimes, reordering of a matrix behaves the same way as permuting the rows. This is a motivation for the following definition.

Definition 4.3 (Automorphisms group of a matrix) *Let M be a matrix with m rows. The set of all automorphisms of M is defined as follows,*

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

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

By Proposition 4.5, $\mathrm{Aut}(M)$ is a subgroup of S_m. It is also easy to verify that the reordering that corresponds to an automorphism σ is unique, which we denote by f_σ. Conversely, the automorphism that corresponds to a reordering is *unique* if the matrix does not have duplicate rows, which we assume to be the case throughout the paper.

Example 4.4 *Below we present a matrix M along with all its automorphisms and their corresponding reorderings (e is the identity permutation):*

$$M = \begin{bmatrix} a & b & a \\ a & a & b \\ b & b & b \\ b & a & a \end{bmatrix},$$

$$\begin{array}{ll} \sigma_1 = e & f_{\sigma_1} = (e, e, e) \\ \sigma_2 = (1\ \ 2)(3\ \ 4) & f_{\sigma_2} = (e, (a\ \ b)(a\ \ b)) \\ \sigma_3 = (1\ \ 3)(2\ \ 4) & f_{\sigma_3} = ((a\ \ b), e, (a\ \ b)) \\ \sigma_4 = (1\ \ 4)(2\ \ 3) & f_{\sigma_4} = ((a\ \ b), (a\ \ b), e)\,. \end{array}$$

Some properties of automorphisms and relabelings are given in the following proposition, which will be used later.

Proposition 4.5 *The following statements are true for a matrix M:*

i) *For every permutations σ and relabelings f, we have $f \cdot (\sigma \cdot M) = \sigma \cdot (f \cdot M)$.*
ii) *If $\sigma, \tau \in \mathrm{Aut}(M)$, then we have $\sigma \circ \tau \in \mathrm{Aut}(M)$. Additionally, $f_{\sigma\circ\tau} = f_\tau \circ f_\sigma$.*
iii) *If $\sigma \in \mathrm{Aut}(M)$, then $\sigma^{-1} \in \mathrm{Aut}(M)$. Additionally, $f_{\sigma^{-1}} = f_\sigma^{-1}$.*
iv) *$\mathrm{Aut}(M)$ is a subgroup of S_m.*
v) *For every relabeling f, we have $\mathrm{Aut}\,(f \cdot M) = \mathrm{Aut}(M)$.*
vi) *For every $\tau \in S_m$, we have $\mathrm{Aut}\,(\tau \cdot M) = \tau \circ \mathrm{Aut}(M) \circ \tau^{-1}$.*
vii) *For every $A \subseteq [n]$, we have $\mathrm{Aut}(M) = \mathrm{Aut}\left(M^A\right) \cap \mathrm{Aut}\left(M^{[n]\setminus A}\right)$, where M^A is the sub-matrix with columns indexed by elements in A.*

Proof. All statements are easy to prove. For example we prove part (vi).

$$\begin{aligned} \sigma \in \mathrm{Aut}\,(\tau \cdot M) &\iff \exists f \quad s.t. \quad \sigma \cdot (\tau \cdot M) = f \cdot (\tau \cdot M) \\ &\iff \exists f \quad s.t. \quad (\sigma \circ \tau) \cdot M = \tau \cdot (f \cdot M) \\ &\iff \exists f \quad s.t. \quad \left(\tau^{-1} \circ \sigma \circ \tau\right) \cdot M = f \cdot M \\ &\iff \tau^{-1} \circ \sigma \circ \tau \in \mathrm{Aut}(M) \\ &\iff \sigma \in \tau \circ \mathrm{Aut}(M) \circ \tau^{-1} \end{aligned}$$

□

4.2 The key theorem

We now present and prove our key theorem which provides a necessary and sufficient condition for a matrix to be IGC. The reader may recall the notion of transitivity of a group action, given in Appendix B.

Theorem 4.6 (Key theorem) *A matrix M is IGC if and only if the group $\mathrm{Aut}(M)$ acts transitively on the set $[m]$, where m is the number of rows of M.*

Proof. **(Only-if part)** First assume that the matrix $M = [m_{ij}]_{m\times n}$ is itself GC and induced by $[G : G_1, \cdots, G_n]$. We show that for every $i, j \in [m]$, there exists a $\sigma \in \mathrm{Aut}(M)$ such that $\sigma(i) = j$.

Observe that for a given $g \in G$, the (left) multiplication of g by entries of M, i.e., $[gm_{ij}]$, is a row-permutation of M. Denote its corresponding permutation by $\sigma_g \in S_m$. Therefore, $\sigma_g \cdot M = [gm_{ij}]$. On the other hand, $[gm_{ij}]$ is a relabeling

of M for $f_g = (f_g^1, \ldots, f_g^n)$, where $f_g^j : G/G_j \to G/G_j$ sends xG_j to gxG_j. Therefore, $f_g \cdot M = [gm_{ij}]$ and hence $\sigma_g \in \mathrm{Aut}(M)$.

Let $(x_iG_1, \ldots, x_iG_n)$ and $(x_jG_1, \ldots, x_jG_n)$ be the i-th and j-th rows of M, respectively. Let $g = x_j x_i^{-1}$ and $\sigma = \sigma_g$. Since $\sigma \cdot M = \sigma_g \cdot M = [gm_{ij}]$, the i-th row of $\sigma \cdot M$ is the j-th row of M. That is, $\sigma(i) = j$.

Now let M be an IGC matrix. Thus, there exists a GC matrix M' and a relabeling f such that $M = f \cdot M'$. By Proposition 4.5 (part v)), $\mathrm{Aut}(M) = \mathrm{Aut}(M')$, from which the claim follows.

(If part) Let $M = [m_{ij}]_{m\times n}$ and $H = \mathrm{Aut}(M)$ act transitively on the set $[m]$. For every $j \in [m]$, let

$$H_j = \{\sigma \in H : f_\sigma^j(m_{1j}) = m_{1j}\},$$

where $f_\sigma = \left(f_\sigma^1, f_\sigma^2, \ldots, f_\sigma^n\right)$ is the corresponding reordering of σ. Let M_H be the matrix representation of $[H : H_1, \cdots, H_n]$. It is enough to show that M is a relabeling of M_H and, therefore, M is IGC. For every $j \in [n]$, define F^j from the set of elements of M_H^j to the set of elements of M^j by $F^j(\sigma H_j) = m_{\sigma(1)j}$. We claim that $F = (F^1, \ldots, F^n)$ is a relabeling. First notice that F^j, $j \in [m]$, is well-defined and one-to-one; because:

$$\begin{aligned}
\sigma H_j = \tau H_j &\iff \tau^{-1} \circ \sigma \in H_j \\
&\iff f^j_{\tau^{-1}\circ\sigma}(m_{1j}) = m_{1j} \\
&\iff \left(\left(f_\tau^j\right)^{-1} \circ f_\sigma^j\right)(m_{1j}) = m_{1j} \\
&\iff f_\sigma^j(m_{1j}) = f_\tau^j(m_{1j}) \\
&\iff m_{\sigma(1)j} = m_{\tau(1)j} \\
&\iff F^j(\sigma H_j) = F^j(\tau H_j).
\end{aligned}$$

It remains to show that F^j is onto. Let m_{ij} be an arbitrary element of M^j. Since the action of H on $[m]$ is transitive, for all $i \in [m]$, there is a $\sigma \in H$ such that $\sigma(1) = i$. Therefore, $F^j(\sigma H_j) = m_{\sigma(1)j} = m_{ij}$. □

The above proof provides a systematic way of finding a group characterization for an IGC matrix M. We remark that if M itself is GC, the constructed group characterization might differ from the original one. For completeness and ease of reference, below we present a proposition which was essentially proved in the "if part".

Proposition 4.7 *Let $M = [m_{i,j}]_{m\times n}$ be a matrix and H be a subgroup of $\mathrm{Aut}(M)$ that acts transitively on the set $[m]$. Then, $[H : H_1, \cdots, H_n]$ is a group-characterization of M, where*

$$H_j = \{\sigma \in H : f_\sigma^j(m_{1j}) = m_{1j}\},$$

and $\left(f_\sigma^1, f_\sigma^2, \ldots, f_\sigma^n\right)$ is the (unique) reordering that corresponds to σ.

Corollary 4.8 *For an inherently group-characterizable matrix M with m rows, it holds that m divides $|\mathrm{Aut}(M)|$.*

Proof. Let $H = \mathrm{Aut}(M)$ and $H_1, \ldots, H_n$ be as in Proposition 4.7. Since M is IGC, the matrix representation of $\pi = [H : H_1, \cdots, H_n]$, which we denote by M_π, is a relabeling of M. We know that M_π has $\frac{|H|}{|\bigcap_{i=1}^n H_i|}$ rows. On the other hand, M is a relabeling of M_π and, hence, they have the same number of rows. Therefore, m divides $|H|$. Since H is a subgroup of $\mathrm{Aut}(M)$, m divides $|\mathrm{Aut}(M)|$ too. □

4.3 Applications of the key theorem

Recall that our key theorem provides a necessary and sufficient condition for a matrix to be IGC. The *sufficiency condition* is useful for constructing a main group and some subgroups for an IGC matrix (see Proposition 4.7). In the next section, we present an application of this result to homomorphic SSSs.

The *necessary* condition, on the other hand, helps us to give examples of RVs which are not IGC. In a follow-up work [31], we have used this part of the theorem to show the existence of ideal perfect SSS which are not IGC (refer to [31] for motivations of this result). Below, we mention another application to what we call strongly-uniform RVs.

On strongly-uniform RVs. We say that a jointly distributed RV $(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ is *strongly-uniform* if, for all $A \subseteq [n]$, the marginal distribution $\mathbf{x}_A = (\mathbf{x}_i)_{i \in A}$ is uniformly distributed on its support. Such random variables have been studied in [11][1]. GCRVs are clearly strongly-uniform. We show that the converse is not necessarily true. Consider the following matrix with six rows and uniform distribution on each row. The corresponding RV is clearly quasi-uniform. However, since $\mathrm{Aut}(M) = \{e, (1\ 6)(2\ 5)(3\ 4)\}$, by Corollary 4.8, it is not IGC (because $6 \nmid |\mathrm{Aut}(M)|$).

$$M = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 3 & 2 & 3 \\ 1 & 2 & 2 \\ 2 & 3 & 3 \\ 3 & 3 & 1 \end{bmatrix} .$$

Strongly-uniform RVs are interesting in the context of SSSs because it is an open problem if there are *optimal* perfect SSSs which are not strongly-uniform. See the second part of Remark 3.5.

[1] In [11], they have been called *quasi-uniform*, but we prefer the terminology strongly-uniform as it is clear from the context.

5 An equivalent definition for homomorphic SSSs

In this section, we use our key theorem (Theorem 4.6) to present an equivalent definition for homomorphic SSSs in terms of GC ones.

5.1 Homomorphic SSSs

A homomorphic SSS is a scheme with the following properties. First, the secret space and all share spaces are groups. Second, multiplying the corresponding shares of two secrets results in valid shares for the product of the secrets. Third, the scheme is uniformly distributed on its support (see Remark 3.5). This notion can be extended to RVs and matrices. Below, we present the definition for matrices.

Definition 5.1 (Homomorphic matrix) *Let M be a matrix such that the set of elements in each column has a group structure. We call M homomorphic if the product of every pair of rows $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$, defined by $\alpha\beta = (\alpha_1\beta_1, \ldots, \alpha_n\beta_n)$, is also a row of the matrix.*

Now, consider a GC SSS which is induced by $[G : G_0, G_1, \cdots, G_n]$ and assume that each subgroup G_i is normal in the main group G. Consequently, each quotient G/G_i is a group and it is easy to see that the scheme is homomorphic.

Proposition 5.2 (Normal $\Longrightarrow$ Homomorphic) *Every GC SSS with normal subgroups in the main group is homomorphic.*

In the following subsection we show that the converse of the above proposition is true.

5.2 Homomorphic SSSs are IGC with normal subgroups

In this subsection, we prove the following theorem.

Theorem 5.3 (Homomorphic $\Longrightarrow$ Normal) *Every homomorphic SSS is IGC with normal subgroups in the main group.*

Using the sufficient condition of our key theorem (Theorem 4.6), we first show that a homomorphic matrix is IGC. However, the theorem does not guarantee the existence of a group-characterization with normal subgroups. To handle this issue, we introduce the notion of *inner automorphisms group* for homomorphic matrices which helps us to find a group-characterization with normal subgroups.

Existence of a group-characterization. Let $M = [m_{ij}]_{m\times n}$ be a homomorphic matrix and β be a row of M. It is easy to see that the mapping $\alpha \longmapsto \beta\alpha$, on the set of rows of M, is a permutation. Let $\sigma_\beta \in S_m$ denote the corresponding permutation. We show that σ_β is an automorphism of M. That is, there exists a reordering f such that $f \cdot M = \sigma_\beta \cdot M$. Let $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$. Since β_j and m_{ij} are elements of the same group, their product is well-defined. Let

$$f_\beta^j(m_{ij}) = \beta_j m_{ij} \ , \tag{5.1}$$

which is obviously a permutation. Therefore, $f = \left(f_\beta^1, f_\beta^2, \ldots, f_\beta^n\right)$ is a reordering that satisfies $\sigma_\beta \cdot M = [\beta_j m_{ij}] = f \cdot M$. Thus, $\sigma_\beta \in \mathrm{Aut}(M)$.

Now, let α_i and α_j be the i'th and j'th rows of M, respectively, and $\beta = \alpha_j \alpha_i^{-1}$. It is clear that $\sigma_\beta(i) = j$. Hence, $\mathrm{Aut}(M)$ acts transitively on the set $[m]$. Therefore, by Theorem 4.6, M is IGC.

Inner automorphisms group. In order to show the existence of a group-characterization with normal subgroups, we introduce the notion of *inner automorphisms group* of a homomorphic matrix. Let M be a homomorphic matrix with m rows and β be a row of M. Let $\sigma_\beta \in S_m$ correspond to the permutation $\alpha \longmapsto \beta\alpha$, on the set of rows of M. We call σ_β an inner automorphism of M and define the set of inner automorphisms of M as

$$\mathrm{Inn}(M) = \{\sigma_\beta : \beta \text{ is a row of } M\} \ .$$

Finding a normal characterization. Clearly, $\mathrm{Inn}(M)$ is a subgroup of $\mathrm{Aut}(M)$. Also, based on our previous discussion, $\mathrm{Inn}(M)$ acts transitively on the set $[m]$, because σ_β's belong to $\mathrm{Inn}(M)$. By Proposition 4.7, $[H : H_1, \cdots, H_n]$ is a group-characterization for M, where $H = \mathrm{Inn}(M)$ and

$$H_j = \{\sigma \in H : f_\sigma^j(m_{1j}) = m_{1j}\}$$

where $f_\sigma = \left(f_\sigma^1, f_\sigma^2, \ldots, f_\sigma^n\right)$ is the reordering that corresponds to the permutation $\sigma \in H$ and $(m_{11}, \ldots, m_{1n})$ is the first row of M.

We show that $[H : H_1, \cdots, H_n]$ is a normal characterization; that is, for all $j \in [n]$, the subgroup H_j is normal in $H = \mathrm{Inn}(M)$. By Equation (5.1), we have:

$$H_j = \{\sigma_\beta : \beta \text{ is a row of } M \text{ and } \beta_j = e\} \ ,$$

where $\beta = (\beta_1, \ldots, \beta_n)$.

For proof of normality, we need to show that for every $\sigma_\alpha \in \mathrm{Inn}(M)$ and $\sigma_\beta \in H_j$, we have $\sigma_\alpha \circ \sigma_\beta \circ \sigma_\alpha^{-1} \in H_j$. It is clear that $\sigma_\alpha \circ \sigma_\beta \circ \sigma_\alpha^{-1} = \sigma_\alpha \circ \sigma_\beta \circ \sigma_{\alpha^{-1}} = \sigma_{\alpha\beta\alpha^{-1}}$. The claim then follows because $\alpha\beta\alpha^{-1}$ is a row of M and its j'th element is identity (since $\beta_j = e$).

6 Applications of our equivalent definition

Except a few results about homomorphic SSSs (HSSSs), which was reviewed in the introduction (Section 1.1), our knowledge about theses schemes is very limited. In this subsection, we will provide two applications of our equivalent definition for HSSSs to achieve some new results about them. We need some preliminaries for this section that will be introduced in Section 6.1. Applications will be mentioned in Sections 6.2 and 6.3

6.1 Preliminaries

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 *commuting*; that is, $H * K = K * H$.

Let $(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ be a GCRV induced by a tuple $[G : G_0, G_1, \ldots, G_n]$. As we mentioned at the end of Section 2.1, for every subset $A \subseteq [n]$, the marginal RV $\mathbf{x}_A = (\mathbf{x}_i)_{i \in A}$ is uniformly distributed on its support $\left\{ (gG_i)_{i \in A} : \ g \in G \right\}$ which has $|G/G_A|$ elements, where $G_A = \bigcap_{i \in A} G_i$. Therefore, $\mathrm{H}(\mathbf{x}_A) = \log \frac{|G|}{|G_A|}$.

By definitions of conditional entropy and mutual entropy, the following relations then easily follow:

$$\mathrm{H}(\mathbf{x}_A | \mathbf{x}_B) = \log \frac{|G_B|}{|G_{A \cap B}|} \ , \tag{6.1}$$

$$\mathrm{I}(\mathbf{x}_A : \mathbf{x}_B) = \log \frac{|G|}{|G_A * G_B|} \ , \tag{6.2}$$

where the latter is obtained by using the product formula $|G_A * G_B| = \frac{|G_A| \cdot |G_B|}{|G_A \cap G_B|}$.

6.2 Lower bound on the information ratio of HSSS

Determining the information ratio of access structures is a challenging open problem in theory of SSS, even for restricted classes of interest. A notable approach for finding a lower bound on the information ratio is to use the so-called Shannon-type or non-Shanon-type information inequalities (e.g., see [4, 10, 15]). Recently, Farràs et al. [20] have used the *common information (CI)* property of random variables to derive lower bounds on the information ratio of access structures. The derived lower bounds apply to any class of SSSs that satisfies the CI property. In particular, it applies to the class of linear and abelian SSSs, which are known to satisfy the CI property, as it was explicitly mentioned in [20]. In the following we show that the CI property is satisfied by a subclass of GC SSSs whose subgroups have some particular property. Then, we show that normal subgroups satisfy that property, and consequently, HSSSs are included in this subclass (because by our equivalent definition HSSSs are GC with normal subgroups). We conclude that every lower bound achieved using the CI method applies to the class of HSSSs too. In particular, this observation has the following negative consequence.

A negative consequence. The information ratios of several small access structures, including some on five participants and several graph-access structures on six participants are still open for general SSSs. But the exact value of their information ratios have been determined for the class of linear schemes. This

project was initiated in [28, 37]; see [20, 24] for the latest status and references therein for the history of progress. Our result shows that *one cannot hope to improve the upper-bounds by constructing HSSSs for them*; because the lower-bounds achieved by the CI method are already met by optimal linear schemes for all the mentioned access structures.

The remaining part of this subsection is devoted to show that homomorphic RVs satisfy the CI property. Let us start by a formal definition of CI.

Definition 6.1 (Common information) *We say that a pair of jointly distributed RVs* $(\mathbf{x}, \mathbf{y})$ *satisfies the common information (CI) property if there exists a RV* $\mathbf{z}$ *such that* $\mathrm{H}(\mathbf{z}|\mathbf{x}) = \mathrm{H}(\mathbf{z}|\mathbf{y}) = 0$ *and* $\mathrm{H}(\mathbf{z}) = I(\mathbf{x} : \mathbf{y})$*. We say that a vector* $(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ *of jointly distributed RVs satisfies the CI property if for every pair of (not necessarily disjoint) subsets* $A, B \subseteq [n]$*, the joint distribution* $(\mathbf{x}_A, \mathbf{x}_B)$ *satisfies the CI property.*

The following proposition introduces a subclass of GCRVs that satisfies the CI property. Recall the notation $G_A = \bigcap_{i \in A} G_i$ and refer to Appendix A for the definition of *commuting subgroups*.

Proposition 6.2 (GCRVs with CI) *Let* $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_n)$ *be a GCRV induced by* $[G : G_1, \cdots, G_n]$ *such that for every pair of subsets* $A, B \subseteq [n]$*, the subgroups* G_A *and* G_B *are commuting. Then, the RV* $\mathbf{x}$ *satisfies the CI property.*

Proof. Fix some $A, B \subseteq [n]$. We show that there exists a RV $\mathbf{x}_0$ that captures the common information of $\mathbf{x}_A$ and $\mathbf{x}_B$. That is, $\mathrm{H}(\mathbf{x}_0|\mathbf{x}_A) = \mathrm{H}(\mathbf{x}_0|\mathbf{x}_B) = 0$ and $\mathrm{I}(\mathbf{x}_A : \mathbf{x}_B) = \mathrm{H}(\mathbf{x}_0)$.

By (6.1), we have $\mathrm{H}(\mathbf{x}_0|\mathbf{x}_A) = \log \frac{|G_A|}{|G_A \cap G_0|} = \log \frac{|G_A|}{|G_A|} = 0$. Similarly, we have $\mathrm{H}(\mathbf{x}_0|\mathbf{x}_B) = 0$. By (6.2), $\mathrm{I}(\mathbf{x}_A : \mathbf{x}_B) = \log \frac{|G|}{|G_A * G_B|}$. Since G_A and G_B are commuting subgroups, their product is a subgroup too, say G_0, which contains both G_A and G_B. Therefore, $\mathrm{I}(\mathbf{x}_A : \mathbf{x}_B) = \log \frac{|G|}{|G_0|}$. Now consider the GCRV $(\mathbf{x}_0, \mathbf{x}_A)$ induced by $[G : G_0, G_A]$. Also, $\mathrm{H}(\mathbf{x}_0) = \log \frac{|G|}{|G_0|}$. Therefore, $\mathbf{x}_0$ satisfies the required conditions. □

The following corollary then follows easily.

Corollary 6.3 *Homomorphic RVs satisfy the CI property.*

Proof. Since homomorphic RVs are equivalent to GCRVs with normal subgroups, it is sufficient to show that GCRVs with normal subgroups satisfy the property mentioned in Proposition 6.2. That is, for every pair of subsets $A, B \subseteq [n]$, the subgroups G_A and G_B are commuting. But this is clear because the intersection of normal subgroups is also normal, and any normal subgroup commutes with any other subgroup. □

6.3 On statistical and almost-perfect HSSSs

Several well-known non-perfect security notions for SSSs have been introduced in the literature. We refer to [30] for an extensive study of such notions. Two notable

examples are *statistical* and *almost-perfect* security notions. In this subsection, we will show that perfect, almost-perfect, and statistical security notions all coincide for a subclass of GC SSSs whose secret subgroup (G_0) is normal in the main group (G). By our equivalent definition for HSSSs, this class trivially contains the homomorphic ones.

Security definitions. The statistical security is a well-known and standard relaxation of perfect security, probably first mentioned in [8]. Here, we recall a definition from [30] (a similar definition can be found in [3]). A function $\varepsilon : \mathbb{N} \to \mathbb{R}$ is called negligible if $\varepsilon(k) = k^{-\omega(1)}$.

Definition 6.4 (Statistical security) *Let $\{\Pi_k\}_{k\in\mathbb{N}}$ be a family of SSSs, where $\Pi_k = (\mathbf{x}_0^k, \mathbf{x}_1^k, \ldots, \mathbf{x}_n^k)$, and Γ be an access structure on n participants. 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 $A \in \Gamma$, for 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.*

The almost-perfect SSSs have recently been studied by Csirmaz [16] in the context of *duality*. Csirmaz defines almost-perfect security in terms of the so-called *almost entropic polymatroids*. Here, we present an equivalent definition in terms of a family of SSSs.

Definition 6.5 (Almost-perfect security) *Let $\{\Pi_k\}_{k\in\mathbb{N}}$ be a family of SSSs, where $\Pi_k = (\mathbf{x}_0^k, \mathbf{x}_1^k, \ldots, \mathbf{x}_n^k)$, and Γ be an access structure on n participants. We say that $\{\Pi_k\}$ is an almost-perfect family for Γ if:*

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

Why are non-perfect SSSs important? Here, we mention one motivation for studying non-perfect security notions. We refer to [30] for further motivations. There is a natural notion for dual of an access structure and it is a long-standing open problem whether the information ratios of dual access structures are the same with respect to perfect security [27]. Building on a result by Kaced [33], Csirmaz showed that the answer is negative for the almost-perfect security notion. Therefore, it is important to understand if the information ratio of an access structure is invariant with respect to different security notions. It is a challenging open problem whether the best achievable information ratio for an access structure is the same for non-perfect and perfect SSSs. If this turns out to be the case for almost-perfect security, the original open problem for dual access structures is resolved too.

What we know. For a specific class of SSSs, the almost-perfect security notion is weaker than the statistical security. Recently, it has been proved in [30] that for the general class of SSSs (i.e., non-linear), information ratios of an access structure with respect to almost-perfect and statistical security are equal (but it is an open problem whether it remains invariant for perfect security too). For the class of linear SSSs, it is easy to argue that almost-perfect (and consequently statistical) security coincides with perfect security. This observation has already been noticed for statistical security by Beimel and Ishai [3, right after Definition 2.3]. Extending this observation to the class of abelian schemes is fairly easy[2]. But proving coincidence for any class beyond abelian SSSs (particularly, the homomorphic class using the traditional definition) is not that straightforward.

Main result. The following proposition states that almost-perfect, statistical and perfect security notions all coincide for a subclass of GC SSSs whose secret subgroup is normal in the main group. In Appendix D, we provide some technical discussion on the proof and also on the size of the discovered class.

Proposition 6.6 (Normal secret subgroup) *Let Γ be an access structure and $\{\Pi_k\}_{k\in\mathbb{N}}$ be a family of GC SSSs that almost-perfectly or statistically realizes Γ, such that the secret subgroup of every scheme Π_k is normal in its main group. Then, for every sufficiently large k, the scheme Π_k perfectly realizes Γ.*

Proof. The proof follows by the following observation. Let $\Pi = (\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_n)$ be an arbitrary group-characterizable secret sharing scheme induced by groups $[G : G_0, G_1, \ldots, G_n]$. Let $A \subseteq \{0, 1, \ldots, n\}$. By (6.1), if $\mathrm{H}(\mathbf{x}_A|\mathbf{x}_B) > 0$, then the quantity must be at least one; because $G_{A\cap B}$ is a (proper) subgroup of G_B and, hence, its order divides $|G_B|$; i.e., the ratio $\frac{|G_B|}{|G_{A\cap B}|}$ is at least two. However, in general, the analogous statement is not true for the mutual information since $G_A * G_B$ is not necessarily a subgroup of G to ensure that its size divides $|G|$. Nevertheless, if one of these subgroups is a normal subgroup in G, then $G_A * G_B$ is a subgroup of G_B and, therefore, $\mathrm{I}(\mathbf{x}_A : \mathbf{x}_B)$ must be at least one if it is positive. This argument shows that if $\{\Pi_k\}_{k\in\mathbb{N}}$ almost-perfectly realizes an access structure, then for every sufficiently large k, Π_k must be a perfect scheme for it. □

By our equivalent definition for HSSS, not only the secret subgroup, but also all share subgroups are normal in the main group. The following corollary then follows.

Corollary 6.7 (Homomorphic) *Let Γ be an access structure and $\{\Pi_k\}_{k\in\mathbb{N}}$ be a family of homomorphic SSSs that almost-perfectly or statistically realizes Γ. Then, for every sufficiently large k, the scheme Π_k perfectly realizes Γ.*

[2] Let $(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_n)$ be an abelian SSS induced by subgroups $G_0, G_1, \ldots, G_n$ of an abelian group G as defined in Definition 2.2–ii.. It can be shown that for every subset A of participants we have $\mathrm{I}(\mathbf{x}_0 : \mathbf{x}_A) = \log|G_0 \cap G_A|$, where $G_A = \sum_{i\in A} G_i$. If this quantity has a negligible difference with either $\mathrm{H}(\mathbf{x}_0)$ (for qualified A) or 0 (for unqualified A), then the difference must be zero. That is, the scheme must be perfect.

7 Conclusion and discussion

We believe that GCRVs provide a rich tool that may deepen our understating of SSSs. This concept was introduced in information theory literature in 2002. However, to the best of our knowledge, it has not grabbed the attention of cryptographers, particularly those with interests in theory of SSS.

Well-known classes of SSSs (i.e., linear, multi-linear, abelian and homomorphic) are now known to be special cases of GC SSSs. But the technicality of the proof for the homomorphic case, which was shown in this paper, is incomparable with the others.

In particular, we presented an equivalent definition for homomorphic SSSs in terms of GC schemes with normal subgroups in the main group. We also demonstrated the potential of our equivalent definition in enhancing our understanding of homomorphic SSSs, by considering two concrete examples.

We remark that our equivalent definition for homomorphic SSSs was based on the proof of our key theorem (a necessary and sufficient condition for a RV to be GC). It is interesting to see if our key theorem finds other applications. In the paper, we used it to show the existence of quasi-uniform random variables which are not inherently GC. In a follow-up work [31], as another application, we have shown the existence of ideal perfect SSSs which are not inherently GC.

On duality for non-abelian groups. Our proof for equivalence of two different definitions for homomorphic SSSs, compared to the linear and abelian schemes, is rather more complex. What makes the proof more involved is the lack of a proper notion for the dual of general (i.e., non-abelian) groups. The notion of dual of a vector space and Pontryagin dual of an abelian group leads to a useful definition for linear RVs (Definition 2.1–ii.) and abelian RVs (Definition 2.2–ii.) which makes the proof for these two classes of RVs fairly easy. A similar situation also arises with dual SSSs, which we will discuss next. It is an interesting problem to see if advanced concepts from abstract algebra, such as *unitary group representation* [5], can be used to achieve new results, which we leave for the future.

SSSs and duality. There is a well-known notion for the dual of an access structure defined by Jackson and Martin in [27]. It is a long-standing open problem if the information ratios of dual access structures are the same with respect to perfect security. The equality is known to hold for linear SSSs [19,27] and has recently been extended to abelian schemes by Jafari and Khazaei in [29], and also to ideal homomorphic schemes in the same paper. However, it is an open problem if the result can be extended to all homomorphic SSSs. The difficulty stems from the issue that we discussed earlier; i.e., lack of a proper notion of duality for general non-abelian groups.

References

1. Amos Beimel. Secret-sharing schemes: a survey. In *International Conference on Coding and Cryptology*, pages 11–46. Springer, 2011.

2. 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.
3. 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.
4. 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.
5. Bachir Bekka and Pierre de la Harpe. Unitary representations of groups, duals, and characters. *arXiv preprint arXiv:1912.07262*, 2019.
6. Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 1–10, 1988.
7. 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.
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. 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.
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 H Chan. Group characterizable entropy functions. In *2007 IEEE International Symposium on Information Theory*, pages 506–510. IEEE, 2007.
13. 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.
14. Ronald Cramer and Serge Fehr. Optimal black-box secret sharing over arbitrary abelian groups. In *Annual International Cryptology Conference*, pages 272–287. Springer, 2002.
15. László Csirmaz. The size of a share must be large. *Journal of cryptology*, 10(4):223–231, 1997.
16. László Csirmaz. Secret sharing and duality. *CoRR*, abs/1909.13663, 2019.
17. Yvo G Desmedt and Yair Frankel. Homomorphic zero-knowledge threshold schemes over any finite abelian group. *SIAM journal on Discrete Mathematics*, 7(4):667–679, 1994.
18. Randall Dougherty, Christopher F. Freiling, and Kenneth Zeger. Linear rank inequalities on five or more variables. *CoRR*, abs/0910.0284, 2009.
19. 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.

20. 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.
21. Yair Frankel and Yvo Desmedt. Classification of ideal homomorphic threshold schemes over finite abelian groups (extended abstract). In *EUROCRYPT*, 1992.
22. Yair Frankel, Yvo Desmedt, and Mike Burmester. Non-existence of homomorphic general sharing schemes for some key spaces (extended abstract). In *CRYPTO*, 1992.
23. Joseph Gallian. *Contemporary abstract algebra*. Nelson Education, 2012.
24. Motahhareh Gharahi and Shahram Khazaei. Optimal linear secret sharing schemes for graph access structures on six participants. *Theoretical Computer Science*, 2018.
25. 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.
26. 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.
27. Wen-Ai Jackson and Keith M. Martin. Geometric secret sharing schemes and their duals. *Des. Codes Cryptography*, 4(1):83–95, 1994.
28. Wen-Ai Jackson and Keith M Martin. Perfect secret sharing schemes on five participants. *Designs, Codes and Cryptography*, 9(3):267–286, 1996.
29. 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.
30. Amir Jafari and Shahram Khazaei. Partial secret sharing schemes. Cryptology ePrint Archive, Report 2020/448, 2020. https://eprint.iacr.org/2020/448.
31. Reza Kaboli, Shahram Khazaei, and Maghsoud Parviz. On ideal and weakly-ideal access structures. Cryptology ePrint Archive, Report 2020/483, 2020. https://eprint.iacr.org/2020/483.
32. 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.
33. Tarik Kaced. Information inequalities are not closed under polymatroid duality. *IEEE Trans. Information Theory*, 64(6):4379–4381, 2018.
34. 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.
35. Mulan Liu and Zhanfei Zhou. Ideal homomorphic secret sharing schemes over cyclic groups. *Science in China Series E: Technological Sciences*, 41(6):650–660, 1998.
36. Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.
37. Marten van Dijk. On the information rate of perfect secret sharing schemes. *Designs, Codes and Cryptography*, 6(2):143–169, 1995.
38. Zhanfei Zhou. Classification of universally ideal homomorphic secret sharing schemes and ideal black-box secret sharing schemes. In *International Conference on Information Security and Cryptology*, pages 370–383. Springer, 2005.

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.32], [23].

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. The intersection of a collection of normal subgroups of a group G is also a normal subgroup of G.

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*.

B Group action

We recall the notion of *group action* for readers who are less familiar with abstract algebra, along with an example.

Definition B.1 (Group action) *(Left)* action *of the group G on the set X is a function $\cdot : G \times X \to X$ with the following properties*

1. *For all $x \in X$ and for the identity element $e \in G$, we have $e \cdot x = x$.*
2. *For all $x \in X$ and $g, g' \in G$, we have $g' \cdot (g \cdot x) = (g'g) \cdot x$.*

An action of group G on X is transitive *if for all $x, y \in X$ there exists some $g \in G$ for which $g \cdot x = y$.*

Notice that if a group G acts on a set X, then each subgroup of G acts on X naturally.

Example B.2 *Here are some examples of group actions:*

- *Each subgroup of a group naturally acts on the group. The action is simply the group operation, which is not necessarily transitive. In particular, each group acts on itself transitively.*
- *Let G be a group, H be a subgroup of G and G/H be the set of left cosets of H in G. For $g \in G$ and $xH \in G/H$, $g \cdot (xH) = (gx)\, H$ is a transitive action; because for $x, y \in G$ if $g = yx^{-1}$ then $g \cdot (xH) = yH$.*
- *Let X be an arbitrary set. Any collection of functions on X, specially the set of all permutation on X denoted by S_X, acts on X. The action of a function f on an element $x \in X$ is simply $f \cdot x = f(x)$. This action is not necessarily transitive but it is so for S_X.*

C On equivalent definitions for linear and abelian RVs

In this section, we show that all three definitions for the linear (resp. abelian) RVs given in Definition 2.1 (resp. Definition 2.2) are equivalent. We only present the proof for the linear RVs. The proof for the abelian ones go through the same lines by working with abelian groups instead of vector spaces.

Equivalent (isomorphic) random variables. We say that two RVs $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_n)$ and $\mathbf{y} = (\mathbf{y}_1, \ldots, \mathbf{y}_n)$ are equivalent (or isomorphic) if there exists a tuple $f = (f_1, f_2, \ldots, f_n)$ of mappings $f_i : \mathrm{supp}(\mathbf{x}_i) \to \mathrm{supp}(\mathbf{y}_i)$ such that $(f_1(\mathbf{x}_1), \ldots, f_n(\mathbf{x}_n))$ and $(\mathbf{y}_1, \ldots, \mathbf{y}_n)$ are identically distributed.

C.1 Linear Maps $\iff$ Affine subspaces

(Linear Maps $\implies$ Affine subspaces) Recall the definition by "linear maps" and consider the linear RV $\mathbf{x} = (\mu_1(\mathbf{s}), \ldots, \mu_n(\mathbf{s}))$, defined by linear maps $\mu_i : S \to S_i$ and a uniform RV $\mathbf{s}$ on S. We show that $\mathbf{x}$ is equivalent to some linear RV $\mathbf{y}$ in terms of "affine subspaces". Let U be the vector space consisting of all tuples $(\mu_1(s), \ldots, \mu_n(s))$ with $s \in S$ and let U_i be the subspace of elements of U whose i'th component is zero. Then we have an onto linear map $U \to S_i$ that sends $(\mu_1(s), \ldots, \mu_n(s))$ to $\mu_i(s)$. By definition, the kernel of this map is U_i. Hence, we have an isomorphism $f_i : S_i \to U/U_i$. More generally, for a subset $A \subseteq \{1, \ldots, n\}$, one can show that we have the isomorphism $f_A : S_A \to U/U_A$, where $f_A = (f_i)_{i \in A}$, $S_A = \bigoplus_{i \in A} S_i$ and $U_A = \bigcap_{i \in A} U_i$. Therefore, $\big(f_1(\mu_1(\mathbf{s})), \ldots, f_n(\mu_n(\mathbf{s}))\big)$ and $\mathbf{y} = (\mathbf{u} + U_1, \ldots, \mathbf{u} + U_n)$ are identically distributed, where $\mathbf{u}$ is a uniform RV on U.

(Affine subspaces $\Longrightarrow$ Linear maps) Recall the definition by "affine subspaces" and consider the linear RV $\mathbf{x} = (\mathbf{u} + U_1, \ldots, \mathbf{u} + U_n)$, defined by the vector space U, a subspace collection $U_1, \ldots, U_n$ and a uniform RV $\mathbf{u}$ on U. Let $\mu_i : U \to U/U_i$ be the canonical projection defined by $u \mapsto u + U_i$, where U/U_i's are the quotient subspaces. Clearly, $\mathbf{x} = (\mu_1(\mathbf{u}), \ldots, \mu_n(\mathbf{u}))$, which corresponds to the definition by "linear maps".

C.2 Dual space $\Longleftrightarrow$ Affine subspaces

(Dual space $\Longrightarrow$ Affine subspaces) Recall the definition by "dual space". Let $\boldsymbol{\alpha}$ be a uniform RV on T^* and $T_1, \ldots, T_n$ be a collection of subspaces of T. Denote the induced RV by $\mathbf{x} = (\boldsymbol{\alpha}|_{T_1}, \ldots, \boldsymbol{\alpha}|_{T_n})$. Let U_i be the kernel of the map $T^* \to {T_i}^*$ defined by $\alpha \mapsto \alpha|_{T_i}$. Clearly, $\mathbf{x} = (\boldsymbol{\alpha} + U_1, \ldots, \boldsymbol{\alpha} + U_n)$. That is, $\mathbf{x}$ corresponds to the definition by "affine subspaces" where $U_1, \ldots, U_n$ is a collection of subspaces of $U = T^*$.

(Affine subspaces $\Longrightarrow$ Dual space) Recall the definition by "affine subspaces" and consider the linear RV $\mathbf{x} = (\mathbf{u} + U_1, \ldots, \mathbf{u} + U_n)$, defined by the vector space U, the subspace collection $U_1, \ldots, U_n$ and the uniform RV $\mathbf{u}$ on U. Let $T = U^*$ and T_i be a subspace of T that vanishes on U_i; that is, $T_i = \{\alpha \in U^* : \alpha(x) = 0 \text{ for every } x \in U_i\}$.

Let $\mathbf{y}$ be the RV induced by T and the subspace collection $T_1, \ldots, T_n$ according to the definition by "dual space". The same transformation that was introduced above for "Dual space $\Longrightarrow$ Affine subspaces" takes $\mathbf{y}$ to $\mathbf{x}$ isomorphically.

D Some technical discussion on proof of Proposition 6.6

Recall that the proof of Proposition 6.6 relied on the following observation. For given subgroups G_0, G_B of a finite group G, if G_0 is a normal subgroup in G, then $G_0 * G_B$ is a subgroup of G and, therefore, $\mathrm{I}(\mathbf{x}_0 : \mathbf{x}_B) = \log \frac{|G|}{|G_0 * G_B|}$ must be one if it is arbitrarily close to one.

This argument does not go through for the (general) class of GC schemes (i.e., when G_0 is not necessarily a normal subgroup in G). In general, one can construct an example where the ratio $|G|/|G_0 * G_B|$ is arbitrarily close to one. Let G be the group of order $p(p+1)$ generated by two elements a of order p and b of order $p+1$ where p is a given prime number. The only relation between a and b is $ab = b^p a$. Then it is easy to check that if we take G_0 and G_B to be the subgroups of order p generated by a and bab^{-1}, respectively, then $G_0 * G_B$ will be a subset of order p^2 and hence the ratio is $1 + 1/p$ which can be made arbitrarily close to one.

Nevertheless, this argument does not show that almost-perfect and perfect security notions do not coincide for the class of group-characterizable schemes (it just shows that the above proof does not work). More importantly, even if the two notions do not coincide for this class of schemes, their corresponding information ratios might still coincide. Both problems remain open.

How large is the discovered class. GC SSSs cover a large class of non-linear schemes. It is large enough to be "complete" for a non-perfect security notion called *quasi-perfect* [32, Chapter 5]. That is, the information ratio of an access structure with respect to quasi-uniform security can be computed by only considering the group-characterizable secret sharing schemes. This is quite non-trivial and follows by a surprising property of group-characterizable random variables [13, Theorem 4.1]. Quasi-perfect security is weaker than almost-perfect security for a specific class of schemes. However, for the general class of SSSs as well as the linear class, the quasi-perfect and almost-perfect information ratios are equal [30]. It is an open problem if GC SSSs are complete for almost-perfect, statistical or perfect security notions. It is an interesting open problem how much the normality condition of the secret subgroups shrinks the class of GC schemes.