# On Non-Perfect Secret Sharing Schemes

Amir Jafari and Shahram Khazaei

Sharif University of Technology, Tehran, Iran
{amirjafa,shahram.khazaei}@gmail.com

February 27, 2020

**Abstract.** The information ratio of an access structure is an important parameter for quantifying the efficiency of the best secret sharing scheme realizing it. The most common security notion for a secret sharing is that of perfect realization. Several relaxations have been studied in the literature, but very little is known about the relations between information ratios of access structures with respect to different security notions. In this article, we study the relations between several well-known non-perfect security notions. Additionally, we introduce and study an extremely relaxed security notion, called *partial secret sharing*.
*First*, we prove that partial and perfect information ratios coincide for the class of linear secret sharing schemes. *Second*, we show that partial and perfect information ratios do not coincide for the class of mixed-linear schemes (i.e., schemes constructed by combining linear schemes with different underlying finite fields).
At the heart of our first result, there exists a construction that transforms a partial linear scheme into a perfect one. This result is interesting for the theory of secret sharing in the situation where one wishes to construct a perfect linear scheme for a given access structure, but for some reason it is easier to first construct a partial scheme. This situation, for example, happens in the so-called *decomposition methods*.

**Keywords:** Secret sharing · Access structure · Information ratio · Non-perfect secret sharing · Decomposition techniques.

## 1 Introduction

A *secret sharing scheme* [7, 34] is a cryptographic tool that allows a dealer to share a secret among a set of participants such that only certain *qualified* subsets of them are able to reconstruct the secret. The secret must remain hidden from the remaining subsets, called *unqualified*. The collection of all qualified subsets is called an *access structure* [20], which is supposed to be monotone, i.e., closed under the superset operation.

The *information ratio* [9, 10, 31] of a participant in a secret sharing scheme is defined as the ratio of the size (entropy) of his share and the size of the secret. The information ratio of a secret sharing scheme is the maximum (also sometimes defined as the average) of all participants' information ratios. The information ratio of an access structure is defined as the infimum of the information ratios of

all secret sharing schemes that realize it. Realization is defined with respect to some security notion, e.g., perfect or any variants of non-perfect to be discussed in next subsection. Computation of information ratio of access structures is a challengingly difficult problem.

The most common type of secret sharing schemes is the class of *linear* schemes. In these schemes, the secret is composed of some finite field elements and the sharing is done by applying some fixed linear mapping on the secret elements and some randomly chosen elements from the finite field[1].

### 1.1 Motivations

Some closely related security notions for realization of an access structure by secret sharing schemes are given below. Other examples of security notions include weakly-private [3], probabilistic [14] and computational [29] secret sharing.

- **Perfect [34]:** the qualified sets must recover the secret with probability one and it must remain information-theoretically hidden form unqualified sets.
- **Statistically-perfect [4, 6]:** the qualified sets may fail to recover the secret with some negligible probability of error; and some negligible amount of information about the secret can be leaked to unqualified sets which is quantified using the so-called notion of "statistical distance".
- **Almost-perfect [13]:** some tiny[2] amount of information (in terms of entropy) about the secret is allowed to be missed by qualified sets and to be leaked to unqualified ones.
- **Quasi-perfect [26, Chapater 5][3]:** some tiny percentage of information (in terms of entropy after normalization to the secret entropy) about the secret is allowed to be missed by qualified sets and to be leaked to unqualified ones.

In this paper, we introduce a new relaxed security notion for secret sharing schemes, called *partial security*, which will be described in Section 1.3. Our main motivation for introducing partial secret sharing is its applications in the so-called *decomposition methods* [15, 18, 35, 36], which are useful techniques for constructing a secret secret sharing scheme for a given access structure, by combining several simpler ones. We will return back to this point in Section 1.5. Other motivations for introducing and studying partial, and more generally non-perfect, secret sharing are discussed next.

We will prove (Section 6) that the following relation holds for the information ratios of an access structure with respect to the mentioned security notions:

[1] These schemes in the literature are usually called multi-linear and when the secret is a single field element, the scheme is called linear. In this paper we do not make such a distinction and simply call them linear.

[2] In the literature, a function $\varepsilon : \mathbb{N} \to \mathbb{R}^+$ is called negligible if $\varepsilon(k) = k^{-\omega(1)}$. We call it tiny if $\varepsilon(k) = \mathrm{o}(1)$.

[3] Chapter 5 of Kaced's Ph.D thesis [26] is based on the conference publication [25], in which the term "almost-perfect" has been used instead of "quasi-perfect". We reserve the former term for the third definition mentioned above.

$$\text{partial} \leqslant \text{quasi-perfect} \leqslant \text{almost-perfect} \leqslant \text{statistically-perfect} \leqslant \text{perfect} \quad (1.1)$$

Beyond that, the following trivial relation is known for the restricted class of linear schemes (e.g., see [4, right after Definition 2.3]): the notions of perfect secret sharing and almost-perfect secret-sharing coincide in the case of linear schemes; that is, any almost-perfect linear scheme by itself is a perfect one. The same holds true for statistically-perfect secret sharing.

One contribution of this work is to extend (Section 6.4) this result to a larger class which turns out to contain *homomorphic* schemes (i.e., schemes for which multiplying the corresponding shares of two secrets results in a sharing of the product of the secrets). Our extension indeed leads to a properly larger class because homomorphic schemes are known to be superior to linear ones (we say that class $A$ of schemes is superior to class $B$ if there exists an access structure whose information ratio with respect to class $A$ is smaller than when we restrict to class $B$).

In the following, we describe a situation that shows the importance of understanding the relations between different security notions.

**On duality.** Duality is a prevalent concept in different areas in mathematics such as coding and matroid theory, and there is a natural definition for the dual of an access structure [21] too. It is a long-standing open problem if the perfect information ratios of dual access structures are the same. The equality was proved for the case of linear schemes in [16, 21], which has recently been extended to the class of *abelian* schemes in [23]. Even though the original problem has resisted all efforts for more than 25 years, in a remarkable work, Kaced [27] has recently shown that the information ratios of dual access structures are not the same with respect to the weaker notion of *almost-perfect* security. An explicit access structure on 174 participants was then exhibited by Csirmaz in [13]. By (1.1), if it turns out that almost perfect and perfect information ratios coincide, the original problem is resolved too.

**Our main road map.** Notice that by (1.1), the partial and perfect security notions are farthest apart, among all mentioned security notions. Therefore, studying their corresponding information ratios with respect to different classes of schemes —with the hope to prove some coincidence or separation result— might be a good start for understanding the information ratio of non-perfect schemes. We have some results with this respect which are discussed in next subsection.

### 1.2 Main results

Unfortunately, it remains open if the partial and perfect information ratios are equal. Based on our previous discussion on duality, if this turns out to be true[4],

[4] We do not make any conjecture with this regard.

the long-standing open problem on perfect information ratios of dual access structures is resolved. Nevertheless, we resolve the problem for the following two restricted classes:

(I) **Linear.** We prove that the partial information ratio of an access structure is the same as its perfect information ratio for the class of linear schemes.
(II) **Mixed-linear.** We provide an example of an access structures such that its partial information ratio is smaller than its perfect one, for the class of mixed-linear schemes.

The class of *mixed-linear* schemes has recently been introduced in [23]. These schemes are constructed by combining linear schemes whose underlying finite fields could possibly be different. Mixed-linear schemes are superior to linear ones; but, it is an open problem if they are as powerful as the larger class of abelian schemes, or even homomorphic schemes, that they belong to.

We will discus the technicality of proving our first result in Section 1.5. For the second result, we refer to the main body of the paper in Section 5.

By result (I) and relation (1.1), information ratios of all mentioned non-perfect security notions coincide with that of perfect security, for the class of linear schemes. Two cases (i.e., statistically-perfect and almost-perfect) are trivial, as we discussed earlier. However, the other two cases (i.e., quasi-perfect and partial) are not entirely trivial as they might look at a first sight. Below, we discuss the challenge for the easier case of quasi-perfect secret sharing.

**Discussion on quasi-perfect information ratio for linear schemes.** Consider a family of linear schemes such that the secret of the $m$th scheme consists of $m$ field elements. Consider a simple case where every unqualified set learns exactly one linear relation about the secret and every qualified set learns exactly $m-1$ independent linear relations. The amount of information leak/miss, after normalization to the secret entropy, is $\frac{1}{m}$ which can be arbitrarily small if $m$ is sufficiently large. As we will see, our result on partial linear secret sharing schemes indicates that, by increasing the information ratio by a factor of $1+\mathrm{O}(\frac{1}{m})$, we can construct a perfect scheme. This may at first seem easy but notice that in the original scheme different sets of qualified/unqualified participants might have missed/gained different information on the secret (which is expressible in the form of a single linear combination of the secret elements). Some may have missed/learned one coordinate of the secret and others a different linear combination of the coordinates. So our construction needs to find a way that works no matter what the missed/learned linear combinations are. We remark that for the case where we only allow one coordinate to be missed or learned, there exists a simple solution using the so-called *ramp* [8] secret sharing schemes (e.g., see [18, Theorem 3.2]). But, as we will see, the general case needs more care.

In the remaining subsections of the introduction, we elaborate on the notion of partial secret sharing and result (I).

### 1.3 Partial secret sharing

We introduce an extremely relaxed security notion, called *partial* security, and a slightly stronger one called *semi-partial*. We say that a secret sharing scheme partially realizes an access structure if the amount of information gained by any qualified set is strictly greater than that of any unqualified one. In other words, the qualified sets have a positive *advantage* $\delta$ over the unqualified ones with regard to the secret recovery. In the semi-partial realization, we additionally require that the secret remain perfectly hidden from the unqualified sets. A perfect scheme is a partial scheme with $\delta = 1$, because qualified and unqualified sets recover 100 % and 0 % of the secret, respectively.

The perfect information ratio of a secret sharing scheme is defined on its own, i.e., regardless of what access structure it realizes, if any. However, we quantify the efficiency of a partial scheme, with respect to an access structure that it partially realizes. We define the *partial information ratio* as a scaled version of the perfect information ratio, where the scale factor is $1/\delta$ and $\delta$ is the advantage mentioned above. The intuition behind this choice stems from *decomposition constructions* [15, 18, 35, 36], which will be discussed further in the paper (Section 7).

**Main goal.** We would like to study if there is a general method to turn a partial scheme into a perfect one (of the same class) such that the information ratio of each participant increases only by a factor of $1/\delta$ (consequently, the partial and perfect information ratios will coincide). As we mentioned in Section 1.1, this is not possible for mixed-linear schemes but it is possible for linear schemes. The general case of non-linear schemes remains an open problem.

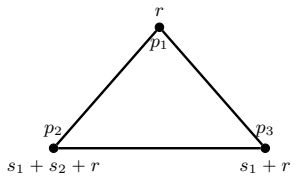
**Another view on partial secret sharing.** In perfect secret sharing, one requires every subset of participants to be either qualified (i.e., entirely recover the secret) or unqualified (i.e., gain no information on the secret). If a secret sharing scheme is not perfect, it does no define an access structure. Semi-partial secret sharing scheme allows us to associate a unique access structure to the scheme, even if it is not perfect: qualified sets are those that gain a positive amount of information about the secret. On the other hand, it might be possible to associate more than one access structure to a partial scheme, because the same scheme can be a partial secret sharing scheme for different access structures. Therefore, another novelty of our work is how to define access structure for non-perfect schemes.

### 1.4 Some examples

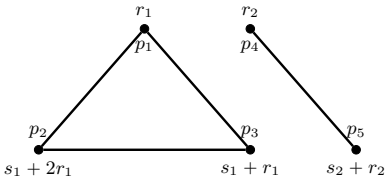
Consider the following two access structures:

$\Gamma_1$ on 3 participants with minimal qualified sets $\{p_1, p_2\}, \{p_2, p_3\}, \{p_1, p_3\}$,
$\Gamma_2$ on 5 participants with minimal qualified sets $\{p_1, p_2\}, \{p_2, p_3\}, \{p_1, p_3\}, \{p_4, p_5\}$,

where a qualified set is called *minimal* if any proper subset of it is unqualified.




(a) A linear partial scheme for $\Gamma_1$. The secret is $(s_1, s_2) \in \mathbb{F}_2 \times \mathbb{F}_2$ and $r \in \mathbb{F}_2$ is the randomness.




(b) A mixed-linear partial scheme for $\Gamma_2$. The secret is $(s_1, s_2) \in \mathbb{F}_3 \times F_2$ and the randomness is $(r_1, r_2) \in \mathbb{F}_3 \times \mathbb{F}_2$

Fig. 1: Partial schemes for $\Gamma_1$ and $\Gamma_2$. All random variables are independent and uniform on their supports.

An access structure whose all minimal qualified sets are of size two can be represented by a graph. Figure 1 shows a partial scheme for each of these access structures. The scheme for $\Gamma_1$ is linear, its secret contains two bits of information and every participant receives one bit of information as his share. The scheme for $\Gamma_2$ is mixed-linear and its secret contains $\log 6 \approx 2.58$ bits of information. The share of participants $p_4, p_5$ are each one bit, and those of participants $p_1, p_2, p_3$ are $\log 3 \approx 1.58$ bits. The scheme for $\Gamma_1$ is semi-partial with advantage $\delta_1 = \frac{1}{2}$ (every minimal qualified set gains 50 % information about the secret and unqualified sets gain no information). The scheme for $\Gamma_2$ is semi-partial too with advantage $\delta_2 = \frac{\log 2}{\log 6} \approx 0.387$.

Therefore, the partial information ratios of all participants in $\Gamma_1$ are $\frac{1}{\delta_1}\frac{1}{2} = 1$. The partial information ratios of participants $p_1, p_2, p_3$ in $\Gamma_2$ are all $\frac{1}{\delta_2}\frac{\log 3}{\log 6} = \log 3 \approx 1.58$. The partial information ratios of participants $p_4, p_5$ in $\Gamma_2$ are both $\frac{1}{\delta_2}\frac{\log 2}{\log 6} = 1$.

### 1.5 Transforming a partial linear scheme into a perfect one

Given a partial linear scheme for an access structure, we turn it into a perfect one for the same access structure while the information ratio is increased by a factor of $\frac{1}{\delta}$. For example, consider the partial linear scheme for access structure $\Gamma_1$, mentioned in Section 1.4, whose (usual) information ratio is $\frac{1}{2}$; but since its advantage is $\delta = \frac{1}{2}$, its partial information ratio is one. This scheme can be used to construct a perfect linear scheme for $\Gamma_1$ with information ratio one as follows. Use two instances of the partial scheme with independent randomnesses, one with secret $(s_1, s_2)$ and one with secret $(s_1 + s_2, s_1)$. The privacy of the scheme is immediate and its correctness can easily be verified. For example, participants $p_1$ and $p_2$ recover $s_1 + s_2$ and $s_2$ from the first and second schemes, respectively, and

since these relations are linearly independent, the secret can be fully recovered. The constructed scheme is linear with (perfect) information ratio one.

The above example was easy to handle because the partial scheme was already known to us. For the general case, we need to seek a "universal" transformation that works for "every" linear partial scheme.

**Our construction.** Assume that we are given a linear partial scheme for an access structure such that:

- the secret is composed of $m$ elements of a finite field $\mathbb{F}$,
- participant $p_i$ receives $m_i$ field elements as his share,
- every qualified subset learns at least $\lambda$ independent linear combinations of the secret elements and there is a qualified set that learns exactly $\lambda$ independent relations,
- every unqualified subset learns at most $\omega$ independent linear combinations of the secret elements and there is an unqualified set that learns exactly $\omega$ independent relations ($0 \leqslant \omega < \lambda \leqslant m$),

Clearly $\delta = \frac{\lambda-\omega}{m}$ and the partial information ratio of participant $p_i$ is $\frac{1}{\delta}\frac{m_i}{m} = \frac{m_i}{\lambda-\omega}$. In Section 4, we will show that this scheme can be turned into a perfect scheme such that the information ratio of participant $p_i$ is $\frac{m_i}{\lambda-\omega}$. Here, we present the idea for the case where $\lambda = 1$ and $\omega = 0$.

The main idea is to share carefully-chosen linear functions of the secret using the partial scheme independently. More precisely, the secret of the perfect scheme consists of $m$ field elements too which we denote by $s \in \mathbb{F}^m$. We use $m$ instances of the partial scheme with independent randomnesses. The secret of the $i$'th instance is $L_i s$, where $L_i$ is a suitable $m \times m$ matrix and $s$ is interpreted as a column vector. The challenge is to find $L_i$'s such that it works for every partial scheme. To this end, as we will see, we need to find the $m \times m$ matrices $L_1, \ldots, L_m$ such that for every non-zero row vector $x \in \mathbb{F}^m$, it holds that $xL_1, \ldots, xL_m$ are linearly independent. It is possible to construct such matrices, even though it may not sound trivial at a first glance. We will not discuss the construction here, since the more general case is discussed in the paper (Lemma 4.1).

Now let us see why the scheme is perfect. It is easy to see that the unqualified sets do not gain any information on the secret. Since $\lambda = 1$ and $\omega = 0$, a qualified set such as $B$ learns at least one linear combination on the secret elements which correspond to some non-zero row vector $x_B \in \mathbb{F}^m$ (the row vector corresponding to different sets may differ). Therefore, the qualified set $B$ learns the linear combinations $x_B L_1 s, \ldots, x_B L_m s$ of the secret $s$. Since $x_B L_1, \ldots, x_B L_m$ are linearly independent (no matter what $x_B$ is), the secret $s$ can be recovered.

The perfect and partial information ratios of participant $p_i$ are clearly the same; because the share size has increased by a factor of $m$ and, hence, his information ratio in the constructed scheme is $\frac{m \times m_i}{m} = \frac{m_i}{\lambda-\omega}$, as promised (recall $\lambda = 1, \omega = 0$).

**On weighted decompositions.** The above construction is useful in the situation where one wants to construct a linear scheme for a given access structure, but it is for some reason easier to first construct partial schemes. For example, in the so-called *weighted decomposition methods* [18, 36], several simple perfect or partial linear schemes are combined to construct a more complex partial linear scheme. Our method can then be used to transform the final partial scheme into a perfect one. Such an approach has been taken in [18] to construct optimal linear schemes for several graph access structures on six participants, which had remained open for a long time. But in [18, Theorem 3.2], a simple transformation has been used, which only works for partial linear schemes of a particular type; and this was enough for the purpose of results in [18]. More precisely, in [18], similar to [36], it is assumed that every subset of participants in the partial linear schemes, qualified or unqualified, recovers a subset of the secret elements; in other words, arbitrary linear combinations of secret elements are not allowed (for example the linear combination $s_1 + s_2$ can be learned only if $s_1$ and $s_2$ are learned). This case is rather easy to handle using ramp [8] secret sharing, as it has been employed in [18, Theorem 3.2]. To remove this strong requirement, a more complex tool than ramp secret sharing is required, which is indeed the construction discussed above.

### 1.6 Paper organization

In Section 2, we present the required preliminaries and introduce our notation. In Section 3, the partial and semi-partial security notions are introduced. Section 4 is devoted to the proof of the equality of partial and perfect information ratios for the class of linear schemes. In Section 5, we show that perfect and partial information ratios are not the same with respect to the class of mixed-linear schemes. In Section 6, we will study the relations between non-perfect secret sharing schemes and prove relation (1.1). In this section we also prove that statistical and almost-perfect security notions coincide with perfect notion for a class of secret sharing schemes that include the homomorphic ones. In Section 7, we revisit decomposition techniques and strengthen previous results. Section 8 concludes the paper.

## 2 Secret sharing schemes

In this section, we provide the basic background along with some notations. We refer the reader to Beimel's survey [1] on secret sharing.

### 2.1 General notations

All random variables are discrete in this paper. The Shannon entropy of a random variable $\boldsymbol{X}$ is denoted by $\mathrm{H}(\boldsymbol{X})$ and the mutual information of random variables $\boldsymbol{X}, \boldsymbol{Y}$ is denoted by $\mathrm{I}(\boldsymbol{X} : \boldsymbol{Y})$. The support of a random variable $\boldsymbol{X}$ is denoted by $\mathrm{supp}(\boldsymbol{X})$. For a positive integer $m$, we use $[m]$ to represent the set $\{1, \ldots, m\}$.

Throughout the paper, $P = \{p_1, \ldots, p_n\}$ stands for a finite set of *participants*. A distinguished participant $p_0 \notin P$ is called the *dealer*. Unless otherwise stated, we identify the participant $p_i$ with its index $i$; i.e., $P \cup \{p_0\} = P \cup \{0\} = \{0, 1, \ldots, n\}$. We use $2^X$ to denote the power set of a set $X$.

### 2.2 Perfect secret sharing

A secret sharing scheme is used by a dealer to share a secret among a set of participants. To this end, the dealer chooses a randomness according to a pre-specified distribution and applies a fixed and known mapping on the secret and randomness to compute the share of each participant. This definition does not assume a priori a distribution on the secret space. In this paper, we use the following definition for secret sharing.

**Definition 2.1 (Secret sharing scheme)** *A tuple $\Pi = \big(\boldsymbol{S}_i\big)_{i\in P\cup\{0\}}$ of jointly distributed random variables with finite supports is called a* secret sharing scheme *on participants set $P$ when $\mathrm{H}(\boldsymbol{S}_0) > 0$. The random variable $\boldsymbol{S}_0$ is called the* secret *random variable and its support is called the* secret space*. The random variable $\boldsymbol{S}_i$, $i \in P$, is called the* share *random variable of participant $i$ and its support is called his* share space*.*

When we say that a secret $s_0$ *is shared using* $\Pi$, we mean that a tuple $\big(s_i\big)_{i\in P\cup\{0\}}$ is sampled according to the distribution $\Pi$ conditioned on the event $\{\boldsymbol{S}_0 = s_0\}$. The share $s_i$, $i \in P$, is then privately transmitted to the participant $i$.

The above definition of secret sharing does not convey any notion of security. In the most common type of secret sharing, called perfect secret sharing, the goal of dealer is to allow pre-specified subsets of participants to recover the secret. The secret must remain information-theoretically hidden from all other subset of participants. This intuition is formally captured by following definitions.

**Definition 2.2 (Access structure)** *A non-empty subset $\Gamma \subseteq 2^P$, with $\varnothing \notin \Gamma$, is called an* access structure *on $P$ if it is* monotone*; that is, $A \subseteq B \subseteq P$ and $A \in \Gamma$ imply that that $B \in \Gamma$. A subset $A \subseteq P$ is called* qualified *if $A \in \Gamma$; otherwise, it is called* unqualified*.*

**Definition 2.3 (Perfect realization)** *We say that a secret sharing scheme $\Pi = \big(\boldsymbol{S}_i\big)_{i\in P\cup\{0\}}$ is a* (perfect) scheme *for $\Gamma$, or it* (perfectly) realizes *$\Gamma$, if the following two hold, where $\boldsymbol{S}_A = (\boldsymbol{S}_i)_{i\in A}$, for a subset $A \subseteq P$:*

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

### 2.3 Access function

Non-perfect secret sharing schemes have been studied in several works including [8,30,36]. The notion of access function, introduced in [16], is a generalization of the definition of access structures that facilitates study of non-perfect schemes.

**Definition 2.4 (Access function [16])** *A mapping $\Phi : 2^P \to [0,1]$ is called an* access function *if $\Phi(\varnothing) = 0$ and it is monotone; i.e., $A \subseteq B \subseteq P$ implies that $\Phi(A) \leqslant \Phi(B)$.*

The access function of a secret sharing scheme is then naturally defined as a function that quantifies the percentage of information about the secret gained by every subset of participants.

**Definition 2.5 (Access function of a scheme)** *The* access function *of a secret sharing scheme $\Pi = \big(\boldsymbol{S}_i\big)_{i\in P\cup\{0\}}$ is a function $\Phi_\Pi : 2^P \to [0,1]$ defined by:*

$$\Phi_\Pi(A) = \frac{\mathrm{I}(\boldsymbol{S}_0 : \boldsymbol{S}_A)}{\mathrm{H}(\boldsymbol{S}_0)} \ .$$

### 2.4 Convec and information ratio

Convec is short for contribution vector [22] and a norm on it can be used as an indication of efficiency of a secret sharing scheme.

**Definition 2.6 (Convec of a scheme)** *The* (usual) convec *of a secret sharing scheme $\Pi = \big(\boldsymbol{S}_i\big)_{i\in P\cup\{0\}}$ is denoted by* $\mathrm{cv}(\Pi)$ *and defined as follows:*

$$\mathrm{cv}(\Pi) = \big(\frac{\mathrm{H}(\boldsymbol{S}_i)}{\mathrm{H}(\boldsymbol{S}_0)}\big)_{i\in P} \ .$$

The *maximum* and *average* information ratios of a secret sharing scheme on $n$ participants with convec $(\sigma_1, \ldots, \sigma_n)$ are defined to be $\max\{\sigma_1, \ldots, \sigma_n\}$ and $(\sigma_1 + \ldots + \sigma_n)/n$, respectively. The maximum/average information ratio of an access structure is defined to be the infimum of all maximum/average information ratios of all secret sharing schemes that realize it. In this paper, we restrict our attention to maximum information ratio, unless otherwise stated.

### 2.5 Linear secret sharing

The most common definition of a linear scheme is based on linear maps. A secret sharing scheme $(\boldsymbol{S}_i)_{i\in P\cup\{0\}}$ is said to be *linear* if there are finite dimensional vector spaces $E$ and $(E_i)_{i\in P\cup\{0\}}$, and linear maps $\mu_i : E \to E_i$, $i \in P \cup \{0\}$ such that $\boldsymbol{S}_i = \mu_i(\boldsymbol{E})$, where $\boldsymbol{E}$ is the uniform distribution on $E$. The following equivalent definition turns out convenient for the purpose of this paper.

**Definition 2.7 (Linear scheme)** *A tuple $\Pi = (T; T_0, T_1, \ldots, T_n)$ is called an $\mathbb{F}$-linear (or simply a linear) secret sharing scheme if $T$ is a finite dimensional vector space over the finite field $\mathbb{F}$ and all $T_i$'s are subspaces of $T$ with $\dim T_0 \geqslant 1$. When there is no confusion, we omit $T$ and simply write $\Pi = (T_i)_{i\in P\cup\{0\}}$.*

In the following we describe the connection between Definition 2.7 and the description which was given before the definition. One can thinks of a linear secret sharing scheme as being represented by a matrix, where each row is associated to a participant or the secret. Sharing is performed by multiplying this matrix by a random vector. Then the vector space $T_i$ is the vector space generated by the rows that correspond to participant $i$; $T_0$ is the vector space generated by the rows corresponding to the secret. This is similar to the well-known definition of a linear secret sharing scheme in terms of monotone span programs [28], by Karchmer and Wigderson (or multi-target span programs [2]).

The above description essentially tells us how to associate a collection of random variables $(\boldsymbol{S}_i)_{i\in P\cup\{0\}}$ to a collection $(T_i)_{i\in P\cup\{0\}}$ of subspaces of a common vector space $T$ on a finite field $\mathbb{F}$. The induced random variable, however, depends on the selected bases for $T_i$'s. In the following, we describe a method, introduced in [19], to define an induced random variable which does not depend on the chosen bases. First, we pick a linear function $\boldsymbol{\alpha} : T \to \mathbb{F}$ uniformly at random from the set of all possible such linear functions. The random variable associated to the subspace $T_i$ is defined by $\boldsymbol{S}_i = \boldsymbol{\alpha}|_{T_i}$, i.e., the restriction[5] of the map $\boldsymbol{\alpha}$ to the domain $T_i$. It is easy to see that for $i, j \in P \cup \{0\}$, the pair $(\boldsymbol{S}_i, \boldsymbol{S}_j)$ has the same distribution as $\boldsymbol{\alpha}|_{T_i+T_j}$. More generally, for any subset $A \subseteq P \cup \{0\}$, the distribution of the random variable $\boldsymbol{S}_A = (\boldsymbol{S}_i)_{i\in A}$ is the same as $\boldsymbol{\alpha}|_{T_A}$, where $T_A = \sum_{i\in A} T_i$. Finally, notice that we have $\mathrm{H}(\boldsymbol{S}_A) = \dim T_A \log|\mathbb{F}|$. Also, using the relation $\dim(V \cap W) = \dim V + \dim W - \dim(V + W)$ for vector spaces, it easily follows that $\mathrm{I}(\boldsymbol{S}_A : \boldsymbol{S}_B) = \dim(T_A \cap T_B) \log|\mathbb{F}|$, for every pair of subsets $A, B \subseteq P \cup \{0\}$.

**Access function and convec of a linear scheme.** Based on our previous discussion, it easily follows that the access function and convec of a linear secret sharing scheme $\Pi = (T_i)_{i\in P\cup\{0\}}$ are given by the following relations

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

where $T_A = \sum_{i\in A} T_i$.

**Linear and mixed-linear information ratios.** If, in the computation of information ratio, we restrict ourselves to the class of linear schemes, we refer to the corresponding parameter as the linear information ratio. Later in Section 5.1, we define the class of mixed-linear schemes, where the corresponding parameter is referred to as the mixed-linear information ratio.

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

## 3 Partial and semi-partial secret sharing

In this section, we introduce two relaxed security notions for secret sharing schemes, referred to as semi-partial and partial realizations. Properties and applications of these new security notions will be studied in later sections.

### 3.1 Security definition

A scheme is said to partially realize an access structure if the amount of information gained on the secret by every qualified set is strictly larger than that of any unqualified one. The semi-partial definition is less relaxed since it requires that the secret still remain information theoretically hidden from unqualified sets. Below, we give a formal definition. The reader may first recall definition of access function of a secret sharing scheme (Definition 2.5).

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

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

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

The parameter $\delta$ is a *normalized* value for quantifying the advantage of the qualified sets over the unqualified ones with respect to the amount of information that they gain on the secret. The inverse of $\delta$ is an important factor that will be taken into account in next subsection to quantify the efficiency of partial schemes.

### 3.2 Partial convec and partial information ratio

We quantify the efficiency of a semi-partial or partial scheme via a scaled version of its usual convec (Definition 2.6), that we call *partial convec*. Clearly, unlike the usual convec of a scheme, which is defined on its own, the partial convec depends on the access structure that it partially realizes.

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

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

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

The intuition behind the choice of factor $\frac{1}{\delta}$ stems from decomposition constructions [15, 18, 35, 36], in which a similar scale factor appears. We will revisit decomposition methods in Section 7.

**Partial and semi-partial information ratios.** The partial information ratio of a secret sharing schemes is defined to be the maximum coordinate of its partial convec. The partial information ratio of an access structure is the infimum of all partial information ratios of all secret sharing schemes that partially realize it. Semi-partial information ratio of an access structure is defined similarly (notice that we do not actually need to define semi-partial information ratio of a secret sharing scheme as its partial information ratio just works fine). One can also speak about (semi-)partial linear information ratio of an access structure; that is, when the infimum is taken over the restricted class of linear schemes. Similarly, the (semi-)partial mixed-linear information ratio of an access structure is defined with respect to the mixed-linear class.

### 3.3 Relations between different information ratios

Denote the semi-partial, partial and perfect information ratios of an access structure $\Gamma$ by $\sigma_{\mathrm{sp}}(\Gamma)$, $\sigma_{\mathrm{p}}(\Gamma)$ and $\sigma(\Gamma)$, respectively. Clearly, we have

$$\sigma_{\mathrm{p}}(\Gamma) \leqslant \sigma_{\mathrm{sp}}(\Gamma) \leqslant \sigma(\Gamma) \ .$$

Unfortunately, it remains open if any of the inequalities is strict (more precisely, if there exists an access structure for which the inequality is strict). In Section 4 we prove that if, in the computation of information ratio, we restrict ourselves to the class of linear schemes, the three parameters coincide. In Section 5, however, we prove that the right inequality can be strict for the class of mixed-linear schemes.

## 4 Equality of perfect and partial linear information ratios

In this section, we prove that the partial linear information ratio of an access structure is the same as its perfect linear information ratio. Two linear algebraic lemmas lie at the core of our proof which are presented in Section 4.1. The first one is used in Section 4.2 for transforming a semi-partial linear secret sharing scheme into a perfect one without changing its convec. The second lemma is needed to handle the partial case, which is discussed in Section 4.3.

### 4.1 Two linear algebraic lemmas

Let $\mathbb{F}$ be a finite field and $x_1, \ldots, x_\lambda \in \mathbb{F}^m$ be linearly independent row vectors. The following lemma essentially states that there exists $m \times \lambda m$ matrices $L_1, \ldots, L_m$ such that the collection $\{x_i L_j : i \in [\lambda], j \in [m]\}$ of vectors in $\mathbb{F}^{\lambda m}$ are linearly independent.

We remark that the lemma does not hold in general if the base field is not finite. So the claim is truly a property of finite fields.

**Lemma 4.1 (Linear transformation lemma)** *Let $1 \leqslant \lambda \leqslant m$ be integers. Let $T_0$ be a vector space over some finite field with dimension $m$. Then, there exist $m$ linear maps $L_1, \ldots, L_m : T_0 \to T_0^\lambda$ such that for any subspace $E \subseteq T_0$ of dimension $\dim E \geqslant \lambda$, the following holds*

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

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

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

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

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

When turning a partial linear scheme into a perfect one, as we will see, the above lemma is needed to argue about the correctness of constructed scheme. To argue about its privacy, we need the following lemma. The second lemma is true for finite fields that are sufficiently large and, unlike the first lemma, it holds for infinite fields.

**Lemma 4.2 (Non-intersecting subspace lemma)** *Let $T_0$ be a vector space of dimension $m$ over a finite field with $q$ elements and let $E_1, \ldots, E_N$ be subspaces of $T_0$ of dimension at most $\omega$, $1 \leqslant \omega < m$. If $N < \frac{q^m - 1}{q^{m-1} - 1}$, then there is a subspace $S \subset T_0$ of dimension $m - \omega$ such that $S \cap E_i = 0$, for every $i \in [N]$.*

*Proof.* Without loss of generality we can assume that $\dim E_i = \omega$. Let $\mathbb{F}$ be the underlying finite field with $q$ elements. We show that if $N < \frac{q^m - 1}{q^{m-1} - 1}$, then

the required subspace $S$ of dimension $m-w$ with zero intersection with $E_i$'s exists. We prove this by induction on $m-w$. If $m-w=1$, then each $E_i$ has $q^{m-1}-1$ non-zero elements so we have at most $N(q^{m-1}-1)$ non-zero elements in their union. If $N < \frac{q^m-1}{q^{m-1}-1}$ then there is a non-zero element outside this union that generates the required subspace $S$. If $E_i$'s are of dimension $w$, then since $N < \frac{q^m-1}{q^w-1}$ the above proof shows that there is a non-zero vector $u$ outside their union. If we add this vector to each $E_i$ we get subspace $E_i'$ of dimension $w+1$. Therefore, by induction, we have a subspace $S'$ of dimension $m-w-1$ that has zero intersection with each $E_i'$. Now the space generated by $S$ and $u$ is the required subspace of dimension $m-w$ and zero intersection with each $E_i$. □

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

The following proposition will be generalized in next subsection. However, we present it separately in this subsection since we will build on its proof in the course of the proof of Proposition 4.4. We recall that the usual and partial convecs of a secret sharing scheme $\Pi$ are denoted by $\mathrm{cv}(\Pi)$ and $\mathrm{pcv}(\Pi)$, respectively; see Definitions 2.6 and 3.2.

**Proposition 4.3 (Semi-partial $\Longrightarrow$ Perfect)** *Let $\Gamma$ be an access structure and $\Pi'$ be a semi-partial $\mathbb{F}$-linear secret sharing scheme for it. Then, there exists a perfect $\mathbb{F}$-linear secret sharing scheme $\Pi$ for $\Gamma$ such that $\mathrm{cv}(\Pi) = \mathrm{pcv}(\Pi')$. Consequently, for every access structure, the semi-partial and perfect information ratios are the same if we restrict ourselves to the class of linear schemes.*

**Construction.** Here is how we construct $\Pi$ from $\Pi'$. Identify the secret space of $\Pi'$ by $\mathbb{F}^m$. Since $\Pi'$ is a semi-partial scheme for $\Gamma$, there exists an integer $\lambda$, with $1 \leqslant \lambda \leqslant m$, such that every qualified participant set discovers at least $\lambda$ independent linear relations on the secret, and there exists a qualified set that recovers exactly $\lambda$ such relations. Recall that the case of $\lambda = 1$ was described in the introduction (Section 1.5). In this case, the secret space of the constructed scheme $\Pi$ was $\mathbb{F}^m$ too. For the general case, we let the secret space of $\Pi$ to be $\mathbb{F}^{\lambda m}$. Simply represent the linear maps in Lemma 4.1 by be $m \times \lambda m$ matrices $L_1, \ldots, L_m$. To share a secret $s \in \mathbb{F}^{\lambda m}$, viewed as a column vector, we share each of the $m$ secrets $L_1 s, \ldots, L_m s \in \mathbb{F}^m$ using an independent instance of $\Pi'$. Each participant in $\Pi$ receives a share from each instance of $\Pi'$. Hence, while the secret length has been multiplied by $\lambda$, the share of each participant has increased by a factor of $m$. Therefore, the usual convec of $\Pi$ and partial convec of $\Pi'$ are equal. Note that since the $m$ different instances of $\Pi'$ use independent randomnesses, the secret remains hidden from every unqualified set. By Lemma 4.1, each qualified set gets $\lambda m$ independent linear relations on $s$. We conclude that the scheme $\Pi$ is perfect.

In the following, we prove Proposition 4.3 more formally.

*Proof (of Proposition 4.3).* Let $\Pi' = (T'; T'_0, T'_1, \ldots, T'_n)$ be the $\mathbb{F}$-linear semi-partial scheme that satisfies $\lambda = \min_{A \in \Gamma}\{\dim(T'_A \cap T'_0)\} \geqslant 1$ and $\dim(T'_A \cap T'_0) = 0$ for all $A \in \Gamma^c$. Let $m = \dim(T'_0) \geqslant 1$.

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

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

Let $L_1, \ldots, L_m : T'_0 \to {T'}_0^{\lambda}$ be the linear maps of Lemma 4.1 and define $\phi : {T'}^m \to T$ by

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

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

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

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

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

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

If $A \in \Gamma$, then $\dim(T'_A \cap T'_0) \geqslant \lambda$. Therefore, by Lemma 4.1, we have $T_A \cap T_0 = T_0$. Also, if $B \in \Gamma^c$, then $T'_B \cap T'_0 = 0$ and hence $T_B \cap T_0 = 0$. This shows that $\Pi$ is a perfect scheme for $\Gamma$. □

### 4.3 A convec-preserving perfect linear scheme from a partial linear one

The following proposition is a generalization of Proposition 4.3. The proof essentially follows the same lines as that of Proposition 4.3. We will need Lemma 4.2 for arguing about the privacy of constructed scheme, which is "almost" the same as previous one. The difference is due to the the fact that Lemma 4.2 is true for sufficiently large finite fields; therefore, we first need to "lift" the scheme into a larger field and then apply construction of Section 4.2.

**Proposition 4.4 (Partial $\Longrightarrow$ Perfect)** *Let $\Gamma$ be an access structure and $\Pi'$ be a partial $\mathbb{F}$-linear secret sharing scheme for it. Then, there exists a finite extension $\mathbb{K}$ of $\mathbb{F}$ and a perfect $\mathbb{K}$-linear secret sharing scheme $\Pi$ for $\Gamma$ such that $\mathrm{cv}(\Pi) = \mathrm{pcv}(\Pi')$. Consequently, for every access structure, the partial and perfect information ratios are the same if we restrict ourselves to the class of linear schemes.*

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

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

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

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

Construct $(T_0, \ldots, T_n)$ from $\Pi'$ the same way as in the proof of Proposition 4.3 and recall that $\dim T_0 = \lambda m$ and $\dim T_i \leqslant m \dim T'_i$. The same argument, which was used in the proof of Proposition 4.3, shows that for any $A \in \Gamma$, we have $T_A \cap T_0 = T_0$. It is also trivial that for every $B \in \Gamma$, we have $\dim\big(T_B \cap T_0\big) \leqslant m\omega$.

By Lemma 4.2 ($E_i$ is $T_B \cap T_0$ for some maximal unqualified set $B$, $\dim E_i \leqslant m\omega$ and $\dim T_0 = \lambda m$), one can choose $S \subseteq T_0$ of dimension $(\lambda - \omega)m$ such that $T_B \cap S = 0$, for every $B \in \Gamma^c$. Also, it is trivial that $T_A \cap S = S$, for every $A \in \Gamma$. Now, it is clear that $\Pi = (S, T_1, \ldots, T_n)$ is a perfect secret sharing scheme for $\Gamma$ such that $\dim S = (\lambda - \omega)m$. Therefore, $\mathrm{cv}(\Pi) \preceq \mathrm{pcv}(\Pi')$. Again, it is straightforward to tweak the scheme such that the convec equality holds. □

## 5 Separating perfect and partial mixed-linear information ratios

Equality of perfect and partial linear information ratios was proved in Section 4. In this section, we show that for the $\mathcal{F} + \mathcal{N}$ access structure, introduced in [5], the mixed-linear information ratios do not match.

### 5.1 Mixed-linear schemes

The class of mixed-linear secret sharing schemes has been recently introduced in [23] and it has been proved that they are superior to linear ones. Mixed-linear schemes are a subclass of homomorphic schemes and it is an open problem if homomorphic schemes can outperform mixed-linear ones [23, Problem 6.4].

Informally, a mixed-linear scheme is constructed by combining different linear schemes with possibly different underlying finite fields. Here is a formal definition.

**Definition 5.1** *Mixed-linear schemes are recursively defined as follows. A linear scheme is mixed-linear. If $\Pi = (\boldsymbol{S}_i)_{i \in P \cup \{0\}}$ and $\Pi' = (\boldsymbol{S}'_i)_{i \in P \cup \{0\}}$ are mixed-linear schemes, their mix, defined and denoted by $\Pi \oplus \Pi' = (\boldsymbol{S}''_i)_{i \in P \cup \{0\}}$, is also mixed-linear, where $\boldsymbol{S}''_i = (\boldsymbol{S}_i, \boldsymbol{S}'_i)$.*

Informally, to share a secret $(s, s')$ using $\Pi \oplus \Pi'$, where $s$ and $s'$ are in the secret spaces of $\Pi$ and $\Pi'$, respectively, we independently share $s$ using $\Pi$ and $s'$ using $\Pi'$. Hence, each participant in $\Pi \oplus \Pi'$ receives a share form $\Pi$ and one form $\Pi'$.

### 5.2 The access structure $\mathcal{F} + \mathcal{N}$

We study $\mathcal{F} + \mathcal{N}$, a well-known 12-participant access structure [5, page 2641] which has both Fano ($\mathcal{F}$) and non-Fano ($\mathcal{N}$) access structures as minors. Both $\mathcal{F}$ and $\mathcal{N}$ have six participants with the following minimal qualified sets:

$$\begin{aligned}
\mathcal{F}: &\ \{p_1,p_4\},\{p_2,p_5\},\{p_3,p_6\},\\
&\ \{p_1,p_2,p_3\},\{p_1,p_5,p_6\},\{p_2,p_4,p_6\},\{p_3,p_4,p_5\},\\
\mathcal{N}: &\ \{p_1,p_4\},\{p_2,p_5\},\{p_3,p_6\},\\
&\ \{p_1,p_2,p_3\},\{p_1,p_5,p_6\},\{p_2,p_4,p_6\},\{p_3,p_4,p_5\},\{p_4,p_5,p_6\}.
\end{aligned}$$

The access structure $\mathcal{F}$ (resp. $\mathcal{N}$) is the port of Fano (resp. non-Fano) matroid and it is known [32] to be ideal only on finite fields with even (resp. odd) characteristic. Recall that a secret sharing scheme is called ideal if the share size of every participant is the same as the secret size and an access structure is called ideal if it admits an ideal (perfect) scheme. Consider the following ideal linear secret sharing scheme:

$$\begin{array}{ll}
p_1 : r_1 & p_4 : r_1 + s\\
p_2 : r_2 & p_5 : r_2 + s\\
p_3 : r_1 + r_2 + s & p_6 : r_1 + r_2
\end{array}$$

where $s, r_1, r_2$ are all uniformly and indecently chosen from a finite field $\mathbb{F}_q$ of order $q$. It is easy to check that if $q$ is a power of two, the scheme realizes $\mathcal{F}$ and if $q$ is an odd prime-power, the scheme realizes $\mathcal{N}$.

The access structure $\mathcal{F} + \mathcal{N}$, with 12 participants, is the union of $\mathcal{F}$ and $\mathcal{N}$ (the parties in $\mathcal{N}$ are renamed form $p_1, \ldots, p_6$ to $p_7, \ldots, p_{12}$ respectively). It is known that $\mathcal{F}+\mathcal{N}$ is not ideal but its information ratio is one; hence, it is called *nearly-ideal* [5]. Recently, in [23], the exact value of its linear information ratio has been determined (max= 4/3 and average= 41/36). Also, its mixed-linear information ratio has been determined exactly (max= 7/6 and average= 41/36), proving that mixed-linear schemes are superior to the linear ones.

Below, we construct a family of semi-partial mixed-linear scheme for this access structure with partial information ratio one. Table 1 summarizes the known results about the $\mathcal{F} + \mathcal{N}$ access structure. For completeness, we also include the result for other security notions that will be discussed in Section 6.

### 5.3 A nearly-ideal semi-partial mixed-linear scheme for $\mathcal{F} + \mathcal{N}$

Let $k$ be a positive integer and let $2^k + 1 = q_1 \times \cdots \times q_\ell$, where $q_i$'s are pairwise co-prime prime-powers. We construct a family of semi-partial schemes for $\mathcal{F}+\mathcal{N}$ whose information ratio approaches to one when $k \to \infty$.

The secret space of the $k$th scheme is $\mathbb{F}_{2^k} \times \mathbb{F}_{q_1} \times \cdots \times \mathbb{F}_{q_\ell}$. We share a secret $(s', s_1, \cdots, s_\ell)$, where $s' \in \mathbb{F}_{2^k}$ and $s_i \in \mathbb{F}_{q_i}$, as follows. We share $s'$ using the ideal linear scheme for Fano such that each participant in the set $\{p_1, \ldots, p_6\}$ receives a share. For each $i = 1, \ldots, \ell$, we share $s_i$ using the ideal linear scheme for non-Fano such that each participant in the set $\{p_7, \ldots, p_{12}\}$ receives a share for each $i$. Clearly, all participants $p_1, \ldots, p_6$ recover $s'$ and gain no information about $(s_1, \cdots, s_\ell)$. Similarly, all participants $p_7, \ldots, p_{12}$ recover $(s_1, \cdots, s_\ell)$ and gain no information about $s'$. Therefore, the scheme is semi-partial with advantage $\delta = \frac{\log 2^k}{\log 2^k + \log(2^k+1)}$. The partial information ratios of participants $p_1, \ldots, p_6$ are all one and those of participants $p_7, \ldots, p_{12}$ are all $\frac{\log(2^k+1)}{\log 2^k}$. That is, the $k$th scheme is semi-partial for $\mathcal{F} + \mathcal{N}$ and its partial information ratio approaches to one when $k \to \infty$.

| | | (almost/stat.-) perfect | quasi-perfect | (semi-) partial | reference |
|---|---|---|---|---|---|
| general | max | 1 | | | [5] |
| | average | | | | |
| mixed-linear | max | 7/6 | $1 \leqslant \cdot \leqslant 7/6$ | 1 | [23] & Sections 5.3 & 6.4 |
| | average | 41/36 | $1 \leqslant \cdot \leqslant 41/36$ | | |
| linear | max | 4/3 | | | [23] & Section 4 |
| | average | 41/36 | | | |

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

## 6 Relations between non-perfect secret sharing schemes

In this section, we will first provide a formal definition of the following relaxations of perfect security for secret sharing schemes: statistically-perfect [4, 6], almost-perfect [13] and quasi-perfect [26, Chapater 5]. Then, we will show that the following relation holds for the information ratios of an access structure with respect to different security notions:

$$\text{partial} \leqslant \text{quasi-perfect} \leqslant \text{almost-perfect} \leqslant \text{statistically-perfect} \leqslant \text{perfect}$$

Counting from left to right, the second and last inequalities follow by definition, straightforwardly. We will prove the first and third inequalities in Sections 6.2 and 6.3, respectively. Additionally, in Section 6.4, we present a class of schemes for which almost-perfect (and consequently statistically-perfect) security notions coincide with perfect security.

### 6.1 Definitions

Perfect and partial security notions are defined for a single secret sharing scheme. The security notions that we study in this subsection are defined with respect to a family of schemes. To this end, we need the following definition.

**Definition 6.1 (Convec-converging family of schemes)** *A sequence $\mathcal{F} = \{\Pi_k\}_{k\in\mathbb{N}}$ of secret sharing schemes, all defined on the same set of participants, is called a* convec-converging family of schemes *if:*

1. *The entropy of secret does not vanish; i.e.,* $\mathrm{H}(\boldsymbol{S}_0^k) = \Omega(1)$.
2. *The secret length grows at most polynomially in $k$; that is,* $\log_2 |\mathrm{supp}(\boldsymbol{S}_0^k)| = \mathrm{O}(k^c)$ *for some $c > 0$.*
3. *The sequence $\{\mathrm{cv}(\Pi_k)\}_{k\in\mathbb{N}}$ is converging.*

*We refer to the vector $\lim_{k\to\infty} \mathrm{cv}(\Pi_k)$ as the convec of $\mathcal{F}$. The information ratio of $\mathcal{F}$ is defined to be the maximum coordinate of its convec.*

We need the first two requirements for technical reasons (e.g., see Lemma 6.8).

**Almost-perfect secret sharing.** In [13], Csirmaz defines almost-perfect security in terms of *almost-entropic polymatroids* [27], below we present an equivalent definition in terms of secret sharing schemes. In a perfect scheme $\Pi = (\boldsymbol{S}_i)_{i\in P\cup\{0\}}$, the amount of information on the secret that is missed by a qualified set $A \subseteq P$ (i.e., $\mathrm{H}(\boldsymbol{S}_0|\boldsymbol{S}_A)$) or leaked to an unqualified set $A \subseteq P$ (i.e., $\mathrm{I}(\boldsymbol{S}_0 : \boldsymbol{S}_A)$) are both zero. Almost-perfect security relaxes this requirements by allowing these values to be *tiny*, where a function $\varepsilon : \mathbb{N} \to \mathbb{R}^+$ is called tiny if $\varepsilon(k) = \mathrm{o}(1)$.

**Definition 6.2 (Almost-perfect realization [13])** *Let $\Gamma$ be an access structure on participants set $P$ and $\mathcal{F} = \{\Pi_k\}_{k\in\mathbb{N}}$ be a convec-converging family of secret sharing schemes and denote $\Pi_k = (\boldsymbol{S}_i^k)_{i\in P\cup\{0\}}$. We say that $\mathcal{F}$ is an almost-perfect family for $\Gamma$ if:*

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

**Quasi-perfect secret sharing.** In almost-perfect security, the information miss/leak to qualified/unqualified sets are required to be tiny. In quasi-perfect secret sharing, this requirements are more relaxed since the fraction of information miss/leak is taken into account. For example, if the secret is $k$-bit-long, quasi-perfect security allows the qualified/unqualified sets to miss/gain one bit of information about the secret; because the fraction of missed/gained information is $\frac{1}{k}$, which is tiny. But, this is not acceptable in an almost-perfect secret sharing scheme.

**Definition 6.3 (Quasi-perfect realization [25])** *Let $\Gamma, \mathcal{F}$ and $\boldsymbol{S}_i^k$'s be as before. We say that $\mathcal{F}$ is a quasi-perfect family for $\Gamma$ if:*

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

**Statistically-perfect secret sharing.** In almost-perfect security, if the secret is $k$-bit-long, it is acceptable if the qualified sets fail to recover the secret with probability $\frac{1}{k}$, because the amount of information which is missed is $\mathrm{O}(\frac{1}{k})$, which is tiny. In statistically-perfect secret sharing, we require that the qualified sets fail to recover the secret with at most a *negligible* probability of error. Here, a function $\varepsilon : \mathbb{N} \to \mathbb{R}$ is called negligible if $\varepsilon(k) = k^{-\omega(1)}$; that is, it approaches to zero faster than the inverse of any polynomial. Similarly, for privacy of statistically-secure secret sharing schemes, we require a stronger requirement which is specified in terms of "statistical distance" between distributions of the shares that correspond to two secrets. We first define the notion of statistical distance and then formally define the statistical-security notion.

**Definition 6.4 (Statistical distance)** *The* statistical distance *between two random variables $\boldsymbol{X}_0$ and $\boldsymbol{X}_1$ is defined by*

$$\mathrm{SD}(\boldsymbol{X}_0, \boldsymbol{X}_1) = \frac{1}{2} \sum_x |\Pr[\boldsymbol{X}_0 = x] - \Pr[\boldsymbol{X}_1 = x]| \ .$$

**Definition 6.5 (Statistical realization)** *Let $\Gamma, \mathcal{F}$ and $\boldsymbol{S}_i^k$'s be as before. We say that $\mathcal{F}$ is a statistically-perfect family for $\Gamma$, or $\mathcal{F}$ realizes $\Gamma$ statistically, if:*

- *For every qualified set $A \in \Gamma$ there exists a reconstruction function $\textsc{Recon}_A : \mathrm{supp}(\boldsymbol{S}_A^k) \to \mathrm{supp}(\boldsymbol{S}_0^k)$, such that for every secret $s \in \mathrm{supp}(\boldsymbol{S}_0^k)$, the error probability $\Pr[\textsc{Recon}_A(\boldsymbol{S}_A^k) \neq s | \boldsymbol{S}_0^k = s]$ is negligible in $k$.*
- *For every unqualified set $A \in \Gamma$, and every pair of secrets $s_1, s_2 \in \mathrm{supp}(\boldsymbol{S}_0^k)$, the statistical distance between the random variable $\boldsymbol{S}_A^k$ conditioned on the event $\boldsymbol{S}_0^k = s_1$ and the random variable $\boldsymbol{S}_A^k$ conditioned on the event $\boldsymbol{S}_0^k = s_2$ is negligible in $k$.*

**Non-perfect information ratios.** For each security notion, a corresponding information ratio can be associated to every access structure. For example, the almost-perfect information ratio of an access structure is the infimum of all information ratios of all convec-converging families of secret sharing schemes that almost-perfectly realize it. The quasi-perfect and statistically-perfect information ratios are defined similarly.

### 6.2 Partial $\leqslant$ Quasi-perfect

We want to show that partial information ratio of an access structure $\Gamma$ is not larger than its quasi-perfect information ratio. To prove this claim, let $\{\Pi_k\}_{k\in\mathbb{N}}$ be a convec-converging family of secret sharing schemes that quasi-perfectly realizes $\Gamma$. We show that $\{\Pi_k\}_{k\in\mathbb{N}}$ is also a family of partial secret sharing schemes for $\Gamma$ such that

$$\lim_{k\to\infty} \mathrm{pcv}(\Pi_k) = \lim_{k\to\infty} \mathrm{cv}(\Pi_k) \ ,$$

where $\mathrm{cv}(\Pi)$ and $\mathrm{pcv}(\Pi)$ stand for the usual and partial convecs of a secret sharing scheme $\Pi$, as defined in Definitions 2.6 and 3.2, respectively.

Recall the definition of access function of a secret sharing scheme (Definition 2.5) and let

- $\lambda_k = \min_{A\in\Gamma}\{\Phi_{\Pi_k}(A)\}$ and,
- $\omega_k = \max_{B\notin\Gamma}\{\Phi_{\Pi_k}(B)\}$.

Since $\{\Pi_k\}_{k\in\mathbb{N}}$ quasi-perfectly realizes $\Gamma$, the sequences $\{\lambda_k\}$ and $\{\omega_k\}$ respectively converge to 1 and 0. Therefore, we have $\delta_k = \lambda_k - \omega_k > 0$ for sufficiently large $k$. This shows that $\Pi_k$ is a partial secret sharing scheme for $\Gamma$ with partial convec $\mathrm{pcv}(\Pi_k) = \mathrm{cv}(\Pi_k)/\delta_k$. The claim then follows since $\delta_k \to 1$ as $k \to \infty$.

### 6.3 Almost-perfect $\leqslant$ Statistically-perfect

We want to show that the almost-perfect information ratio of an access structure is not larger than its statistically-perfect information ratio. We show that if a family of schemes realizes an access structure statistically, so does it almost-perfectly, proving the claim. Let us first provide two definitions which simplify our notations.

**Definition 6.6 (Maximum Reconstruction Error)** *Let $(\boldsymbol{X},\boldsymbol{Y})$ be jointly distributed random variables. The* Maximum Reconstruction Error (MRE) *of $\boldsymbol{X}$ from $\boldsymbol{Y}$ is defined as below, where* max *is taken over all $x \in \mathrm{supp}(\boldsymbol{X})$ and* min *is taken over all reconstruction functions* $\textsc{Recon} : \mathrm{supp}(\boldsymbol{Y}) \to \mathrm{supp}(\boldsymbol{X})$*,*

$$\mathrm{MRE}(\boldsymbol{X}|\boldsymbol{Y}) = \min_{\textsc{Recon}} \max_{x} \Pr[\textsc{Recon}(\boldsymbol{Y}) \neq x | \boldsymbol{X} = x] \ .$$

**Definition 6.7 (Maximum Conditional Statistical Distance)** *Let $(\boldsymbol{X},\boldsymbol{Y})$ be jointly distributed random variables. The* Maximum Conditional Statistical Distance (MCSD) *of $\boldsymbol{Y}$ with respect to $\boldsymbol{X}$ is defined as follows, where* max *is taken over all pairs $x_0, x_1 \in \mathrm{supp}(\boldsymbol{X})$,*

$$\mathrm{MCSD}(\boldsymbol{Y}|\boldsymbol{X}) = \max_{x_0,x_1} \mathrm{SD}(\boldsymbol{Y}|\{\boldsymbol{X}=x_0\}, \boldsymbol{Y}|\{\boldsymbol{X}=x_1\}] \ .$$

Given above definitions, the correctness and privacy requirements in the definition of statistical secret sharing (Definition 6.5) can be restated as follows:

- For every qualified set $A \in \Gamma$, $\mathrm{MRE}(\boldsymbol{S}_0^k|\boldsymbol{S}_A^k)$ is negligible in $k$,
- For every unqualified set $A \in \Gamma$, $\mathrm{MCSD}(\boldsymbol{S}_A^k|\boldsymbol{S}_0^k)$ is negligible in $k$.

Our claim then easily follows by the following lemma, by letting $\boldsymbol{X}_k = \boldsymbol{S}_0^k$ and $\boldsymbol{Y}_k = \boldsymbol{S}_A^k$.

**Lemma 6.8** *Let $\{(\boldsymbol{X}_k,\boldsymbol{Y}_k)\}_{k\in\mathbb{N}}$ be a family of jointly distributed random variables and assume that $\log|\mathrm{supp}(\boldsymbol{X}_k)|$ is polynomial in $k$. Then:*

*(i) If $\mathrm{MRE}(\boldsymbol{X}_k|\boldsymbol{Y}_k)$ is negligible in $k$, then $\lim_{k\to\infty} \mathrm{H}(\boldsymbol{X}_k|\boldsymbol{Y}_k) = 0$.*

*(ii) If* $\mathrm{MCSD}(\boldsymbol{Y}_k|\boldsymbol{X}_k)$ *is negligible in* $k$*, then* $\lim_{k\to\infty} \mathrm{I}(\boldsymbol{X}_k : \boldsymbol{Y}_k) = 0$.

*Proof.* Part (i) follows by Fano's inequality [12] which is stated as follows. Suppose that we wish to estimate the random variable $\boldsymbol{X}$, with support $\mathcal{X}$, by an estimator $\boldsymbol{Y}$, and furthermore, assume that $\epsilon = \Pr[\boldsymbol{X} \neq \boldsymbol{Y}]$. Then, $\mathrm{H}(\boldsymbol{X}|\boldsymbol{Y}) \leqslant \mathrm{H}(\epsilon) + \epsilon \log(|\mathcal{X}| - 1)$, where $\mathrm{H}(\epsilon)$ is the entropy of a Bernoulli random variable with parameter $\epsilon$. Denote $n(k) = |\mathrm{supp}(\boldsymbol{X}_k)|$ and $\epsilon(k) = \mathrm{MRE}(\boldsymbol{Y}_k|\boldsymbol{X}_k)$. By Fano's inequality and definition of MRE, we have $\mathrm{H}(\boldsymbol{X}_k \mid \boldsymbol{Y}_k) \leqslant \mathrm{H}(\epsilon(k)) + \epsilon(k) \log(n(k) - 1)$. This proves that $\lim_{k\to\infty} \mathrm{H}(\boldsymbol{X}_k \mid \boldsymbol{Y}_k) = 0$ since $\log n(k)$ is polynomial and $\epsilon(k)$ is negligible. Part (ii) has been implicitly proved in [33]. □

### 6.4 Almost-perfect ≡ Perfect (for a large class)

In this subsection, we show that almost-perfect (and consequently statistically-perfect) security notion coincide with perfect security for a large class of secret sharing schemes. The class that we find is a subclass of the so-called *group-characterizable* secret sharing schemes which turns out to contain homomorphic secret sharing schemes. This coincidence was already known to hold for class of linear schemes [4]. By [23], homomorphic schemes are known to be better than linear schemes in terms of information ratio; therefore, our extension indeed results into a larger class.

The notion of *group-characterizable random variables* was introduced by Chan and Yeung in [11]. Here, we tailor the definition for secret sharing schemes. We refer the reader to Appendix A for basics of group theory.

**Definition 6.9 (Group-characterizable secret sharing scheme)** *A tuple* $\Pi = [G : G_0, G_1, \ldots, G_n]$ *is called a group-characterizable secret sharing scheme if* $(G, *)$ *is a finite group and* $G_i$*'s are subgroups of* $G$ *with* $|G|/|G_0| \geqslant 2$.

A group-characterizable scheme $\Pi = [G : G_0, G_1, \ldots, G_n]$ induces a random variable $(\boldsymbol{S}_0, \boldsymbol{S}_1, \ldots, \boldsymbol{S}_n)$ as follows. Let $\boldsymbol{g}$ be a uniform random variable on $G$ and let $\boldsymbol{S}_i = \boldsymbol{g}G_i$; that is, the support of $\boldsymbol{S}_i$ is the left cosets of $G_i$. Clearly, $\mathrm{H}(\boldsymbol{S}_i) = \log \frac{|G|}{|G_i|}$. More generally, one can show that $\mathrm{H}(\boldsymbol{S}_A) = \log \frac{|G|}{|G_A|}$ for every subset $A \subseteq \{0, 1, \ldots, n\}$, where

$$G_A = \bigcap_{i \in A} G_i \ .$$

The following relations then easily follow:

$$\mathrm{H}(\boldsymbol{S}_A|\boldsymbol{S}_B) = \log \frac{|G_B|}{|G_{A\cap B}|} \ , \qquad \mathrm{I}(\boldsymbol{S}_A : \boldsymbol{S}_B) = \log \frac{|G|}{|G_A * G_B|} \ , \tag{6.1}$$

where the relation for mutual information is achieved by taking the relation $|G_A * G_B| = \frac{|G_A| \cdot |G_B|}{|G_A \cap G_B|}$ for subgroup product into account, where $G_A * G_B = \{a * b \mid a \in G_A, b \in G_A\}$.

In the following we show that for a subclass of group-characterizable secret sharing with $G_0 \trianglelefteq G$, i.e., the secret subgroup $G_0$ is normal in the main group $G$, the *almost-perfect*, *statistically-perfect* and *perfect* security notions all coincide.

**Theorem 6.10 ($G_0 \trianglelefteq G$)** *Let $\{\Pi_k\}_{k\in\mathbb{N}}$, where $\Pi_k = [G^k : G_0^k, G_1^k, \ldots, G_n^k]$, be a convec-converging family of group-characterizable secret sharing schemes such that $G_0^k \trianglelefteq G^k$ for each $k \in \mathbb{N}$. If $\{\Pi_k\}_{k\in\mathbb{N}}$ almost-perfectly realizes an access structure, then for every sufficiently large $k$, $\Pi_k$ perfectly realizes it.*

*Proof.* The proof follows by the following observation. Let $\Pi = (\boldsymbol{S}_0, \boldsymbol{S}_1, \ldots, \boldsymbol{S}_n)$ 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 $\mathrm{H}(\boldsymbol{S}_A|\boldsymbol{S}_B) > 0$, 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, $\mathrm{I}(\boldsymbol{S}_A : \boldsymbol{S}_B)$ 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 $k$, $\Pi_k$ must be a perfect scheme for it. □

**Technical discussion.** As we discussed in the proof, our argument does not go through for the (general) class of group-characterizable schemes. In general, one can construct an example where the ratio $|G|/|G_A * G_B|$ 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 $G_A$ and $G_B$ to be the subgroups of order $p$ generated by $a$ and $bab^{-1}$, respectively, then $G_A * G_B$ 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). Finally, even if the two notions might not coincide for this class of schemes, their corresponding information ratios might still coincide. Both problems remain open.

**How large is the found class.** Group-characterizable secret sharing schemes cover a large class of non-linear secret sharing schemes. It is large enough to be "complete" for quasi-perfect secret sharing. That is, the quasi-perfect information ratio of an access structure 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 [11, Theorem 4.1]. We provide a poof of this statement in Appendix B. Nevertheless, it is an open problem if group-characterizable secret sharing schemes are complete for other security notions, and in particular, for perfect security.

Well-known classes of secret sharing schemes such as linear, mixed-linear and abelian ones can be equivalently defined in terms of group-characterizable secret sharing schemes (e.g., see [23]). In a recent work [24], it has been proved that group-characterizable secret sharing schemes whose all subgroups are normal in the main group (i.e., $G_i \trianglelefteq G$ for every $i \in \{0, 1, \ldots, n\}$) are equivalent to homomorphic secret sharing schemes. Therefore, the class found in Theorem 6.10 contains at least the homomorphic schemes (which is known to be a proper superset of linear schemes [23]), but we conjecture to be much larger.

## 7 On decomposition techniques

Decomposition techniques are useful to construct secret sharing schemes for a given access structure by combining several (usually simple) secret sharing schemes. For example, the optimal linear schemes for several graph access structures on six participants, which had remained open for a long time, were constructed using these methods in [18].

Decomposition techniques have two flavors. Weighted decompositions [18,36] allow non-perfect sub-schemes but they need to be linear. In fact, the constructions in [18, 36] need the linear sub-schemes to satisfy some additional requirement but, in Section 7.1, we will show that it can be removed. Non-weighted-decompositions [15,35] allow non-linear sub-schemes but they need to be perfect.

In Section 7.2, we present a unified decomposition theorem, that we refer to as the $\delta$-decomposition, which captures the weighted and non-weighted decompositions at one place. The theorem is essentially a restatement of known and folklore results, but it is presented for the following reasons:

1. to see how the partial secret sharing schemes and decomposition methods are entangled together,
2. to provide the intuition behind the scale factor $\frac{1}{\delta}$ in definition of partial convec (Definition 3.2).

### 7.1 Weighted-$(\lambda, \omega)$-decomposition revisited

The following definition is a restatement of Definition 3.4 in [18].

**Definition 7.1 ($(\lambda, \omega)$–weighted decomposition)** *Let $\lambda, \omega, N, m_1, \cdots, m_N$, be non-negative integers, with $0 \leqslant \omega < \lambda$. Let $\Gamma$ be an access structure and $\Phi_1, \ldots, \Phi_N$ be (rational-valued) access functions all defined on the same participants set and further assume that $m_j\Phi_j$ is an integer-valued function for every $j \in [N]$. We call $(m_1, \Phi_1), \ldots, (m_N, \Phi_N)$ a weighted-$(\lambda, \omega)$-decomposition for $\Gamma$ if the following two hold:*

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

The weighted-$(\lambda,\omega)$-decomposition theorem of [18, Theorem 3.2] (as well as its predecessor [36]) has the following limitation. They require that in the linear sub-schemes every subset of participants fully recovers a certain subset of the secret elements and nothing more; in other words, recovering a linear combination such as $s_1+s_3+s_7$ of the secret elements is allowed only if $s_1, s_3, s_7$ are all recovered. The proof in this case is easily handled using a ramp secret sharing. In the following theorem, we remove this strong requirement. Its proof uses the notion of partial secret sharing and the result of Section 4 on the equality of partial and perfect linear information ratios.

**Theorem 7.2 (Strong $(\boldsymbol{\lambda},\boldsymbol{\omega})$–weighted theorem)** *Let $\Gamma$ be an access structure and $(m_1,\Phi_1),\ldots,(m_N,\Phi_N)$ be a weighted-$(\lambda,\omega)$-decomposition for it. If for each $j\in[N]$, the access function $\Phi_j$ has a linear secret sharing scheme with convec $\sigma_j$, such that their field characteristics are all the same, then $\Gamma$ has a linear secret sharing with convec $\frac{1}{\lambda-\omega}\sum_{j=1}^{N} m_j\sigma_j$.*

*Proof.* Let $\Pi_j = (T_{ij})_{i\in P\cup\{0\}}$ be a linear secret sharing scheme for $\Phi_j$ with convec $\sigma_j$, for $j\in[N]$. Without loss of generality, we assume that all schemes are $\mathbb{F}$-linear for a common finite field $\mathbb{F}$ (due to the common characteristic). Let $T'_i=\oplus_{j\in[N]}T_{ij}$ and denote $\Pi'=(T'_i)_{i\in P\cup\{0\}}$. We have $\dim T'_i=\sum_{j\in[N]}\dim T_{ij}$ which implies that

$$\dim T'_i=\textstyle\sum_{j=1}^{N} m_j\sigma_j\ .$$

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

$$\begin{aligned}\dim(T'_A\cap T'_0)&=\textstyle\sum_{j\in[N]}\dim(T_A\cap T_0)\\&=\textstyle\sum_{j\in[N]} m_j\Phi_{\Pi_j}(A)\\&=\textstyle\sum_{j\in[N]} m_j\Phi_j(A)\ .\end{aligned}$$

By definition of the $(\lambda,\omega)$–weighted decomposition, we have

$$\Delta=\min_{A\in\Gamma}\dim(T'_A\cap T'_0)-\max_{B\in\Gamma^c}\dim(T'_B\cap T'_0)\geqslant\lambda-\omega\ .$$

Consequently, $\Pi'$ is an $\mathbb{F}$-linear partial secret sharing scheme for $\Gamma$ with the following partial convec:

$$\mathrm{pcv}(\Pi')=\frac{1}{\Delta}\sum_{j=1}^{N} m_j\sigma_j\ .$$

Then, by Proposition 4.4, there exists a finite extension $\mathbb{K}$ of $\mathbb{F}$, such that $\Gamma$ has a perfect $\mathbb{K}$-linear scheme $\Pi$ with the above convec. It is straightforward to modify the scheme, by adding dummy shares, to have a scheme with convec $\frac{1}{\lambda-\omega}\sum_{j=1}^{N} m_j\sigma_j$. □

### 7.2 $\delta$-decomposition

We present the notion of $\delta$-decomposition, which captures all the weighted and non-weighted decompositions [15,18,35,36], simultaneously (even in a more general form since we allow the coefficients to be real numbers). The resemblance between definition of partial security (Definition 3.1) and $\delta$-decomposition is apparent in the following definition.

**Definition 7.3 ($\delta$-decomposition)** *Let $N$ be an integer and $h_1, \ldots, h_N$ be positive real numbers. Let $\Gamma$ be an access structure and $\Phi_1, \ldots, \Phi_N$ be access functions all on the same set of participants. We say that $(h_1, \Phi_1), \ldots, (h_N, \Phi_N)$ is a $\delta$–decomposition for $\Gamma$ if*

$$\delta = \min_{A \in \Gamma} \sum_{j=1}^{N} h_j \Phi_j(A) - \max_{B \in \Gamma^c} \sum_{j=1}^{N} h_j \Phi_j(B) > 0 \ .$$

As we saw in the previous subsection, the sub-schemes in $(\lambda, \omega)$-weighted decomposition need to be linear and, consequently, the sub-access functions $\Phi_j$'s must be *rational-valued*. In the (non-weighted) $(\lambda, \omega)$-decomposition [15], however, the sub-schemes can be linear or non-linear but they must be prefect. Consequently, the sub-access functions must be *perfect* (that is, they must be 0-1-valued functions to represent access structures).

The following theorem captures the strengths and limitations of both weighted and non-weighted decompositions, collectively. The proof is easy and straightforward and, hence, left to the reader. The reader may first recall the definition of a convec-converging family of secret sharing schemes (Definition 6.1).

**Theorem 7.4 ($\delta$-decomposition theorem)** *Let $\Gamma$ be an access structure and $(h_1, \Phi_1), \ldots, (h_N, \Phi_N)$ be a $\delta$–decomposition for it. Then:*

*(i)* ***(Rational/Linear)*** *If each $\Phi_j$ is a rational-valued access function and realizable by a convec-converging family of linear secret sharing schemes with convec $\sigma_j$, such that all the underlying finite fields have the same characteristic, then $\Gamma$ is realizable by a convec-converging family of linear schemes with the following convec*

$$\sigma = \frac{1}{\delta} \sum_{j=1}^{N} h_j \sigma_j \ . \tag{7.1}$$

*(ii)* ***(Perfect/Non-linear)*** *If each $\Phi_j$ is perfect (i.e., 0-1-valued) and realizable by a convec-converging family of (linear or non-linear) secret sharing schemes with convec $\sigma_j$, then $\Gamma$ is realizable by a convec-converging family of schemes with convec $\sigma$, defined in Equation (7.1).*

### 7.3 Discussion

It remains open if we can have a general decomposition theorem with the advantages of both weighted and non-weighted decompositions.

**Problem 7.5** *Let $\Gamma$ be an access structure and $(h_1, \Phi_1), \ldots, (h_N, \Phi_N)$ be a $\delta$–decomposition for it. Suppose that each $\Phi_j$ (not necessarily rational or 0-1-valued) is realizable by a convec-converging family of (linear or non-linear) secret sharing schemes with convec $\sigma_j$. Is it true that $\Gamma$ is realizable by a convec-converging family of schemes with convec $\sigma$, defined in Equation (7.1)? What if we restrict our attention to a sub-class of secret sharing schemes?*

A necessary condition for the answer to be positive for some class of secret sharing schemes is that there must exists a way to transform a partial scheme $\Pi$ for $\Gamma$ with advantage $\delta$ and convec $\mathrm{cv}(\Pi)$ into a perfect one with convec $\frac{1}{\delta}\mathrm{cv}(\Pi)$ (simply consider the case $N = 1$ with $h_1 = 1$). As we saw earlier, this holds true for the class of linear schemes (Sections 4) but it does not hold for the class of mixed-linear schemes (Sections 5). In addition to the above necessary condition, other strong properties may be needed to combine partial schemes to be able to handle the case of $N \geqslant 2$, which is hard to believe to exist for non-linear schemes, in general. Based on these observations, we tend to believe that it is not possible to substantially extend the $\delta$-decomposition theorem, apart from the two cases mentioned in Theorem 7.4. Our tendency does not change even if it turns out that partial and perfect information ratios coincide for some non-linear class of schemes.

## 8 Conclusion

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

We also reviewed several well-known non-perfect security notions and studied their relations. It remains challengingly an open problem that for which classes of schemes, the non-perfect and perfect information ratios coincide. Understanding this relation is not only an interesting problem in theory of non-perfect secret sharing, but also it may deepen our understanding of perfect schemes (for example in the case of duality).

Also, as rare example, we separated the partial and perfect information ratios for the class of mixed-linear schemes.

Table 2a, summarizes known results about the relations between non-perfect information ratios and perfect ones. Table 2b, summarizes known results about information ratios of dual access structures with respect to different security notions and different classed of schemes.

**Acknowledgment.** The authors would like to thank anonymous reviewers (Eurocrypt 2019 and TCC 2019) for constructive feedbacks which has substantially shaped our work.

| notion | class: linear | mixed-linear | abelian | homomorphic | GC ($G_0 \not\preccurlyeq G$) | GC | general |
|---|---|---|---|---|---|---|---|
| stat.-perfect | ✓ | ✓* | ✓* | ✓* | ✓* | ? | ? |
| almost-perfect | ✓ | ✓* | ✓* | ✓* | ✓* | ? | ? |
| quasi-perfect | ✓* | ? | ? | ? | ? | ? | ? |
| partial | ✓* | ✗* | ? | ? | ? | ? | ? |

(a) Coincidence of the non-perfect information ratios with perfect one

| notion | class: linear | mixed-linear | abelian | general |
|---|---|---|---|---|
| perfect | ✓ | ✓ | ✓ | ? |
| stat.-perfect | ✓ | ✓ | ✓ | ? |
| almost-perfect | ✓ | ✓ | ✓ | ✗ |
| quasi-perfect | ✓ | ✓ | ✓ | ? |
| partial | ✓* | ? | ? | ? |

(b) Coincidence of information ratios of dual access structures

Table 2: Summary of known results. A check mark (✓) stands for a match, a cross mark (✗) stands for a mismatch and a question mark (?) for an open situation. New results have been distinguished with a star. GC stands for group-characterizable.

## References


1. Beimel, A.: Secret-sharing schemes: A survey. In: Coding and Cryptology - Third International Workshop, IWCC 2011, Qingdao, China, May 30-June 3, 2011. Proceedings. pp. 11–46 (2011), http://dx.doi.org/10.1007/978-3-642-20901-7_2
2. Beimel, A., Ben-Efraim, A., Padró, C., Tyomkin, I.: Multi-linear secret-sharing schemes. In: Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings. pp. 394–418 (2014). https://doi.org/10.1007/978-3-642-54242-8_17, https://doi.org/10.1007/978-3-642-54242-8_17
3. Beimel, A., Franklin, M.K.: Weakly-private secret sharing schemes. In: Theory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007, Proceedings. pp. 253–272 (2007), https://doi.org/10.1007/978-3-540-70936-7_14
4. Beimel, A., Ishai, Y.: On the power of nonlinear secret-sharing. In: Proceedings of the 16th Annual IEEE Conference on Computational Complexity, Chicago, Illinois, USA, June 18-21, 2001. pp. 188–202 (2001), https://doi.org/10.1109/CCC.2001.933886
5. Beimel, A., Livne, N.: On matroids and nonideal secret sharing. IEEE Trans. Information Theory **54**(6), 2626–2643 (2008), https://doi.org/10.1109/TIT.2008.921708
6. Bertilsson, M., Ingemarsson, I.: A construction of practical secret sharing schemes using linear block codes. In: Advances in Cryptology - AUSCRYPT '92, Workshop on the Theory and Application of Cryptographic Techniques, Gold Coast, Queensland, Australia, December 13-16, 1992, Proceedings. pp. 67–79 (1992), https://doi.org/10.1007/3-540-57220-1_53
7. Blakley, G.R.: Safeguarding cryptographic keys. Proc. of the National Computer Conference1979 **48**, 313–317 (1979)

8. Blakley, G.R., Meadows, C.: Security of ramp schemes. In: Workshop on the Theory and Application of Cryptographic Techniques. pp. 242–268. Springer (1984)
9. Blundo, C., Santis, A.D., Stinson, D.R., Vaccaro, U.: Graph decompositions and secret sharing schemes. In: Advances in Cryptology - EUROCRYPT '92, Workshop on the Theory and Application of of Cryptographic Techniques, Balatonfüred, Hungary, May 24-28, 1992, Proceedings. pp. 1–24 (1992), http://dx.doi.org/10.1007/3-540-47555-9_1
10. Brickell, E.F., Stinson, D.R.: Some improved bounds on the information rate of perfect secret sharing schemes. J. Cryptology **5**(3), 153–166 (1992), http://dx.doi.org/10.1007/BF02451112
11. Chan, T.H., Yeung, R.W.: On a relation between information inequalities and group theory. IEEE Trans. Information Theory **48**(7), 1992–1995 (2002), https://doi.org/10.1109/TIT.2002.1013138
12. Cover, T.M., Thomas, J.A.: Elements of information theory (2. ed.). Wiley (2006)
13. Csirmaz, L.: Secret sharing and duality. CoRR **abs/1909.13663** (2019), http://arxiv.org/abs/1909.13663
14. D'Arco, P., Prisco, R.D., Santis, A.D., del Pozo, A.L.P., Vaccaro, U.: Probabilistic secret sharing. In: 43rd International Symposium on Mathematical Foundations of Computer Science, MFCS 2018, August 27-31, 2018, Liverpool, UK. pp. 64:1–64:16 (2018). https://doi.org/10.4230/LIPIcs.MFCS.2018.64, https://doi.org/10.4230/LIPIcs.MFCS.2018.64
15. van Dijk, M., Jackson, W., Martin, K.M.: A general decomposition construction for incomplete secret sharing schemes. Des. Codes Cryptography **15**(3), 301–321 (1998), https://doi.org/10.1023/A:1008381427667
16. Farràs, O., Hansen, T.B., Kaced, T., Padró, C.: On the information ratio of non-perfect secret sharing schemes. Algorithmica **79**(4), 987–1013 (2017). https://doi.org/10.1007/s00453-016-0217-9, https://doi.org/10.1007/s00453-016-0217-9
17. Gallian, J.: Contemporary abstract algebra. Nelson Education (2012)
18. Gharahi, M., Khazaei, S.: Optimal linear secret sharing schemes for graph access structures on six participants. Theoretical Computer Science (2018), https://doi.org/10.1016/j.tcs.2018.11.007
19. Hammer, D., Romashchenko, A.E., Shen, A., Vereshchagin, N.K.: Inequalities for shannon entropy and kolmogorov complexity. J. Comput. Syst. Sci. **60**(2), 442–464 (2000). https://doi.org/10.1006/jcss.1999.1677, https://doi.org/10.1006/jcss.1999.1677
20. Ito, M., Saito, A., Nishizeki, T.: Secret sharing scheme realizing general access structure. Electronics and Communications in Japan (Part III: Fundamental Electronic Science) **72**(9), 56–64 (1989)
21. Jackson, W., Martin, K.M.: Geometric secret sharing schemes and their duals. Des. Codes Cryptography **4**(1), 83–95 (1994). https://doi.org/10.1007/BF01388562, https://doi.org/10.1007/BF01388562
22. Jackson, W.A., Martin, K.M.: Perfect secret sharing schemes on five participants. Designs, Codes and Cryptography **9**(3), 267–286 (1996)
23. Jafari, A., Khazaei, S.: On abelian and homomorphic secret sharing schemes. Cryptology ePrint Archive, Report 2019/575 (2019), https://eprint.iacr.org/2019/575
24. Kaboli, R., Khazaei, S., Parviz, M.: Group-homomorphic secret sharing schemes are group-characterizable with normal subgroups. Cryptology ePrint Archive, Report 2019/576 (2019), https://eprint.iacr.org/2019/576

25. Kaced, T.: Almost-perfect secret sharing. In: 2011 IEEE International Symposium on Information Theory Proceedings, ISIT 2011, St. Petersburg, Russia, July 31 - August 5, 2011. pp. 1603–1607 (2011), https://doi.org/10.1109/ISIT.2011.6033816
26. Kaced, T.: Secret Sharing and Algorithmic Information Theory. (Partage de secret et the'orie algorithmique de l'information). Ph.D. thesis, Montpellier 2 University, France (2012), https://tel.archives-ouvertes.fr/tel-00763117
27. Kaced, T.: Information inequalities are not closed under polymatroid duality. IEEE Trans. Information Theory **64**(6), 4379–4381 (2018). https://doi.org/10.1109/TIT.2018.2823328, https://doi.org/10.1109/TIT.2018.2823328
28. Karchmer, M., Wigderson, A.: On span programs. In: Proceedings of the Eigth Annual Structure in Complexity Theory Conference, San Diego, CA, USA, May 18-21, 1993. pp. 102–111 (1993). https://doi.org/10.1109/SCT.1993.336536, https://doi.org/10.1109/SCT.1993.336536
29. Krawczyk, H.: Secret sharing made short. In: Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings. pp. 136–146 (1993). https://doi.org/10.1007/3-540-48329-2_12, https://doi.org/10.1007/3-540-48329-2_12
30. Kurosawa, K., Okada, K., Sakano, K., Ogata, W., Tsujii, S.: Nonperfect secret sharing schemes and matroids. In: Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings. pp. 126–141 (1993), https://doi.org/10.1007/3-540-48285-7_11
31. Martin, K.M.: New secret sharing schemes from old. J. Combin. Math. Combin. Comput **14**, 65–77 (1993)
32. Matús, F.: Matroid representations by partitions. Discrete Mathematics **203**(1-3), 169–194 (1999), https://doi.org/10.1016/S0012-365X(99)00004-7
33. Rogers, R.M., Roth, A., Smith, A.D., Thakkar, O.: Max-information, differential privacy, and post-selection hypothesis testing. In: IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016, 9-11 October 2016, Hyatt Regency, New Brunswick, New Jersey, USA. pp. 487–494 (2016). https://doi.org/10.1109/FOCS.2016.59, https://doi.org/10.1109/FOCS.2016.59
34. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979), http://doi.acm.org/10.1145/359168.359176
35. Stinson, D.R.: Decomposition constructions for secret-sharing schemes. IEEE Transactions on Information Theory **40**(1), 118–125 (1994)
36. Sun, H.M., Chen, B.L.: Weighted decomposition construction for perfect secret sharing schemes. Computers & Mathematics with Applications **43**(6), 877–887 (2002)

## A Basics of group theory

For reader's convenience, we recall the basic concepts from group theory which are used in this paper. They can be found in any standard textbook in algebra, e.g., [17].

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

**Subgroup.** A subset $H$ of a group $G$ is called a *subgroup* of $G$ if it satisfies the group axioms under the operation of $G$. By Lagrange 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.

**Subgroup product.** For subgroups $H, K$ of a group $(G, *)$, their product is defined to be $K * H = \{k * h : h \in K, h \in H\}$. Trivially, $K * H$ contains both $K$ and $H$. The set $K * H$ is not necessarily a subgroup and its size is given by the *product formula*: $|K * H| = \frac{|K||H|}{|k \cap H|}$. The product of two subgroups $H, K$ is a group if and only if they are *permuting*; that is, $H * K = K * H$. If one of these subgroups is normal in $G$, the requirement is satisfied and, hence, $H * K$ becomes a subgroup of $G$ too.

## B Completeness of group-characterizable schemes for quasi-perfect security

We show that group-characterizable schemes are "complete" for computing the quasi-perfect information ratio of access structures.

**Proposition B.1** *Group characterizable schemes are complete for quasi-perfect security. That is, the quasi-perfect information ratio of every access structure can be computed by restricting to the class of group-characterizable schemes.*

*Proof.* The Chan-Yeung's theorem [11, Theorem 4.1] is about random variables and can be stated for secret sharing schemes as follows: for every scheme $\Pi = (\boldsymbol{S}_i)_{i \in P \cup \{p_0\}}$, there exists a sequence $\{\Pi_k\}$ of group-characterizable schemes,

with $\Pi_k = (\boldsymbol{S}_i^k)_{i\in P\cup\{p_0\}}$, such that for every $A \subseteq P \cup \{p_0\}$ it holds that $\lim_{k\to\infty} \frac{1}{k}\mathrm{H}(\boldsymbol{S}_A^k) = \mathrm{H}(\boldsymbol{S}_A)$. It then follows that $\lim_{k\to\infty} \mathrm{cv}(\Pi_k) = \mathrm{cv}(\Pi)$ and $\lim_{k\to\infty} \Phi_{\Pi_k} = \Phi_\Pi$ (recall Definitions 2.4 and 2.6).

Now we return to the proof of our theorem. Let $\Gamma$ be an access structure and $\{\Pi_m\}_{m\in\mathbb{N}}$ be a quasi-perfect family for $\Gamma$. We need to show that, there exists a family $\{\Pi_{j,j}\}_{j\in\mathbb{N}}$ of group-characterizable schemes that quasi-perfectly realizes $\Gamma$ and satisfies

$$\lim_{j\to\infty} \mathrm{cv}(\Pi_{j,j}) = \lim_{m\to\infty} \mathrm{cv}(\Pi_m)\ . \tag{B.1}$$

By, Chan-Yeung's theorem, for each scheme $\Pi_m$, there exists a a sequence $\{\Pi_{k,m}\}$ of group-characterizable schemes such that $\lim_{k\to\infty} \mathrm{cv}(\Pi_{k,m}) = \mathrm{cv}(\Pi_m)$ and $\lim_{k\to\infty} \Phi_{\Pi_{k,m}} = \Phi_{\Pi_m}$. It is then easy to see that the family $\{\Pi_{j,j}\}$ of group-characterizable schemes satisfies (B.1) and $\lim_{j\to\infty} \Phi_{\Pi_{j,j}} = \lim_{m\to\infty} \Phi_{\Pi_m}$; that is, it also realizes $\Gamma$ quasi-perfectly. □