Group-homomorphic Secret Sharing Schemes Are Group-characterizable with Normal Subgroups[⋆]

Reza Kaboli, Shahram Khazaei, Maghsoud Parviz

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

July 7, 2019

Abstract. Since the seminal work of Frankel, Desmedt and Burmester [Eurocrypt'92 & Crypto'92] there has been almost no result on the algebraic structure of homomorphic secret sharing schemes. In this paper, we revisit *group-homomorphic* schemes— those whose secret and share spaces are groups—via their connection to *group-characterizable random variables* [Chan and Yeung 2002].
A group-characterizable random variable is induced by a joint distribution on the (left) cosets of some subgroups of a main group. It is easy to see that a group-characterizable secret sharing with *normal* subgroups in the main group is group-homomorphic. In this paper, we show that the converse holds true as well.
To achieve the above claim, we present a *necessary and sufficient* condition for a joint distribution to be *inherently* group-characterizable (i.e., up to a relabeling of the elements of the support). Then, we show that group-homomorphic secret sharing schemes satisfy the sufficient condition and, consequently, they are inherently group-characterizable. We strengthen our result by showing that they indeed have a group characterization with normal subgroups in the main group.
Group-characterizable random variables are known to be *quasi-uniform* (namely, all marginal distributions are uniform). As an additional contribution, we present an example of a quasi-uniform random variable which is not inherently group-characterizable.

Key words: homomorphic secret sharing schemes, group-characterizable distribution, quasi-uniform distribution

1 Introduction

Secret sharing schemes were introduced for the case of threshold access structures by Shamir and Blakley [Sha79, Bla79]. Ito *et al.* [ISN89] extended the notion for general access structures. A *total* secret sharing scheme is a method that allows a dealer to share a secret among some participants in such a way that

[⋆] Updates of this paper will be available at: https://eprint.iacr.org/2019/576 only some certain *authorized* subsets of participants can reconstruct the secret; additionally, the *non-authorized* subsets must learn no information about the secret. A secret sharing scheme is formally defined as a joint distribution of the secret and shares which might not necessary be total to realize an access structure; that is, different subsets may gain different amount of information about the secret [OKT93, SRR02, FHKP17].

In a *homomorphic secret sharing* scheme, first introduced by Benaloh [Ben86], the secret and shares are algebraic structures—such as magma, quasi-group, semi-group, group, etc.— such that the product of the shares of a participant produces a share for the product of their corresponding secrets. Homomorphic schemes have found numerous applications in cryptographic protocols such as secure multi-party computation [BGW88].

Very little is known about homomorphic secret sharing schemes and, in particular, two classes have been studied earlier. The first one considers the secret and share spaces as magmas (hence we call them *magma-homomorphic*), and the second one assumes that they have group structures (hence termed as *group-homomorphic*). Frankel, Desmedt and Burmester [FDB92] have proved that in total group-homomorphic secret sharing schemes, the secret space is an abelian group. In a subsequent work, Frankel and Desmedt [FD92] have shown that, when the scheme is ideal, the share spaces are all isomorphic to the secret space, and hence abelian too. Additionally, they have proved that there exist infinitely many abelian groups over which there does not exist an ideal homomorphic scheme.

Group-characterizable random variables were introduced by Chan and Yeung in [CY02]. A group-characterizable random variable is induced by a finite group, called the *main group*, and some of its subgroups, along with a probability distribution on the main group[1]. A distribution $\mathbf{g}$ on G defines the joint random variable $(\mathbf{g}G_1, \dots, \mathbf{g}G_n)$ on the left cosets of its subgroups. Surprisingly, Chan and Yeung [CY02] have shown that the closure of the set of entropic points, known as the entropy region [ZY97], is equal to the convex closure of the group-characterizable entropic points with uniform distribution on the main group.

We call a secret sharing scheme group-characterizable if, as a random variable it is group-characterizable. As a consequence of Chan and Yeung's result, group-characterizable secret sharing schemes are "complete" [Kha19, Proposition C.6] for a non-total security notion called *quasi-total* [Kac11] (i.e., the information ratio of an access structure remains invariant when we restrict to the class of group-characterizable schemes).

For a group-characterizable scheme, if all the subgroups are *normal* in the main group, it is easy to check that the scheme is group-homomorphic. In this paper, we show that the converse is almost true as well. More precisely, we show that all group-homomorphic schemes are *inherently* group-characterizable

[1] This definition is a generalization of the usual definition of group-characterizable random variables in which the distribution on the main group is considered to be uniform.

with normal subgroups. That is, by *relabeling* the secret and shares, we get a group-characterizable scheme with the same joint distribution.

A discrete joint random variable with finite support can be represented by a matrix. Its rows are the elements of the support of the random variable and a distribution on the rows are sufficient to fully describe the random variable. The basic tool of this paper is to associate a group to a matrix, called the *isomorphisms group* of that matrix. By using this group and a set of well chosen subgroups, we are able to provide a group description for an inherently group-characterizable random variable. In fact, we present an easy-to-check *necessary and sufficient* condition for a random variable to be inherently group-characterizable based on its matrix representation.

As an additional contribution, we prove that the *quasi-uniform* random variables [CY99] are not necessarily inherently group-characterizable. A quasi-uniform random variable is a joint random variable such that all marginal distributions are uniform on their supports [CY02]. It is known that every group-characterizable random variable, with uniform distribution on its main group, is quasi-uniform. However, the converse is not known to be true. Using our necessary condition for group-characterizability of random variables, we present an example of a quasi-uniform random variable which is not group-characterizable.

Paper organization. Preliminaries are presented in Section 2. In Section 3, we discuss matrix representation of random variables and the concept of inherent group-characterizability. The notion of automorphisms group of a matrix is introduced in Section 4. A necessary and sufficient condition for inherent group-characterizability of random variables is introduced in Section 5. In this section, we also present our counterexample for a non-group-characterizable quasi-uniform random variable. The main result of the paper on homomorphic secret sharing is presented in Section 6.

2 Preliminaries and notation

In this section, we introduce our notation and basic concepts.

Notation. We use boldface letters for random variables. For a positive integer n, $[n]$ stands for the set $\{1, 2, \ldots, n\}$. All random variables considered in this paper are discrete with finite support. The support and Shannon entropy of a random variable $\mathbf{x}$ are denoted by $\operatorname{supp}(\mathbf{x})$ and $H(\mathbf{x})$, respectively. For a joint distribution $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)$ and a subset $A \subseteq [n]$, $\mathbf{x}_A = (\mathbf{x}_i)_{i \in A}$ denotes the marginal distribution of $\mathbf{x}$ on coordinates with elements in A. A permutation on a set E is a bijection on E. The set of all permutations on $[n]$ is denoted by S_n. The j'th column of a matrix M is denoted by M^j.

2.1 Group action

We assume that the reader is comfortable with the basics of finite groups. We recall the notion of *group action* for readers who are less familiar with the subject.

Definition 2.1 (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 2.2 *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.*

2.2 Group-characterizable and quasi-uniform random variables

In this paper, we may use random variable (r.v.) and distribution interchangeably.

Definition 2.3 (Group-characterizable r.v.) *Let G be a finite group, called the* main group*, and $G_1, \ldots, G_n$ be some subgroups of G. Let $\mathbf{g}$ be a random variable with* $\operatorname{supp}(\mathbf{g}) = G$ *and define $\mathbf{x}_i = \mathbf{g}G_i$ for all i in $[n]$; that is, the support of $\mathbf{x}_i$ is the left cosets of G_i in G. The joint random variable $(\mathbf{x}_i)_{i\in[n]}$ is said to be* group-characterizable*, induced by $(G; G_1, \cdots, G_n)$ and $\mathbf{g}$. Also, $(G; G_1, \cdots, G_n)$ is said to be a* group-characterization *for $(\mathbf{x}_i)_{i\in[n]}$.*

For a group-characterizable random variable $\mathbf{x}$, induced by $(G; G_1, \cdots, G_n)$ and $\mathbf{g}$, and for a subset $A \subseteq [n]$, the support of $\mathbf{x}_A$ is $\{(gG_i)_{i\in A} : g \in G\}$, which is a subset of the Cartesian product $\prod_{i\in A} (G/G_i)$. Equivalently, it can be viewed as the induced random variable $f(\mathbf{g})$, where $f : G \to \prod_{i=1}^{n} G_i$ is defined by $g \mapsto (gG_1, gG_2, \ldots, gG_n)$. It is easy to see that $|\operatorname{supp}(\mathbf{x}_A)| = |G/G_A|$, where $G_A = \bigcap_{i\in A} G_i$.

For more information on group-characterizable random variables and their properties refer to [Cha07, CY02]. We remark that in the original definition [CY02] the distribution on the main group was assumed to be uniform.

Definition 2.4 (Quasi-uniform r.v.) *A jointly distributed random variable* $(\mathbf{x}_i)_{i\in[n]}$ *is said to be* quasi-uniform *if, for all* $A \subseteq [n]$*, the marginal distribution* $\mathbf{x}_A$ *on* $\operatorname{supp}(\mathbf{x}_A)$ *is uniform. In other words,*

$$\Pr(\mathbf{x}_A = x_A) = \begin{cases} 1/|\operatorname{supp}(\mathbf{x}_A)| & x_A \in \operatorname{supp}(\mathbf{x}_A) \\ 0 & \text{otherwise} \end{cases} .$$

It is easy to see that a group-characterizable random variable with uniform distribution on the main group is quasi-uniform.

2.3 Secret sharing schemes

A secret sharing scheme is a method that allows a dear to share a secret amongst a set of participants. It is formally defined as a joint distribution of the secret and shares. We refer to [Bei11] for a survey on secret sharing schemes.

Definition 2.5 (Secret sharing) *Let* n *be a positive integer. A secret sharing scheme, on participants set* $[n]$*, is a joint distribution* $\mathbf{x} = (\mathbf{x}_i)_{i\in\{0\}\cup[n]}$ *of* $n+1$ *random variables, where* $\mathbf{x}_0$ *is the secret random variable with* $H(\mathbf{x}_0) > 0$ *and* $\mathbf{x}_i$ *is the share random variable of participant* $i \in [n]$*.*

The dealer samples $(x_i)_{i\in\{0\}\cup[n]}$ according to the joint distribution $\mathbf{x}$ and keeps x_0 as the secret for himself. He then privately sends the share x_i to participant i. In a total secret sharing scheme the secret can be reconstructed only by a certain subset of participants, called *qualified subsets*. The remaining subsets, called *unqualified*, are required to gain no information on the secret. That is, for all $A \subseteq [n]$ either $H(\mathbf{x}_0|\mathbf{x}_A) = 0$ or $H(\mathbf{x}_0|\mathbf{x}_A) = H(\mathbf{x}_0)$. Non-total schemes [FHKP17] allow any subset to gain any (monotone) amount of information on the secret.

A secret sharing scheme is said to be *group-characterizable* if, as a joint distribution, it is group-characterizable.

3 Inherently group-characterizable random variables

In this section, we introduce the notion of *inherently* group-characterizable random variables. We will work with *matrix representation* of random variables and introduce the concept of *relabeling* that allows us to define a notion of isomorphism for matrices.

A joint distribution of random variables can be represented in several ways. For example its support's elements can be viewed as the rows of a matrix, together with a non-zero probability assigned to each row. We are not usually concerned about the distribution on rows and mostly focus on the matrix itself.

Example 3.1 *The matrix representation of a group-characterizable random variable, induced by a tuple $\pi = (G; G_1, \cdots, G_n)$ is of the form*

$$\mathcal{M}(\pi) = \begin{bmatrix} g_1G_1 & g_1G_2 & \cdots & g_1G_n \\ g_2G_1 & g_2G_2 & \cdots & g_2G_n \\ \vdots & \vdots & & \vdots \\ g_mG_1 & g_mG_2 & \cdots & g_mG_n \end{bmatrix},$$

where all the rows are distinct and $\{g_1, g_2, \ldots, g_m\}$ is some (possibly proper) subset of G, because it is easy to show that $m = \frac{|G|}{|\bigcap_{i=1}^{n} G_i|}$.

We do not distinguish between two jointly distributed random variables whose 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. 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 of M^j, the jth column of M, 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

$$f^j \cdot M^j = [f^j \left(m_{ij}\right)]_{m\times 1}.$$

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

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

Definition 3.4 (Inherently group-characterizable r.v.) *A jointly distributed random variable $\mathbf{x}$ is said to be* inherently *group-characterizable if there exists a group-characterizable random variable $\mathbf{y}$ whose matrix representation is a relabeling of that of $\mathbf{x}$.*

Note that the inherent group-characterizability of a random variable is merely defined based on its matrix representation without taking the probability density itself into account. Therefore, we may also call a matrix group-characterizable.

4 Automorphisms group of a matrix

Our main tool for distinguishing an inherently group-characterizable matrix and finding a group characterization for it, if it is group-characterizable, is the notion of automorphism for a matrix.

4.1 Definition

To define the notion of automorphism of a matrix, we first need to introduce two actions on matrices.

Definition 4.1 (Permutation action) *Let M be a matrix with m rows and $\sigma \in S_m$. 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 4.2 (Reordering action) *A relabeling $\left(f^1, f^2, \ldots, f^n\right)$ of a matrix M is called a* reordering *when each f^j is a permutation on the set of distinct elements of M^j.*

Therefore a reordering of a matrix does not introduce new entries and only exchanges entries of each collumn. Sometimes reordering 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 Aut(M) *is called an automorphism.*

One can easily show that Aut(M) is a subgroup of S_m (see Proposition 4.5 parts 3 and 4). It is also easy to verify that the labeling (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.

Example 4.4 *All automorphisms of the matrix*

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

are given below along with their corresponding labellings (e is the identity permutation):

$$\sigma_1 = e \quad , \quad f_{\sigma_1} = (e, e, e)$$

$$\sigma_2 = (1 \;\; 2)(3 \;\; 4) \quad , \quad f_{\sigma_2} = (e, (a \;\; b), (a \;\; b))$$

$$\sigma_3 = (1 \;\; 3)(2 \;\; 4) \quad , \quad f_{\sigma_3} = ((a \;\; b), e, (a \;\; b))$$

$$\sigma_4 = (1 \;\; 4)(2 \;\; 3) \quad , \quad f_{\sigma_4} = ((a \;\; b), (a \;\; b), e)\,.$$

4.2 Properties

Below we present some properties of automorphisms and relabellings. The proofs are easy and left to the reader.

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

1. *$\sigma \cdot M$ and $f \cdot M$ are group action*[2]*.*
2. *For all permutations σ and relabellings f, $f \cdot (\sigma \cdot M) = \sigma \cdot (f \cdot M)$.*
3. *For $\sigma, \tau \in \mathrm{Aut}(M)$, with labellings f_σ and f_τ, we have $\sigma \circ \tau \in \mathrm{Aut}(M)$ with labeling $f_\tau \circ f_\sigma$. In other words $f_{\sigma \circ \tau} = f_\tau \circ f_\sigma$.*
4. *If f_σ is the labeling of $\sigma \in \mathrm{Aut}(M)$, then $\sigma^{-1} \in \mathrm{Aut}(M)$ with the labeling f_σ^{-1}. In other words $f_{\sigma^{-1}} = f_\sigma^{-1}$.*

Proposition 4.6 *The following statements are true for an $m \times n$ matrix M:*

1. *$\mathrm{Aut}(M)$ is a subgroup of S_m.*
2. *For every relabeling f, $\mathrm{Aut}\,(f \cdot M) = \mathrm{Aut}(M)$.*
3. *For every $\tau \in S_m$, $\mathrm{Aut}\,(\tau \cdot M) = \tau \circ \mathrm{Aut}(M) \circ \tau^{-1}$.*
4. *For every $A \subseteq [n]$, $\mathrm{Aut}(M) = \mathrm{Aut}\left(M^A\right) \cap \mathrm{Aut}\left(M^{[n]\setminus A}\right)$, 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 (3).

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

□

5 A necessary and sufficient condition for inherent group-characterizability

In this section, we provide a necessary and sufficient condition for a matrix to be inherently group-characterizable. The sufficiency proof is constructive and, as a result, we give a method for constructing a main group and some subgroups for an inherently group-characterizable matrix. Moreover, the necessary condition helps us to give an example of a quasi-uniform random variable which is not inherently group-characterizable.

[2] The set X and the group G are clear in both cases (see Definition 2.1). For example, in $\sigma \cdot M$, the set X is the set of all row-permutations of M and G is the permutation group S_m, where m is the number of rows of M.

Theorem 5.1 (Inherent group-characterizability) *A matrix M is inherently group-characterizable if and only if* $\mathrm{Aut}(M)$ *acts transitively on* $[m]$*, where* m *is the number of rows of* M*.*

Proof. **(Only-if part)** First assume that the matrix $M = [m_{ij}]_{m\times n}$ itself is group-characterizable and induced by a tuple $(G; G_1, \cdots, G_n)$. We show that for every $i, j \in [m]$, there exist 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 $f_g = (f_g^1, \dots, f_g^n)$, 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 $(x_iG_1, \dots, x_iG_n)$ and $(x_jG_1, \dots, x_jG_n)$ be the i-th and j-th rows of M, respectively. Let $g = x_jx_i^{-1}$ 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 inherently group-characterizable matrix. There exist a group-characterizable matrix M' and a relabeling f such that $M = f \cdot M'$. By Proposition 4.6 (part 2), $\mathrm{Aut}(M) = \mathrm{Aut}(M')$, from which the claim follows.

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

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

where $f_\sigma = \left(f_\sigma^1, f_\sigma^2, \dots, f_\sigma^n\right)$ 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 it inherently group-characterizable. 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 $F = (F^1, \dots, F^n)$ 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's are 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 proof of above theorem provides a systematic way for finding a group characterization for an inherently group-characterizable matrix M. We remark that if M itself is group-characterizable, the constructed group characterization might differ from the original one. For completeness and ease of reference, below we present a proposition which can be proved similar to the proof of the if-part of the theorem.

Proposition 5.2 *Let $M = [m_{i,j}]_{m\times n}$ be a matrix and H be a subgroup of* $\mathrm{Aut}(M)$ *that acts transitively on $[m]$. Then, the tuple $(H; H_1, \cdots, H_n)$ 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 reordering that corresponds to σ.

Corollary 5.3 *For an inherently group-characterizable matrix M with m rows, it holds that $m \mid |\mathrm{Aut}(M)|$.*

Proof. Let $H = \mathrm{Aut}(M)$ and $H_1, \ldots, H_n$ be as in Proposition 5.2. Since M is inherently group-characterizable, the matrix representation of $\pi = (H; H_1, \ldots, H_n)$ is a relabeling of M. By definition, $M(\pi)$ has $m = \frac{|H|}{|\bigcap_{i=1}^n H_i|}$ rows. On the other hand, M is a relabeling of $M(\pi)$ and hence they have the same number of rows. Therefore, $m \mid |\mathrm{Aut}(M)|$. □

As we mentioned earlier, group-characterizable random variables are quasi-uniform. However, the converse is not known to be true. In the following, we demonstrate that there exist a quasi-uniform random variable which is not group-characterizable. Consider the following matrix with six rows and uniform distribution on each row:

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

Obviously, the corresponding joint random variable is quasi-uniform. On the other hand, $\mathrm{Aut}(M) = \{e, (1\ 6)(2\ 5)(3\ 4)\}$. By Corollary 5.3, the distribution is not inherently group-characterizable, because $m = 6$ does not divide $|\mathrm{Aut}(M)| = 2$.

Theorem 5.4 *The class of inherently group-characterizable random variables is a proper subclass of quasi-uniform random variables.*

We remark that it remains open if the set of quasi-uniform entropic points is larger than the set of group-characterizable entropic point. We recall that a point $\left(h_A\right)_{A\subseteq[n]} \in \mathbb{R}^{2^n}$ is said to be (group-characterizable/quasi-uniform) entropic if there exists a (group-characterizable/quasi-uniform) random variable $\mathbf{x} = (\mathbf{x}_i)_{i\in[n]}$ such that $h_A = H(\mathbf{x}_A)$ for every $A \subseteq [n]$.

6 Group-characterizability of homomorphic secret sharing schemes

In this section, we will prove that group-homomorphic secret sharing schemes are inherently group-characterizable with normal subgroups in the main group. For group-characterizability, it is enough to show that the automorphisms group of the matrix representation of a group-homomorphic scheme satisfies the sufficient condition in Theorem 5.1. For proof of normality, we introduce the notion of *inner automorphisms group* of a group-homomorphic matrix (to be defined below) as a subgroup of its automorphisms group and then use Proposition 5.2, which as we will see works fine.

Note. We call group-homomorphic schemes simply homomorphic in this section.

6.1 Homomorphic secret sharing scheme

A homomorphic secret sharing scheme is a secret sharing scheme with the following properties. First, the set of secrets and the set of shares of each participant are groups. Second, the product of shares of two secrets are shares of the product of their corresponding secrets. Here is a formal definition.

Definition 6.1 (Homomorphic secret sharing scheme/matrix) *Let $M_{m\times n}$ be a matrix representation of a secret sharing scheme. For every $j \in [n]$, denote the set of all distinct entries of the j'th columns of M by $\mathcal{M}_j$. We call the scheme/matrix homomorphic if:*

- *each $\mathcal{M}_j$ is equipped with a binary operation that makes $\mathcal{M}_j$ a group and,*
- *the set of rows of M is a subgroup of the product group $\prod_{j=1}^{n} \mathcal{M}_j$.*

This definition shows that the product of two rows $\alpha = (\alpha_1, \ldots, \alpha_m)$ and $\beta = (\beta_1, \ldots, \beta_m)$ of a homomorphic matrix, that is, $\alpha\beta = (\alpha_1\beta_1, \ldots, \alpha_m\beta_m)$, is also a row of the matrix.

6.2 Main result

Consider a group-characterizable secret sharing scheme which is induced by a tuple $(G; G_0, G_1, \ldots, G_n)$ and assume that each subgroup G_i is normal in G. Consequently, each quotient G/G_i is a group and it is easy to see that the scheme is homomorphic.

Proposition 6.2 *Every group-characterizable secret sharing scheme with normal subgroups is homomorphic.*

We prove that the converse of the above proposition is "almost" true.

Theorem 6.3 (Main theorem) *Every homomorphic secret sharing scheme is inherently group-characterizable with normal subgroups.*

We will show in Section 6.3 that homomorphic schemes satisfy the sufficient condition of Theorem 5.1. Therefore, the existence of a group-characterization is guaranteed. However, the subgroups might not necessarily be normal. Motivated by Proposition 5.2, we will work with another group-characterization to ensure normality. This will be discussed in Section 6.4.

6.3 A group-characterization

Let M be a homomorphic matrix with m rows 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 $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$ and $M = [m_{ij}]_{m\times n}$. Since β_j and m_{ij} are elements of the same group, their product is well-defined. Let

$$f_\beta^j\left(m_{ij}\right) = \beta_j m_{ij} \ , \tag{6.1}$$

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

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 $\sigma_\beta\left(i\right) = j$. Thus, $\mathrm{Aut}(M)$ acts transitively on $[m]$. Therefore, by Theorem 5.1, M is inherently group-characterizable.

6.4 A group-characterization with normal subgroups

In order to show that homomorphic schemes are group-characterizable with normal subgroups, we need to introduce the notion of *inner automorphisms group* of a homomorphic matrix.

Definition 6.4 (Inner automorphisms group) *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 (see Section 6.3). We call σ_β an inner automorphism of M and define the set of inner automorphisms of M as*

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

Clearly, $H = \mathrm{Inn}(M)$ is a subgroup of $\mathrm{Aut}(M)$. Also, based on our discussion in Section 6.3, $\mathrm{Inn}(M)$ acts transitively on $[m]$. By, Proposition 5.2, $(H, H_1, \ldots, H_n)$ is a group-characterization for M, where

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

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_j, $j \in [m]$, is normal in $H = \mathrm{Inn}(M)$. By notation of Section 6.3 and relation (6.1), we have:

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

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

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 rows of M and its j'th element is identity (since $\beta_j = e$).

7 Conclusion

In this paper, we presented a necessary and sufficient condition for a given joint random variable to be inherently group-characterizable. It then allowed us to show that group-homomorphic secret sharing schemes are inherently group-characterizable with normal subgroups, which was not clear beforehand. Although every group-characterizable random variable, with uniform distribution on its main group, is quasi-uniform (namely, all marginal distributions are uniform on their supports), by proposing a concrete counterexample, we showed that the converse is not necessarily true. However, it remains an open question if every quasi-uniform entropic point is group-characterizable. In this paper, our focus was on the group-homomorphic secret sharing schemes. Homomorphic schemes with simpler structures, such as magma-homomorphic schemes, and their relation to group-homomorphic ones are not well understood and, hence, left for future. Our result may be useful to achieve new findings about secret sharing schemes. For example, by using the sufficient condition of being inherently group-characterizable, one may be able to show that certain classes of secret sharing schemes (such as the ideal ones) are inherently group-characterizable. As another problem, we propose to find a necessary and sufficient condition for a given random variable to be inherently linear or abelian.

References

Bei11. Amos Beimel. Secret-sharing schemes: a survey. In *International Conference on Coding and Cryptology*, pages 11–46. Springer, 2011.

Ben86. 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.

BGW88. 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.

Bla79. George Robert Blakley. Safeguarding cryptographic keys. *Proc. of the National Computer Conference1979*, 48:313–317, 1979.

Cha07. Terence H Chan. Group characterizable entropy functions. In *2007 IEEE International Symposium on Information Theory*, pages 506–510. IEEE, 2007.

CY99. 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.

CY02. 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.

FD92. Yair Frankel and Yvo Desmedt. Classification of ideal homomorphic threshold schemes over finite abelian groups (extended abstract). In *EUROCRYPT*, 1992.

FDB92. Yair Frankel, Yvo Desmedt, and Mike Burmester. Non-existence of homomorphic general sharing schemes for some key spaces (extended abstract). In *CRYPTO*, 1992.

FHKP17. 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.

ISN89. 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.

Kac11. 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.

Kha19. Shahram Khazaei. A candidate access structure for super-polynomial lower bound on information ratio. Cryptology ePrint Archive, Report 2019/597, 2019. https://eprint.iacr.org/2019/597.

OKT93. Wakaha Ogata, Kaoru Kurosawa, and Shigeo Tsujii. Nonperfect secret sharing schemes. In *Advances in CryptologyAUSCRYPT'92*, pages 56–66. Springer, 1993.

Sha79. Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

SRR02. K. Srinathan, N. Tharani Rajan, and C. Pandu Rangan. Non-perfect secret sharing over general access structures. In *Progress in Cryptology - INDOCRYPT 2002, Third International Conference on Cryptology in India, Hyderabad, India, December 16-18, 2002*, pages 409–421, 2002.

ZY97. Zhen Zhang and Raymond W. Yeung. A non-shannon-type conditional inequality of information quantities. *IEEE Trans. Information Theory*, 43(6):1982–1986, 1997.