Partial Secret Sharing Schemes

Amir Jafari, and Shahram Khazaei,

***Abstract*—The following standard relaxations of perfect security for secret sharing schemes (SSSs) exist in the literature: *quasi-perfect*, *almost-perfect*, and *statistical*. Understanding the power of these relaxations on the efficiency of SSSs, measured via a parameter called *information ratio*, is a long-standing open problem.**

In this article, we introduce and study an extremely relaxed security notion, called *partial security*, for which it is only required that any qualified set gains strictly more information about the secret than any unqualified one. To get a meaningful efficiency measure, we normalize the (standard) information ratio of such schemes by an appropriate parameter and refer to the new measure as *partial information ratio*.

We present three main results in this paper. *First*, we prove that partial and perfect information ratios coincide for the class of linear SSSs. *Second*, we prove that for the general (i.e., non-linear) class of SSSs, partial and statistical information ratios are equal. *Third*, we show that partial and almost-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).

We also use the notion of partial secret sharing to strengthen and unify the previous *decomposition* theorems for constructing SSSs.

***Index Terms*—Information theoretic cryptography, Secret sharing, Perfect and non-perfect security, Wiretap channel, Decomposition methods.**

I. Introduction

A *secret sharing scheme* (SSS) [1], [2] allows a dealer to share a secret among a set of participants such that only certain *qualified* subsets of them can 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* [3], which is supposed to be monotone, i.e., closed under the superset operation.

The *information ratio* [4]–[6] of a participant in a SSS is defined as the ratio of the size (entropy) of his share to the size of the secret. The information ratio of a SSS is the maximum of all participants' information ratios. The information ratio of an access structure is defined as the infimum of the information ratios of all SSSs that realize it. Realization is defined with respect to some security notion, e.g., perfect or any variants of non-perfect security to be discussed in the next subsection. It is a difficult problem to compute the information ratio of access structures in general.

The most common types of SSS fall into the class of *multi-linear* schemes. In these schemes, the secret is composed of some finite field elements and the sharing is performed by applying a fixed linear mapping on the secret elements and some randomly chosen elements from the finite field. When the secret is a single field element, the scheme is called linear. In this paper, we do not make such a distinction and simply call all of them *linear*.

Several extensions of linear schemes exist in the literature. A *mixed-linear* [7] SSS is constructed by combining linear schemes with possibly different underlying finite fields. The class of *abelian* schemes contains mixed-linear schemes and is a subclass of *homomorphic* ones. The class of homomorphic schemes is itself a subclass of the so-called *group-characterizable*[1] schemes [8] since they are equivalent to the group-characterizable schemes when all subgroups are *normal* in the main group [9]. All these classes have an algebraic structure. A non-algebraic class of SSSs, called *quasi-linear*, has been introduced in [10].

A. Perfect and non-perfect security notions

Some closely related security notions for realization of an access structure by SSSs are given below, in decreasing order of security level. These definitions differ in how to quantify the amount of information about the secret that is "missed" by the qualified sects or "leaked" to the unqualified ones. All the notions are defined for a family of schemes indexed by a *secuirty parameter*.

- **Perfect:** The qualified sets must recover the secret with probability one and it must remain information-theoretically hidden from unqualified sets. These requirements are respectively called the *perfect correctness* and *perfect privacy* conditions.
- **Statistical:** The qualified sets may fail to recover the secret with some negligible probability of error and some negligible amount of information about the secret—quantified using the notion of *statistical distance*—can be leaked to unqualified sets. This is a standard relaxation and requires that the reconstruction error probability and statistical distance (which are both considered as functions of the security parameter) be negligible for the *worst* choice of the secret. For some technical and defensible reasons, we additionally require that the secret length grows at most polynomially in the security parameter.
- **Expected-statistical:** This notion is a non-standard variant of statistical security which we introduce in this paper for the first time for ease of reference, presentation, and

Both authors are with the Department of Mathematical Sciences, Sharif University of Technology, Tehran, Iran. E-mails: {ajafari,shahram.khazaei}@sharif.ir

Manuscript received April 19, 2005; revised August 26, 2015.

[1] Group-characterizable SSS will only be mentioned briefly in Section I-C. For completeness, we define it here. Given a finite group G and a collection $G_0, G_1, \ldots, G_n$ of its subgroups, a SSS can be constructed as follows which is called group-characterizable. The secret space is G/G_0, i.e., the set of all left cosets of G_0 in G, and the share space of participant i is G/G_i. To share a secret $s \in G/G_0$, a random $g \in G$ is chosen such that $s = gG_0$ and gG_i is given as a share to participant i.

comparison. It requires that the reconstruction error probability and statistical distance be negligible on *average*, over a random choice of the secret, rather than for the *worst* choice of the secret as in the statistical security.

- **Almost-perfect [11], [12]:** Some negligible amount of information about the secret is allowed to be missed by qualified sets and to be leaked to unqualified ones. The missed and leaked pieces of information are quantified in terms of entropy, which will again be functions of the security parameter.
- **Quasi-perfect [13, Chapter 5]:** This notion is similar to almost-perfect security with the difference that the missed/leaked information is considered relative to the secret entropy.

Similar definitions in other contexts: In the context of information-theoretic security, the privacy requirement for Wyner's *wiretap channel* [14] (1975) and Maurer's *secret key agreement* [15] (1991), were initially defined with respect to a definition similar to the quasi-perfect privacy requirement. Later, Maurer introduced a stronger privacy requirement in [16] (1994) which corresponds to almost-perfect security. Csiszar introduced an even stronger definition in [17] (1996) which corresponds to the expected-statistical definition mentioned above. These three notions have been studied extensively in subsequent works (e.g., see [18]–[20]) and it is known that the *secrecy capacity* is invariant with respect to these security requirements. It is known that the secrecy capacity remains unchanged even if we impose stronger reliability and privacy requirements, similar to those for statistical SSSs.

B. Motivations for studying non-perfect security notions

It is worth mentioning that the only security notions which are suitable for practical applications are the perfect and statistical ones; because, in adversarial settings, the reconstruction error probability, and information leak are taken into account for the worst choice of the message (secret). It is folklore that the weaker security requirements, even at the level of expected-statistical security, are problematic for most cryptographic applications. Nevertheless, not only is studying weaker security notions interesting from a theoretical point of view (e.g., to understand the power of imperfection), but it also helps us to gain insight and new results about stronger security notions. In the following, we provide three specific motivations for studying non-perfect security notions.

1) ***Upper-bounds on information ratio.*** It is generally easier to construct schemes with weaker security guarantees for an access structure. As we will see, in some situations, a scheme can be used to construct a scheme satisfying stronger security requirements (even perfect for some particular classes of schemes such as the linear ones). In particular, in some situations, e.g., in the so-called *weighted decomposition methods* [21], [22], a collection of perfect or non-perfect schemes for a collection of access structures are used for constructing a perfect scheme for a specifically targeted access structure. We will elaborate more on this in Section I-F.
2) ***Lower-bounds on information ratio.*** A well-known method for deriving lower bounds on the information ratio of access structures is based on the properties of *entropy* for random variables. One simple variant derives a lower bound by considering only the so-called *Shannon-type information inequalities* [23], [24]. Modified variants take into account the so-called *non-Shannon-type* information inequalities [25] too, either explicitly [26] or implicitly [27], [28]. As it was noticed by Kaced in [13, Theorem 36], any bound derived using these methods holds for quasi-perfect security as well. Therefore, if it turns out that quasi-perfect and perfect security notions are not equivalent with respect to the information ratio, new techniques must be developed that only apply to perfect security which, to the best of our knowledge, are currently missing.
3) ***Understanding duality.*** There is a natural definition for the *dual* of an access structure [29] and it is a long-standing open problem if the information ratios of dual access structures are equal. For the case of perfect security, the equality was proved for linear schemes in [29], [30] and has recently been extended to the class of *abelian* schemes in [7]. In a remarkable work, Kaced [11] recently showed that the information ratios of dual access structures for *general* schemes are not necessarily equal with respect to the weaker notion of almost-perfect security. An explicit construction was also exhibited by Csirmaz in [12]. Our understanding of the relation between the information ratios for different security notions might help us to resolve this long-standing open problem.

C. Known results and some questions

We are not aware of any extensive study of the non-perfect security notions in the setting of secret sharing. In this setting, special classes of SSSs (such as those mentioned at the beginning of the introduction) are also of particular interest. In particular, for a *given class* of SSSs, it is an open problem if the information ratio of an access structure is invariant with respect to different security notions, and very few results are known in this regard, reviewed next.

Equivalence: We say that two security notions $\mathcal{N}_1, \mathcal{N}_2$ are *equivalent* for a class $\mathcal{C}$ of SSSs and write "$\mathcal{N}_1 \equiv \mathcal{N}_2$ (for class $\mathcal{C}$)" if the following holds: if a family of SSSs in the class $\mathcal{C}$ realizes an access structure with respect to the security notion $\mathcal{N}_1$, so does it with respect to the security notion $\mathcal{N}_2$.

Recently, Kaboli, Khazaei, and Parviz proved in [9] that the almost-perfect (and consequently statistical and expected-statistical) security is equivalent to the perfect security for *group-characterizable* (GC) SSSs whose secret subgroup is *normal* in the main group (see Footnote 1); that is,

$$\text{almost-perfect} \equiv \text{expected-statistical} \equiv \text{statistical} \equiv \text{perfect}$$
$$\text{(for GC schemes with normal secret subgroup).} \tag{I.1}$$

As we discussed earlier, this class includes several well-known classes of SSSs including the *linear* schemes. The equivalence for linear schemes is quite trivial and had already been realized by Beimel and Ishai in [10]. On the other hand, it is easy to see that the quasi-perfect and almost-perfect security notions are not equivalent for the linear class; i.e.,

$$\text{quasi-perfect} \not\equiv \text{almost-perfect} \qquad \text{(for linear schemes).}$$

To see this, consider a family of schemes for the 2-out-of-2 threshold access structure as follows. The secret of the m'th scheme is an m-bit-long string $(s_1, \ldots, s_m)$. The share of the first participant is an $(m-1)$-bit-long random string $(r_1, \ldots, r_{m-1})$. The share of the second party is $(r_1 \oplus s_1, \ldots, r_{m-1} \oplus s_{m-1})$. Clearly, the family is quasi-perfect, but none of the schemes is perfect.

Regarding the inequivalence of quasi-perfect and almost-perfect security notions, it is natural to ask if the two notions coincide with respect to information ratio; that is:

Question I *Does the following equality hold?*

$$\textit{quasi-perfect} \overset{?}{=} \textit{almost-perfect} \qquad \textit{(for linear schemes).}$$

Here, for security notions $\mathcal{N}_1, \mathcal{N}_2$ and a class $\mathcal{C}$ of schemes, the equality "$\mathcal{N}_1 = \mathcal{N}_2$ (for class $\mathcal{C}$)" is understood as follows: when restricted to the class $\mathcal{C}$ of SSSs, the information ratio of every access structure with respect to the security notion $\mathcal{N}_1$ is the same as its information ratio with respect to the security notion $\mathcal{N}_2$.

A trivial inequality: It can be shown (see Section III-D) that the following relation holds for the information ratios of an access structure with respect to the mentioned security notions and for every class of SSSs:

$$\begin{gathered}\text{quasi-perfect} \leqslant \text{almost-perfect} \leqslant \text{expected-statistical} \\ \leqslant \text{statistical} \leqslant \text{perfect} \\ \text{(for any class of schemes).}\end{gathered} \tag{I.2}$$

Csirmaz's observation: In Appendix A, we quote a proof, suggested by Laszlo Csirmaz in private communication, for the equality of quasi-perfect and almost-perfect information ratios, for the general class of SSSs; that is,

$$\begin{gathered}\text{quasi-perfect} = \text{almost-perfect} \\ \text{(for general schemes).}\end{gathered} \tag{I.3}$$

Csirmaz uses the properties of the so-called *entropy region* [25] to prove this equality using a very simple and elegant argument. Unfortunately, his argument does not extend to stronger security notions and it is open if this equality can be extended to stronger security notions.

Question II *Do the following equalities hold?*

$$\begin{gathered}\textit{almost-perfect} \overset{?}{=} \textit{expected-statistical} \overset{?}{=} \textit{statistical} \overset{?}{=} \textit{perfect} \\ \textit{(for any class of schemes).}\end{gathered}$$

In this paper, we will fully resolve Question I and partially resolve Question II. Additionally, we resolve the following rather natural question.

Question III *Let $\mathcal{N}_1, \mathcal{N}_2$ be two security notions and $\mathcal{C}_1 \subseteq \mathcal{C}_2$ be two classes of SSSs such that "$\mathcal{N}_1 = \mathcal{N}_2$ (for $\mathcal{C}_i$)", for $i = 1, 2$. Is it true that for evey class $\mathcal{C}$ of SSSs such that $\mathcal{C}_1 \subseteq \mathcal{C} \subseteq \mathcal{C}_2$, it holds that "$\mathcal{N}_1$=$\mathcal{N}_2$ (for $\mathcal{C}$)"?*

We attack the above three questions by introducing a new non-perfect security notion. We will describe our new security notion in Section I-D and use it in Section I-E to present our results on the mentioned questions. Regarding the first motivation for studying non-perfect SSSs, mentioned in Section I-B, an application of our new notion in the construction of efficient SSSs is also discussed in Section I-F.

We additionally provide some discussion in Section I-G about imperfection in other information-theoretic contexts (and in particular CDS, a cryptographic primitive closely related to SSS) and study their implications in the secret sharing setting.

D. Partial security: a new non-perfect notion

We introduce an extremely relaxed security notion, called *partial* security. We say that a SSS partially realizes an access structure if the amount of information gained about the secret by any qualified set is strictly greater than that of any unqualified one. In other words, the qualified sets have a positive *advantage* δ over the unqualified ones concerning the amount of information gained about the secret relative to the secret entropy. Thus, a perfect scheme is also partial with $\delta = 1$, because the qualified sets recover the whole secret but the unqualified ones gain no information about the secret. We refer to Section IV-D for some examples.

Related security notions: Partial security is related to the so-called *probabilistic/weak* security notions [31], [32], but has much weaker requirements in both correctness and privacy. Probabilistic SSSs can be divided into two categories. The *weakly-private* [31] schemes require perfect correctness whereas, for privacy, it suffices that every secret is probable for an unqualified set. The *weakly-correct* [32] schemes require perfect privacy whereas, for correctness, it suffices that qualified subsets recover the secret with non-zero probability. What makes partial security non-trivial and more interesting is a new parameter that we introduce to quantify their efficiency, to be defined next. We will discuss the effect of this choice for the case of weakly-private SSSs in the paper (Section IV-C and Example IV.4).

Partial information ratio: For all previous security notions, the *standard* notion of information ratio (i.e., the ratio between the largest share size and the secret size) is used to quantify the efficiency of SSSs. However, to compensate for the extreme imperfection that partial SSSs bear by our definition, we quantify the efficiency of such schemes using a parameter called *partial information ratio*. It is defined to be the (standard) information ratio scaled by the factor $1/\delta$, where δ is the advantage mentioned above. The intuition behind this choice stems from two concepts: (i) the *capacity of wiretap channel* [14], [33] and (ii) a similar factor in *decomposition constructions* [21], [22], [34], [35]. These subjects will be studied in detail in the paper in Section VI and Section VIII, respectively.

E. Main results

The notion of partial information ratio makes it fair to compare the efficiency of partial security with other security notions. Recall that by (I.2), quasi-perfect security is weaker than all mentioned non-perfect security notions, for every arbitrary class of SSSs. It is easy to observe that, despite our compensation factor, the partial security is still weaker than all previously mentioned notions; that is:

$$\text{partial} \leqslant \text{quasi-perfect} \quad \text{(for any class of schemes)}.$$

In this paper, we present the following three main results about partial SSSs:

a) **Linear/Perfect/Coincidence:** We prove that the partial information ratio of an access structure is equal to its perfect information ratio for the class of linear schemes; i.e.,

$$\text{partial} = \text{perfect} \qquad \text{(for linear schemes)}, \tag{I.4}$$

from which a postive answer to Question I follows; i.e.,

$$\text{quasi-perfect} = \text{perfect} \qquad \text{(for linear schemes)}.$$

To prove this result, we present a "universal" transformation that turns "every" linear partial scheme into a perfect one without changing its (partial) information ratio. The main idea is to share carefully-chosen linear functions of the secret using the partial scheme independently. The correctness and privacy of the construction are proved using two linear algebraic lemmas.

b) **General/Statistical/Coincidence:** We prove that the partial and statistical information ratios of an access structure coincide for the class of general schemes; that is,

$$\text{partial} = \text{statistical} \qquad \text{(for general schemes)}, \tag{I.5}$$

from which we partially resolve Question II and provide the following generalization of Csirmaz's observation (recall relation (I.3)):

$$\text{quasi-perfect} = \text{almost-perfect} = \text{expected-statistical} = \text{statistical}$$
$$\text{(for general schemes)}.$$

The proof is achieved by viewing a partial SSS as a multi-receiver multi-eavesdropper wiretap channel [14] and providing a *sharp analysis* for the near-capacity behavior of such channels which, to the best of our knowledge, has not appeared in the literature. We remark that the connection between SSSs and wiretap channels has already been realized in [36], [37], however, the motivations of those works are different from ours.

c) **Mixed-linear/Almost-perfect/Separation:** We provide an example of an access structure such that its partial information ratio is smaller than its almost-perfect information ratio, for the class of *mixed-linear* schemes. That is:

$$\text{partial} \lneqq \text{almost-perfect}$$
$$\text{(for mixed-linear schemes)}.$$

This inequality is proved for an access structure on 12 participants, introduced in [38] and further studied in [7], which has both Fano and non-Fano access structures as minors. The proof relies on the fact that these access structures behave differently with respect to the characteristic of the underlying finite field. Since linear schemes are special cases of mixed-linear schemes, by equalities (I.4) and (I.5), it follows that the answer to Question III is negative.

F. General decomposition theorems

Given an access structure, in some situations, it is easier to first construct partial schemes for it. For example, in the so-called *weighted decomposition methods* [21], [22]—which are generalizations of non-weighted decompositions [34], [39], [40]—several perfect or non-perfect linear subschemes are combined to construct a partial linear scheme. The subschemes realize access structures which are usually much simpler than the given one. Our first result can be used to transform the obtained partial scheme for the initial access structure into a perfect one. These methods have been very effective in finding the optimal perfect linear SSSs for small access structures (e.g., see [22], [40]–[44]). The project of finding optimal SSSs for small access structures was initiated in [45], [46] and is not finalized yet; because the optimal perfect non-linear schemes for some access structures on five participants and several graph-based access structures on six participants are still unknown.

Our first result strengthens the decomposition theorem in [21], [22] for constructing perfect linear schemes (the theorems in [21], [22] are only applicable to special linear partial schemes and now this requirement is relaxed). More interestingly, our second result leads to a very strong decomposition theorem for the construction of general (i.e., non-linear) schemes with statistical security (Theorem VIII.6). We believe that our decomposition theorem will turn out useful for constructing almost-optimal statistical SSSs for small access structures, advancing the project initiated in [45], [46] one step forward. We would not be surprised if it also finds applications in designing efficient general statistical SSSs (e.g., by using non-perfect CDS [47]). Currently, the best achieved upper-bound for perfect security is 1.5^n [48] (building on the breakthrough result of [49] and follow-ups [50], [51]).

G. Imperfection in other contexts and implications on secret sharing

As we mentioned earlier, it is open whether imposing weaker correctness and/or privacy conditions in the context of secret sharing leads to more efficient schemes as long as we use the information ratio as a measure of efficiency. In contrast, for several primitives in the context of network information theory (e.g., the wiretap channel), it is well-known that requiring perfect reliability and/or perfect privacy may lead to zero capacity.

On the other hand, in the context of secret key agreement with public discussion [15], [52] or more generally the multi-receiver multi-eavesdropper setting of Wyner's *wiretap channel*, it was long known that requiring perfect correctness does not lead to a stronger security notion; indeed, perfect decoding becomes possible but with the price of increasing the information leakage linearly in the number of eavesdroppers (but still negligible on the block length).

A similar situation arises in the context of non-perfect secret sharing as it was also noticed by Kaced in [13, Theorem 33]; here, it is also possible to achieve perfect correctness, but the information leakage will increase exponentially in the number of participants (linear in the number of minimal unqualified sets).

These observations may justify the recent result of Applebaum and Vasudevan [47] who showed that in the context of CDS [53] (which corresponds to the class of 2-uniform access structures), relaxing correctness requirements in CDS with one-bit secrets improves the communication complexity. In particular, they achieved a $\Theta(n)$ separation for the *non-equality predicate* which takes two n-bit long strings and outputs one iff they are distinct. However, it was left open if such a separation can be achieved by only relaxing the privacy requirement.

Applebaum and Vasudevan's result on non-perfect CDS shows that for one-bit secrets, partial schemes with perfect privacy outperform partial schemes with perfect correctness (and hence perfect schemes too) and a $\Theta(\log n)$ separation for share size can be achieved. However, in terms of information ratio (i.e., when the secret can be arbitrarily-long), it remains open if such a separation holds. Indeed, for the case of 2-uniform access structures, it does not because such access structures are known to have a constant information ratio (which is achieved for exponentially-long secrets [54]). It also remains open if Applebaum and Vasudevan's $\Theta(\log n)$ separation holds for polynomially-long secrets. See Example IV.6 for further details.

H. Paper organization

In Section II, we present the required preliminaries and introduce our notation. In Section IV the notions of partial security and partial information ratio are introduced. Sections V, VI and VII are devoted to proving the first, second and third results, respectively. In Section VIII, we revisit decomposition techniques and strengthen previous results. Section IX concludes the paper.

II. Preliminaries

In this section, we provide the basic background along with some notations. We refer the reader to Beimel's survey [55] on secret sharing.

A. General notations

All random variables (RVS) are discrete in this paper. The Shannon entropy of a RV $\boldsymbol{X}$ is denoted by $\mathrm{H}(\boldsymbol{X})$ and the mutual information of RVs $\boldsymbol{X}, \boldsymbol{Y}$ is denoted by $\mathrm{I}(\boldsymbol{X} : \boldsymbol{Y})$. The support of a RV $\boldsymbol{X}$ 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.

B. 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 distribution on the secret space. In this paper, we use the following definition for secret sharing.

Definition II.1 (Secret sharing scheme) *A tuple* $\Pi = \left(\boldsymbol{S}_i\right)_{i \in P \cup \{0\}}$ *of jointly distributed RVs with finite supports is called a* secret sharing scheme *on participants set* P *when* $\mathrm{H}(\boldsymbol{S}_0) > 0$. *The RV* $\boldsymbol{S}_0$ *is called the* secret *RV and its support is called the* secret space. *The RV* $\boldsymbol{S}_i$*,* $i \in P$*, is called the* share *RV of participant* i*, and its support is called his* share space.

When we say that a secret s_0 *is shared using* Π, we mean that a tuple $\left(s_i\right)_{i \in P \cup \{0\}}$ is sampled according to the distribution Π 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 the dealer is to allow pre-specified subsets of participants to recover the secret. The secret must remain information-theoretically hidden from all other subsets of participants. This intuition is formally captured by the following definitions.

Definition II.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* $B \in \Gamma$*. A subset* $A \subseteq P$ *is called* qualified *if* $A \in \Gamma$*; otherwise, it is called* unqualified. *A qualified subset is called* minimal *if none of its proper subsets are qualified. An unqualified subset is called* maximal *if none of its proper supersets are unqualified.*

Definition II.3 (Perfect realization) *We say that a secret sharing scheme* $\Pi = \left(\boldsymbol{S}_i\right)_{i \in P \cup \{0\}}$ *is a* (perfect) scheme *for* Γ*, or it* (perfectly) realizes Γ*, if the following conditions 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* $B \in \Gamma^c$.

C. Access function

Non-perfect secret sharing schemes have been studied in several works including [21], [56], [57]. The notion of access function, introduced in [30], is a generalization of the definition of access structures that facilitates the study of non-perfect schemes.

Definition II.4 (Access function [30]) *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 amount of information gained by every subset of participants about the secret relative to the secret entropy.

Definition II.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:*

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

We say that a SSS Π realizes an access function Φ if $\Phi = \Phi_\Pi$. It is known [30] that every access function is realizable by some SSS. It is also worth mentioning that *all-or-nothing* (i.e., *0-1-valued*) access functions correspond to access structures.

D. Convec and information ratio

Convec is short for contribution vector [46] and a norm on it can be used as an indication of the efficiency of a secret sharing scheme.

Definition II.6 (Convec of a scheme) *The* (standard) 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 the maximum/average information ratios of all secret sharing schemes that realize it. In this paper, we restrict our attention to maximum information ratios, unless otherwise stated.

E. Linear schemes

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 this paper.

Definition II.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 II.7 and the description preceding it. One can think of a linear secret sharing scheme as being represented by a matrix, where each row is associated with either 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 and 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 [58], by Karchmer and Wigderson (or multi-target span programs [59]).

The above description essentially tells us how to associate a collection of RVs $(\boldsymbol{S}_i)_{i\in P\cup\{0\}}$ 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 RV, however, depends on the selected bases for T_i's. In the following, we describe a method, introduced in [60], to define an induced RV that 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 such possible linear functions. The RV associated to the subspace T_i is defined by $\boldsymbol{S}_i = \boldsymbol{\alpha}|_{T_i}$, i.e., the restriction[2] of the map $\boldsymbol{\alpha}$ to the domain T_i. It is easy to see that for every $i, j \in P \cup \{0\}$, the joint RV $(\boldsymbol{S}_i, \boldsymbol{S}_j)$ is "isomorphic" with the RV $\boldsymbol{\alpha}|_{T_i+T_j}$; that is, they have the same distribution up to renaming the elements of their supports. More generally, for any subset $A \subseteq P \cup \{0\}$, the joint RV $\boldsymbol{S}_A = (\boldsymbol{S}_i)_{i\in A}$ is isomorphic with the RV $\boldsymbol{\alpha}|_{T_A}$, where $T_A = \sum_{i\in A} T_i$. Here, $T_A = \sum_{i\in A} T_i$ denotes the sum of vector subspaces, for a subset $A \subseteq [n]$, i.e., T_A is the set of all possible sums $\sum_{i\in A} t_i$ where $t_i \in T_i$. 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, where $T_A = \sum_{i\in A} T_i$:

$$\Phi_\Pi(A) = \frac{\dim(T_0 \cap T_A)}{\dim(T_0)} \ ,$$

and

$$\mathrm{cv}(\Pi) = \big(\frac{\dim(T_i)}{\dim(T_0)}\big)_{i\in P} \ .$$

Linear and mixed-linear information ratios: In the computation of information ratio, if we restrict ourselves to the class of linear schemes, we refer to it as the linear information ratio. In the following subsection, we define the class of mixed-linear schemes, where the corresponding parameter is referred to as the mixed-linear information ratio.

F. Mixed-linear schemes

The class of mixed-linear SSSs was recently introduced in [7] and it was proved to be superior to the linear class (i.e., there exists an access structure whose linear information

[2] For a function $f : D \to R$ and 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 $x \in A$.

ratio is larger than its mixed-linear information ratio). Mixed-linear schemes are a subclass of homomorphic schemes and it is an open problem if homomorphic schemes can outperform mixed-linear ones [7, Problem 6.4].

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

Definition II.8 *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 Π and Π', respectively, we independently share s using Π and s' using Π'. Hence, each participant in $\Pi \oplus \Pi'$ receives a share from Π and one from Π'.

III. Non-perfect security notions

In this section, we present formal definitions of the non-perfect security notions for SSSs, mentioned in the introduction.

Family of SSSs: Non-perfect security notions are defined with respect to a family $\{\Pi_m\}_{m\in\mathbb{N}}$ of SSSs, where m can be considered a security parameter. We assume that *first*, the sequence of secret entropies does not tend to zero, and *second*, the sequence of information ratios of the SSSs in our families is converging. We, refer to the converged value as the *information ratio of the family*.

A. Statistical and expected-statistical security notions

Statistical SSS is a standard relaxation of perfect security, probably first mentioned in [61]. Here, we present a definition similar to the one in [10].

Notation: A function $\varepsilon : \mathbb{N} \to \mathbb{R}^{\geqslant 0}$ is called *negligible* if $\varepsilon(m) = m^{-\omega(1)}$. Also the *statistical distance* (or total variation) between two (discrete) RVs $\boldsymbol{X}$ and $\boldsymbol{Y}$, with respective probability mass functions $p_{\boldsymbol{X}}$ and $p_{\boldsymbol{Y}}$, is defined as:

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

For jointly distributed RVs $(\boldsymbol{X}, \boldsymbol{Y})$, with the joint probability mass function $p_{\boldsymbol{XY}}$ and marginal mass functions $p_{\boldsymbol{X}}$ and $p_{\boldsymbol{Y}}$, we will use the following notation:

$$\mathrm{SD}(p_{\boldsymbol{XY}}, p_{\boldsymbol{X}}p_{\boldsymbol{Y}}) := \frac{1}{2}\sum_{(x,y)} |\Pr[(\boldsymbol{X}, \boldsymbol{Y}) = (x, y)] - \Pr[\boldsymbol{X} = x]\Pr[\boldsymbol{Y} = y]| \ .$$

Statistical security: Let $\{\Pi_m\}_{m\in\mathbb{N}}$ be a family of secret sharing schemes, where $\Pi_m = (\boldsymbol{S}_0^m, \boldsymbol{S}_1^m, \ldots, \boldsymbol{S}_n^m)$, and Γ is an access structure on n participants. We say that $\{\Pi_m\}$ is a statistical family for Γ (or $\{\Pi_m\}$ statistically realizes Γ) if:

- **(Polynomial secret length growth)** The secret length grows at most polynomially in m; that is, $\log|\mathrm{supp}(\boldsymbol{S}_0^m)| = \mathrm{O}(m^c)$ for some $c > 0$.
- **(Statistical-correctness)** For every qualified set $A \in \Gamma$, there exists a reconstruction function $\textsc{Recon}_A$ such that for every secret s in support of $\boldsymbol{S}_0^m$, the reconstruction probability of error $\Pr[\textsc{Recon}_A(\boldsymbol{S}_A^m) \neq s | \boldsymbol{S}_0^m = s]$ is negligible in m;
- **(Statistical-privacy)** For every unqualified set $B \notin \Gamma$ and for every secret s in the support of $\boldsymbol{S}_0^m$, the statistical distance $\mathrm{SD}(p_{\boldsymbol{S}_B^m|\boldsymbol{S}_0^m=s}, p_{\boldsymbol{S}_B^m})$ is negligible in m.

The statistical privacy condition requires that for every unqualified set B, the statistical distance between the conditional RV $[\boldsymbol{S}_B^m|\boldsymbol{S}_0^m = s]$ and RV $\boldsymbol{S}_B^m$ be negligible for the worst choice of the secret s. Notice that, by the triangle inequality, the privacy condition implies that for every pair of secrets s, s' the statistical distance between the conditional RVs $[\boldsymbol{S}_B^m|\boldsymbol{S}_0^m = s]$ and $[\boldsymbol{S}_B^m|\boldsymbol{S}_0^m = s']$ is negligible too.

Remark III.1 (On the secret length growth) *We remark that the condition on the polynomial secret length growth for statistical and expected-statistical security notions makes sure that the error probability of reconstruction and the statistical distance are negligible not only in the security parameter* m *but also in the secret length. Indeed, the condition on the polynomial secret length growth is not a limit on the family of the SSSs because given any family, we can construct a new family (with the same information ratio) that satisfies this condition. The schemes* Π_m *and* Π_{m+1} *of the old family appear in the new family too but at positions* $\tau(m)$ *and* $\tau(m+1)$*, respectively, where* $\tau : \mathbb{N} \to \mathbb{N}$ *is some mapping for which the distance* $\tau(m+1) - \tau(m)$ *is chosen large enough such that the polynomial secret length growth condition is satisfied in the new family. The schemes at positions* $\tau(m)+1, \ldots, \tau(m+1)-1$ *are considered to be* Π_m*.*

Expected-statistical security: The definition for expected-statistical security is identical to the previous definition except that we require the following correctness and privacy conditions hold instead:

- **(Expected-statistical-correctness)** For every qualified set $A \in \Gamma$, there exists a reconstruction function $\textsc{Recon}_A$ such that $\Pr[\textsc{Recon}_A(\boldsymbol{S}_A^m) \neq \boldsymbol{S}_0^m]$ is negligible in m;
- **(Expected-statistical-privacy)** For every unqualified set $B \notin \Gamma$, the statistical distance $\mathrm{SD}(p_{\boldsymbol{S}_B^m\boldsymbol{S}_0^m}, p_{\boldsymbol{S}_B^m}p_{\boldsymbol{S}_0^m})$ is negligible in m.

The statistical-correctness requirement takes the worst probability of reconstruction error into account whereas the expected-statistical-correctness condition considers the average probability of error; because:

$$\Pr[\textsc{Recon}_A(\boldsymbol{S}_A^m) \neq \boldsymbol{S}_0^m] = \sum_{s\in\mathrm{supp}(\boldsymbol{S}_0^m)} \Pr[\boldsymbol{S}_0^m = s]\Pr[\textsc{Recon}_A(\boldsymbol{S}_A^m) \neq s \mid \boldsymbol{S}_0^m = s] \ . \tag{III.1}$$

Similarly, the expected-statistical-privacy condition requires that an unqualified set B is not able to (statistically) distinguish the joint distributions $(\boldsymbol{S}_B^m, \boldsymbol{S}_0^m)$ and $(\boldsymbol{S}_B^m, \boldsymbol{S}')$, where $\boldsymbol{S}'$ is independent of $\boldsymbol{S}_B^m$ and identically distributed as $\boldsymbol{S}_0^m$. The statistical privacy condition requires that the statistical distance between the conditional RV $[\boldsymbol{S}_B^m|\boldsymbol{S}_0^m = s]$ and RV $\boldsymbol{S}_B^m$ be negligible for the worst choice of the secret s. However, the expected-statistical privacy condition requires this to happen on average; because for every pair of jointly distributed RVs $(\boldsymbol{X}, \boldsymbol{Y})$ we have:

$$\mathrm{SD}(p_{\boldsymbol{X}\boldsymbol{Y}}, p_{\boldsymbol{X}} p_{\boldsymbol{Y}}) = \sum_{y \in \mathrm{supp}(\boldsymbol{Y})} \Pr[\boldsymbol{Y} = y] \mathrm{SD}(p_{\boldsymbol{X}|\boldsymbol{Y}=y}, p_{\boldsymbol{X}}) \ . \tag{III.2}$$

B. Almost-perfect and quasi-perfect security notions

In [12], almost-perfect security has been defined in terms of the so-called *almost entropic polymatroids*. Here, we present an equivalent definition in terms of a family of SSSs.

Notation: We call a function $\varepsilon : \mathbb{N} \to \mathbb{R}^{\geqslant 0}$ *tiny* if $\varepsilon(m) = o(1)$, or equivalently, $\lim\limits_{m \to \infty} \varepsilon(m) = 0$.

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

- **(Almost-correctness)** $\mathrm{H}(\boldsymbol{S}_0^m | \boldsymbol{S}_A^m)$ is tiny for every qualified set $A \in \Gamma$,
- **(Almost-privacy)** $\mathrm{I}(\boldsymbol{S}_0^m : \boldsymbol{S}_B^m)$ is tiny for every unqualified set $B \notin \Gamma$.

Quasi-perfect security: In quasi-perfect security it is required that the percentage of information missed/leaked in the correctness and privacy conditions are negligible. That is:

- **(Quasi-correctness)** $\frac{\mathrm{H}(\boldsymbol{S}_0^m | \boldsymbol{S}_A^m)}{\mathrm{H}(\boldsymbol{S}_0^m)}$ is tiny for every qualified set $A \in \Gamma$,
- **(Quasi-privacy)** $\frac{\mathrm{I}(\boldsymbol{S}_0^m : \boldsymbol{S}_A^m)}{\mathrm{H}(\boldsymbol{S}_0^m)}$ is tiny for every unqualified set $B \in \Gamma^c$.

Using the notion of the access function of a SSS (Definition II.5), we can equivalently say that a family $\{\Pi_m\}_{m \in \mathbb{N}}$ of SSSs quasi-perfectly realizes an access structure Γ if $\lim_{m \to \infty} \Phi_{\Pi_m}(A)$ equals one when $A \in \Gamma$ and zero when $A \notin \Gamma$. The definition straightforwardly extends to access functions (see Section VIII-C).

Remark III.2 (Tiny vs. negligible) *In the informal definitions of almost-perfect and quasi-perfect security notions in the introduction, we required the missed and leaked information be negligible instead of tiny. However, this does not make any difference since the two definitions remain equivalent as we discuss next. Given a family for which these quantities are tiny, we can construct a new family (with the same information ratio) for which these quantities are negligible (by choosing a suitable subsequence of the schemes in which consecutive schemes are far enough in the original family).*

Remark III.3 (On polynomial secret length growth) *In the definitions of almost-perfect and quasi-perfect security notions, we could have also imposed the additional requirement that the secret length grows at most polynomially in m. However, it would be redundant; because similar to our discussion in Remark III.1, we can construct a new family, by repeating each scheme a suitable number of times, such that the secret length grows slowly enough.*

C. Non-perfect information ratios

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

D. Relations between non-perfect information ratios

In this section we show that the following relation holds for the information ratios of an access structure with respect to the mentioned security notions and for every class of SSSs:

$$\begin{gathered}\text{quasi-perfect} \leqslant \text{almost-perfect} \leqslant \text{expected-statistical} \leqslant \text{statistical} \\ \text{(for any class of SSSs)} \ .\end{gathered} \tag{III.3}$$

The left-most inequality is trivial. The right-most inequality follows by relations (III.1) and (III.2). We prove the middle one. As we will see the condition on polynomial secret length growth turns out crucial.

- **Correctness implication.** The expected-statistical-correctness condition implies the almost-correct condition. This follows by Fano's inequality [62] is stated as follows. Suppose that we wish to estimate the RV $\boldsymbol{X}$, with support $\mathcal{X}$, by an estimator $\widehat{\boldsymbol{X}}$, and furthermore, assume that $\varepsilon = \Pr[\boldsymbol{X} \neq \widehat{\boldsymbol{X}}]$. Then, $\mathrm{H}(\boldsymbol{X}|\widehat{\boldsymbol{X}}) \leqslant \mathrm{H}(\varepsilon) + \varepsilon \log(|\mathcal{X}| - 1)$, where $\mathrm{H}(\varepsilon)$ is the entropy of a Bernoulli RV with parameter ε. Let A be a qualified set and $\widehat{\boldsymbol{S}_0^m} = \textsc{Recon}_A(\boldsymbol{S}_A^m)$. By statistical-correctness, for every secret s, the error probability $\varepsilon(m) := \Pr[\widehat{\boldsymbol{S}_0^m} \neq s | \boldsymbol{S}_0^m = s]$ is negligible in m. By polynomial secret length growth and Fano's inequality $\mathrm{H}(\boldsymbol{S}_0^m | \boldsymbol{S}_A^m)$ is negligible too.
- **Privacy implication.** The expected-statistical-privacy condition implies the almost-privacy condition. This follows by a lemma probably first mentioned in [63, Lemma 1], with the following statement. Let $(\boldsymbol{X}, \boldsymbol{Y})$ be a pair of jointly distributed RVs and let $\varepsilon_1 = \mathrm{I}(\boldsymbol{X} : \boldsymbol{Y})$ and $\varepsilon_2 = \mathrm{SD}(p_{\boldsymbol{X}\boldsymbol{Y}}, p_{\boldsymbol{X}} p_{\boldsymbol{Y}})$. Let $\mathcal{X}$ denote the support of $\boldsymbol{X}$ and $\mathcal{X} \geqslant 4$. Then we have the following inequality, where e is the Euler's number and the logarithms are in base two:

$$\frac{\log e}{2} \varepsilon_2^2 \leqslant \varepsilon_1 \leqslant \varepsilon_2 \log \frac{|\mathcal{X}|}{\varepsilon_2} \ . \tag{III.4}$$

IV. Partial secret sharing

In this section, we introduce a relaxed security notion for SSSs, called *partial* security. In addition, we provide some examples and discuss a slightly relevant security notion for SSSs called *weakly-private*, which has already been studied in the literature. Further properties and applications of our new security notion will be studied in later sections.

A. 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. Below, we give a formal definition. The reader may first recall the definition of the access function of a SSS (Definition II.5).

Definition IV.1 (Partial realization) *We say that a SSS* $\Pi = \big(\boldsymbol{S}_i\big)_{i\in P\cup\{0\}}$ *is a* partial scheme *for* Γ*, or it* partially realizes Γ*, if:*

$$\delta = \min_{A\in\Gamma} \Phi_\Pi(A) - \max_{B\in\Gamma^c} \Phi_\Pi(B) > 0\ . \tag{IV.1}$$

The parameter δ 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. In Section VI, we will see that the *unnormalized* parameter

$$C_\Pi := \mathrm{H}(\boldsymbol{S}_0)\delta = \min_{A\in\Gamma} \mathrm{I}(\boldsymbol{S}_0 : \boldsymbol{S}_A) - \max_{B\in\Gamma^c} \mathrm{I}(\boldsymbol{S}_0 : \boldsymbol{S}_B) \tag{IV.2}$$

is related to the capacity of Wyner's wiretap channel [14], which we refer to as the *nominal capacity* of the SSS Π (with respect to Γ). The inverse of δ is an important factor that will be taken into account in the next subsection to quantify the efficiency of partial schemes.

Partially-correct and partially-private SSSs: One can define two more restricted (i.e., less relaxed) versions of partial security by requiring either the correctness or privacy condition of perfect security to hold. Let Π be a partial SSS for an access structure Γ. We say that Π is a *partially-correct* scheme for Γ if $\Phi_\Pi(B) = 0$, for every unqualified set $B \in \Gamma^c$; that is, unqualified sets gain no information about the secret. Similarly, we say that Π is a *partially-private* scheme for Γ if $\Phi_\Pi(A) = 1$, for every qualified set $A \in \Gamma$; that is, qualified sets fully recover the secret.

Another view on partial secret sharing: In perfect SSSs, 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 SSS is not perfect, it does not define an access structure. A partially-correct (resp. partially-private) SSS 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 (resp. full) amount of information about the secret. On the other hand, it might be possible to associate more than one access structure with a partial scheme, because the same scheme can be a partial SSS for different access structures. Therefore, partial security allows us to define the notion of access structure for a non-perfect SSS too.

B. Partial convec and partial information ratio

We quantify the efficiency of a partial scheme via a scaled version of its standard convec (Definition II.6), which we call *partial convec*. Clearly, unlike the standard convec of a scheme, which is defined on its own, the partial convec depends on the access structure that it partially realizes.

Definition IV.2 (Partial convec) *Let* Π *be a partial scheme for* Γ*. The* partial convec *of* Π *(with respect to* Γ*) is defined and denoted by*

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

where δ*, the (normalized) advantage, is defined as in Equation (IV.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 two concepts: (i) the capacity of Wyner's wiretap channel and (ii) a similar compensating factor in decomposition constructions. We will revisit these concepts in Section VI and Section VIII, respectively.

Another motivation for this definition (i.e., adding the factor of $\frac{1}{\delta}$) is that one can take any perfect SSS Π with secret random variable $\boldsymbol{S}_0$ and transform it into a partial secret sharing whose secret is $(\boldsymbol{S}_0, \boldsymbol{S}_0')$ (for any $\boldsymbol{S}_0'$ independent from Π), where given a secret (s_0, s_0') the partial scheme shares s_0 using the original scheme; we do not want such transformations to improve the information ratio of a scheme.

Partial information ratio: The partial information ratio of a SSS is defined to be the maximum coordinate of its partial convec. The partial information ratio of an access structure is the infimum of the partial information ratio of all SSSs that partially realize it. The partially-correct and partially-private information ratios are defined similarly. Additionally, one can discuss the linear and mixed-linear partial information ratios.

The weakest security notion: In the following, we prove that partial security is weaker than all non-perfect security notions mentioned in Section III. By relation (III.3) it suffices to show that:

$$\text{partial} \leqslant \text{quasi-perfect} \quad \text{(for any class of schemes)}\ . \tag{IV.3}$$

The reader may need to recall the definition of quasi-perfect security of Section III-B. We want to show that, for every class of SSSs, the partial information ratio of an access structure Γ is not larger than its quasi-perfect information ratio. To prove this claim, let $\{\Pi_m\}_{m\in\mathbb{N}}$ be a family of SSSs that quasi-perfectly realizes Γ. We show that $\{\Pi_m\}_{m\in\mathbb{N}}$ is also a family of partial SSSs for Γ such that

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

where $\mathrm{cv}(\Pi)$ and $\mathrm{pcv}(\Pi)$ stand for the standard and partial convecs of a SSS Π, as defined in Definitions II.6 and IV.2, respectively.

Recall the definition of the access function of a SSS (Definition II.5) and let

- $\lambda_m = \min_{A\in\Gamma}\{\Phi_{\Pi_m}(A)\}$ and,
- $\omega_m = \max_{B\notin\Gamma}\{\Phi_{\Pi_m}(B)\}$.

Since $\{\Pi_m\}_{m\in\mathbb{N}}$ quasi-perfectly realizes Γ, the sequences $\{\lambda_m\}$ and $\{\omega_m\}$ respectively converge to 1 and 0. Therefore, we have $\delta_k = \lambda_m - \omega_m > 0$ for sufficiently large m. This shows that Π_m is a partial SSS for Γ with partial convec $\mathrm{pcv}(\Pi_m) = \mathrm{cv}(\Pi_m)/\delta_m$. The claim then follows since $\delta_k \to 1$ as $m \to \infty$.

Relations between different information ratios: In Sections V, VI and VII, we will prove the following three results about partial information ratio:

$$\begin{aligned} \text{partial} &= \text{perfect} && \text{(for linear schemes)},\\ \text{partial} &= \text{statisticial} && \text{(for general schemes)},\\ \text{partially-correct} &\lneqq \text{almost-perfect} && \text{(for mixed-linear schemes)}. \end{aligned}$$

Notice the last relation holds for some access structure (we present one in Section VII) but the other ones hold for every access structure. This is a rare example of the power of imperfection in the efficiency of SSSs. It remains open to prove separation/coincidence between "partial and quasi-perfect" and "quasi-perfect and almost-perfect" information ratios for the class of mixed-linear schemes. However, the last relation shows that at least one of them is separated.

The first result shows that partial, partially-correct, and partially-private information ratios are all equal for the linear class. Also, a lemma by Kaced [13, Lemma 17] can be used to show that requiring perfect correctness does not lead to a stronger variant of partial security (for general schemes). However, it remains open if the following equalities hold for other classes of schemes such as mixed-linear, abelian or homomorphic schemes:

$$\begin{aligned} \text{partial} &= \text{partially-private} && \text{(for linear and general schemes)},\\ \text{partial} &= \text{partially-correct} && \text{(for linear schemes)}. \end{aligned}$$

In Example IV.6, using the known results on non-perfect CDS, we achieve a $\Theta(\log n)$ separation between the the partially-correct and partially-private information ratios for the case where the secret is a single bit; that is:

$$\text{partially-correct} \lneqq \text{partially-private}$$
$$\text{(for schemes with one-bit secrets)}.$$

However, for one-bit secrets, the separation between partially-private and perfect information ratios and also between partial and partially-correct information ratios are left open.

C. On choosing a fair criterion for efficiency

We remark that the scale factor $\frac{1}{\delta}$ in the definition of partial information ratio enables us to fairly compare the efficiency of an access structure with respect to partial and perfect security notions. In the following, we recall a non-trivial result, due to Beimel and Franklin [31], which shows that without the compensation factor $\frac{1}{\delta}$, it is possible to have very efficient partially-private schemes.

There is a somewhat relevant security notion to partially-private security called *weakly-private*. In a weakly-private SSS, the qualified sets are required to recover the secret with probability one, but for every unqualified set, it is only required that all secrets are probable; that is, an unqualified set can never rule out any secret. Weakly-private SSSs were first introduced in [64] and it was shown that weakly-ideal and (perfectly) ideal SSSs are equivalent. The notion was then studied in other works [31], [38], [65], [66]. In particular, Beimel and Franklin showed in [31] that for every access structure with n participants, it is possible to construct a weakly-private SSS with an ℓ-bit-long secret and $(\ell + n2^n)$-bit-long shares. We will describe their construction in Example IV.4. Since a weakly-private SSS is partially-private too[3], it follows that if we did not include the scale factor $\frac{1}{\delta}$ in the definition of partial information ratio, then the partial information ratio of every access structure would turn out to be one (since by choosing an arbitrarily large value for ℓ, the ratio $(\ell + n2^n)/\ell$ can be made arbitrarily close to one).

Recall that the best upper-bound on the information ratio of access structures with respect to perfect security is exponential. Therefore, the fact that the (standard) information ratio of weakly-private SSSs is so small may seem surprising (as it also surprised Beimel and Franklin in [31]). However, we will show in Example IV.4 that the partial information ratio of their construction is still exponential for almost all access structures.

D. Some examples

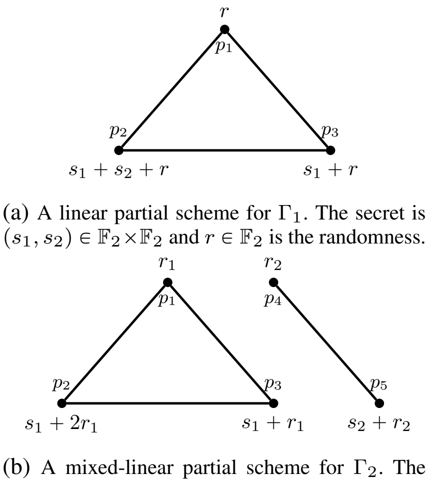
In this subsection, we present some examples of linear, mixed-linear, and non-linear partial SSSs.

Example IV.3 (Toy examples) *Consider the following two access structures:*

Γ_1 *on 3 participants with minimal qualified sets* $\{p_1, p_2\}, \{p_2, p_3\}, \{p_1, p_3\}$,

Γ_2 *on 5 participants with minimal qualified sets* $\{p_1, p_2\}, \{p_2, p_3\}, \{p_1, p_3\}, \{p_4, p_5\}$.

An access structure whose minimal qualified sets are all of size two can be represented by a graph. Fig. 1 shows a partial scheme for each of these access structures.



(a) A linear partial scheme for Γ_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 Γ_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 Γ_1 and Γ_2. All random variables are independent and uniform on their supports.

The scheme for Γ_1 *is linear, its secret contains two bits of information and every participant receives one bit of information as his share. The scheme for* Γ_2 *is mixed-linear and its secret contains* $\log 6 \approx 2.58$ *bits of information. The shares of*

[3] Semantically, it would be better if partially-private SSSs turned out stronger than weakly-private schemes.

participants p_4, p_5 are one bit each, and those of participants p_1, p_2, p_3 are $\log 3 \approx 1.58$ bits. The scheme for Γ_1 is partially-correct 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 Γ_2 is also partially-correct with advantage $\delta_2 = \frac{\log 2}{\log 6} \approx 0.387$.

Therefore, the partial information ratios of all participants in Γ_1 are $\frac{1}{\delta_1}\frac{1}{2} = 1$. The partial information ratios of participants p_1, p_2, p_3 in Γ_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 Γ_2 are both $\frac{1}{\delta_2}\frac{\log 2}{\log 6} = 1$.

Example IV.4 (A partially-private scheme) *Let Γ be an access structure on the participants set $\{p_1, \dots, p_n\}$. Beimel and Franklin [31] proposed the following weakly-private SSS for Γ, which by our discussion in Section IV-C is also partially-private.*

Given a uniformly chosen secret $s \in \{0,1\}^k$, do the following:

1) Choose a maximal unqualified subset $C \in \Gamma^c$ at random.
2) For every participant $p_i \in C$, choose a random string $r_i \in \{0,1\}^k$ and send it to him as a part of his share.
3) Send the secret s to every participant $p_i \in P \backslash C$ as a part of his share.
4) Encode the selected subset C as an n-bit string and then share it among the participants using a trivial perfect scheme with share size $n2^n$.

*The share size of every participant is $k + n2^n$ and therefore, the standard information ratio of the scheme is $1 + \frac{n2^n}{k}$, which can be arbitrarily close to one if k is chosen to be sufficiently large. However, the following claim shows that for almost all access structures, in particular for every $n/2$-*uniform *access structure, the partial information ratio of this scheme is exponential in n. An access structure is called t-uniform if every set of size $t-1$ or smaller is unqualified and every set of size $t+1$ or larger is qualified; the size-t subsets can be either qualified or unqualified. These access structures are known to have perfect SSSs with information ratio $\mathrm{O}(t^2)$ [50], only known to be achieved via exponentially-long secrets. But, the partial information ratio of the above scheme is $\Omega(n^{-3/4}2^{n/2})$ by this claim.*

Claim IV.5 *For $k \geqslant n$, the advantage of the above scheme is $\delta = \mathrm{O}(n^{3/4}2^{-n/2})$ for $2^{\binom{n}{n/2}}$ out of the total $2^{\binom{n}{n/2}(1+\mathrm{O}(\frac{\log n}{n}))}$ access structures on n participants.*

Proof: Let $\Pi = (\boldsymbol{S}_i) \in_{P \cup \{0\}}$ denote the SSS in Example IV.4 and let $B \in \Gamma^c$ be an arbitrary unqualified set. We need to find an upper-bound on $\mathrm{H}(\boldsymbol{S}_0 \mid \boldsymbol{S}_B)/\mathrm{H}(\boldsymbol{S}_0)$.

Define the following events, where C is the unqualified set chosen in the sharing phase:

- *B_0: $B = C$.*
- *B_1: $|B \backslash C| = 1$.*
- *B_2: $|B \backslash C| \geqslant 2$.*
- *D: All the elements of the vector $\boldsymbol{S}_{C \cup \{0\}}$ are distinct.*

Let $p_i = \Pr[B_i]$ and $q = \Pr[\overline{D}]$. Denote the number of maximal unqualified sets of Γ by M and notice that $M = \Omega(2^n/\sqrt{n})$. Clearly, we have $p_0 = \frac{1}{M}$ and $p_1 \leqslant \frac{n/2}{M}$. Also, by the birthday paradox, we have $q = \Pr[\overline{D}] \leqslant \frac{n/2(n/2+1)}{2^k} \leqslant \frac{n^2/2}{2^k}$ (assuming $n \geqslant 2$).

Let $\boldsymbol{D}$ denote the indicator random variable of the event D. That is, $\boldsymbol{D} = 1$ if D occurs and otherwise $\boldsymbol{D} = 0$. Let $\boldsymbol{B}$ be a random variable that is equal to i if B_i occurs.

It is easy to verify that for every $0 \leqslant p \leqslant 1$, we have $-p \log_2 p \leqslant 2\sqrt{p}$ and $-(1-p)\log_2(1-p) \leqslant 2p$. Therefore,

$$\begin{aligned}\mathrm{H}(\boldsymbol{B}) + \mathrm{H}(\boldsymbol{D}) \quad \leqslant \quad & \frac{2(1+\sqrt{n/2})}{\sqrt{M}} + \frac{2(n/2+1)}{2^{k/2}} \\ & + \frac{2(1+n/2)}{M} + \frac{n^2}{2^k}\ ,\end{aligned}$$

and hence,

$$\begin{aligned}\mathrm{H}(\boldsymbol{S}_0 \mid \boldsymbol{S}_A) \quad & \leqslant \quad \mathrm{H}(\boldsymbol{S}_0 \mid \boldsymbol{S}_A \boldsymbol{B}\boldsymbol{D}) + \mathrm{H}(\boldsymbol{B}) + \mathrm{H}(\boldsymbol{D}) \\ & = \quad \mathrm{H}(\boldsymbol{S}_0 \mid \boldsymbol{S}_A B_0)p_0 \\ & \qquad + \mathrm{H}(\boldsymbol{S}_0 \mid \boldsymbol{S}_A B_1)p_1 \\ & \qquad + \mathrm{H}(\boldsymbol{S}_0 \mid \boldsymbol{S}_A B_2 D)p_2(1-q) \\ & \qquad + \mathrm{H}(\boldsymbol{S}_0 \mid \boldsymbol{S}_A B_2 \overline{D})p_2 q \\ & \qquad + \mathrm{H}(\boldsymbol{B}) + \mathrm{H}(\boldsymbol{D}) \\ & \leqslant \quad kp_0 + (\log n)p_1 + kp_2 q + \mathrm{H}(\boldsymbol{B}) + \mathrm{H}(\boldsymbol{D}) \\ & \leqslant \quad k\frac{1}{M} + (\log n)\frac{n}{2M} + k\frac{n^2}{2^k} + \frac{2+\sqrt{2n}}{\sqrt{M}} \\ & \qquad + \frac{n+2}{2^{k/2}} + \frac{2+n}{M} + \frac{n^2}{2^k}\ .\end{aligned}$$

It follows that when $k \geqslant n$, we have $\mathrm{H}(\boldsymbol{S}_0 \mid \boldsymbol{S}_B)/\mathrm{H}(\boldsymbol{S}_0) = \mathrm{O}(n^{3/4}2^{-n/2})$, which completes the proof. ■

We remark that analyzing the advantage for $1 \leqslant k < n$ in the above claim seems harder. However, the advantage becomes intuitively even worse.

Example IV.6 (Non-perfect CDS and secret sharing) *Applebaum and Vasudevan [47] presented a partially-correct (called perfectly-private in [47]) CDS for k-bit secrets for the predicate $\mathrm{NEQ} : \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}$ defined by $\mathrm{NEQ}(x,y) = 1$ iff $x \neq y$. The communication complexity of their protocol is $\Theta(k)$ whereas that of the perfect CDS for one-bit secrets is known to be $\Theta(n)$. Here, we explain their results in terms of SSS terminology.*

Let $P = \{1, \dots, n\}$ be a set of participants (n even) and define the following 2-uniform access structure (also called forbidden graph access structure) and denote it by Γ_{NEQ}. A size-two subset $\{x, y\}$ is unqualified iff $y - x = n/2$. All singleton subsets are unqualified and all size-3 subsets are qualified.

Now consider the following SSS with k-bit secret s, interpreted as an element of the finite filed $\mathbb{F}_{2^k}$: the share of every participant $x \in P$ is $\big(h(x), h(x)s + r\big)$, where r is a random element of $\mathbb{F}_{2^k}$ and $h : [n] \mapsto \mathbb{F}_{2^k}$ is chosen uniformly from a family of pair-wise independent hash functions (i.e., for every $x \neq y$ it holds that $\big(h(x), h(y)\big)$ is uniform over $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ for the random choice of h).

It is easy to verify that this scheme is a partially-correct scheme for Γ_{NEQ} with advantage $\delta = (1 - 2^{-k})$ and, hence, partial information ratio $2/\delta$. For one-bit secrets (i.e., when $k = 1$), we have a partially-correct scheme with the partial information ratio 4 whereas the best achievable information *ratio for perfect schemes is $\Theta(\log n)$. Nevertheless, for exponentially long secrets, both partial and perfect information ratios are $\Theta(1)$; because, as we already mentioned, the information ratio of t-uniform access structures is polynomial in t. For polynomial-length secrets (i.e., when $k = \mathrm{poly}(n)$), it remains open whether partial schemes outperform perfect schemes for Γ_{NEQ}.*

V. Equality of perfect and partial linear information ratios

In this section, we prove that the partial linear information ratio of an access structure is equal to its perfect linear information ratio. Two linear algebraic lemmas lie at the core of our proof which are presented in Section V-A. The first one is used in Section V-B for transforming a partially-correct 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 V-C.

A. Two linear algebraic lemmas

Let $\mathbb{F}$ be a finite field and $x_1, \ldots, x_\lambda \in \mathbb{F}^m$ be linearly independent vectors. The following lemma essentially states that there exist linear mappings $L_1, \ldots, L_m : \mathbb{F}^m \to \mathbb{F}^{\lambda m}$ such that the collection $\{L_j(x_i) : i \in [\lambda], j \in [m]\}$ of vectors in $\mathbb{F}^{\lambda m}$ is linearly independent.

Lemma V.1 (Linear mappings) *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 λ linearly independent vectors $x_1, \ldots, x_\lambda \in \mathbb{F}^m$, the λm 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 mapping $x \longmapsto x^q$ is an $\mathbb{F}$-linear map from $\mathbb{K}$ to $\mathbb{K}$; this is the famous Frobenius map and the key is the following two properties: $(x+y)^q = x^q + y^q$ and $a^q = a$ for $x, y \in \mathbb{K}$ and $a \in \mathbb{F}$. Also, $x \longmapsto x^{q^i}$ 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 $c_{i,j}$, $i \in [m]$ and $j \in [\lambda]$, such that $\Sigma_{j=1}^{\lambda} \Sigma_{i=1}^{m} c_{i,j} L_i(x_j) = 0$, then $\sum_{j=1}^{\lambda} (\sum_{i=1}^{m} c_{i,j} w_i) x_j^{q^{k-1}} = 0$ 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 $\sum_{i=1}^{m} c_{i,j} w_i = 0$ for all $j \in [\lambda]$ and thus $c_{i,j} = 0$, 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 $M = \left(x_i^{q^{k-1}}\right)_{i \in [\lambda], k \in [\lambda]}$ 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^λ 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 the 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 V.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 ω, $1 \leqslant \omega < m$. If $N < \frac{q^m - 1}{q^{m-1} - 1}$, then there exists 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 there are 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. ■

B. Constructing a convec-preserving perfect linear scheme from a partially-correct linear scheme

The following proposition will be generalized in the next subsection. However, we present it separately in this subsection since we will extend its proof in the course of the proof of Proposition V.4. We recall that the standard and partial convecs of a secret sharing scheme Π are denoted by $\mathrm{cv}(\Pi)$ and $\mathrm{pcv}(\Pi)$, respectively; see Definitions II.6 and IV.2.

Proposition V.3 (Partially-correct $\Longrightarrow$ Perfect) *Let Γ be an access structure and Π' be a partially-correct $\mathbb{F}$-linear secret sharing scheme for it. Then, there exists a perfect $\mathbb{F}$-linear secret sharing scheme Π for Γ such that $\mathrm{cv}(\Pi) = \mathrm{pcv}(\Pi')$.*

Construction: We now show how to construct Π from Π'. Identify the secret space of Π' by $\mathbb{F}^m$. Since Π' is a partially-correct scheme for Γ, there exists an integer λ, with $1 \leqslant \lambda \leqslant m$, such that every qualified set of participants discovers at least λ independent linear relations on the secret, and there exists a qualified set that recovers exactly λ such relations. Our construction is a generalization of the one described in Section **??** for the case where $\lambda = 1$. In that case, the secret space of the constructed scheme Π was $\mathbb{F}^m$. For the general case, we let the secret space of Π be $\mathbb{F}^{\lambda m}$. 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 Π', where L_i's are $m \times m\lambda$ matrices representing the linear mappings in Lemma V.1. Each participant in Π receives a share from each instance of Π'. Hence, while the secret length has been multiplied by λ, the share of each participant has increased by a factor of m. Therefore, the standard convec of Π and partial convec of Π' are equal. Note that since the m instances of Π' use independent randomnesses, the secret remains hidden from every unqualified set. By Lemma V.1, each qualified set gets λm independent linear relations on s. We conclude that the scheme Π is perfect.

In the following, we prove Proposition V.3 more formally.

Proof Proposition V.3: Let $\Pi' = (T'; T'_0, T'_1, \ldots, T'_n)$ be the $\mathbb{F}$-linear partially-correct 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 V.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 $\mathrm{cv}(\Pi) \leq \mathrm{pcv}(\Pi')$. It is straightforward to tweak the scheme such that the claimed vector equality holds. It remains to prove that Π perfectly realizes Γ.

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

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

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 V.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 Π is a perfect scheme for Γ. ■

C. Constructing a convec-preserving perfect linear scheme from a partial linear scheme

The following proposition is a generalization of Proposition V.3. The proof essentially follows the same lines as that of Proposition V.3. We will need Lemma V.2 to argue about the privacy of the constructed scheme, which is "almost" the same as the previous one. The difference is due to the fact that Lemma V.2 holds for sufficiently large finite fields; therefore, we first need to "lift" the scheme into a larger field and then apply the construction described in Section V-B.

Proposition V.4 (Partial $\Longrightarrow$ Perfect) *Let Γ be an access structure and Π' 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 Π for Γ 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

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

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

Let N be the number of maximal unqualified subsets in Γ^c and $\mathbb{K}$ be an extension of $\mathbb{F}$ that satisfies $|\mathbb{K}| \geqslant N$. By the process of extending scalars, we can turn Π' 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 Π' is considered to be a $\mathbb{K}$-linear scheme. In particular, the relations for λ, ω, m are still valid.

Construct $(T_0, \ldots, T_n)$ from Π' the same way as in the proof of Proposition V.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 V.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 V.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 Γ such that $\dim S = (\lambda - \omega)m$. Therefore, $\mathrm{cv}(\Pi) \leq \mathrm{pcv}(\Pi')$. Again, it is straightforward to tweak the scheme such that the convec equality holds. ■

On the secret length blow-up: Given a partial linear scheme whose secret length is $m \log|\mathbb{F}|$ bits, the construction of Section V-B results in a perfect scheme with the secret length $\lambda m \log|\mathbb{F}| = \mathrm{O}(m^2 \log|\mathbb{F}|)$. The construction of this section, however, results in a perfect scheme with the secret length $(\lambda - \omega)m \log|\mathbb{K}| = \mathrm{O}(m^2 \max(\log N, \log|\mathbb{F}|)$, where N is the number of minimal unqualified sets.

VI. Equality of statistical and partial information ratios

In this section, we prove the following theorem.

Theorem VI.1 (partial=statistical) *Let* Γ *be an access structure.*

(I) If there exists a partial SSS for Γ *with partial information ratio* σ*, then there exists a family of statistical SSSs for* Γ *with information ratio* σ *and linear secret length growth.*

(II) If there exists a family of partial SSS for Γ *such that the sequence of their partial information ratios converges to* σ*, then there exists a family of statistical SSSs for* Γ *with information ratio* σ *and quadratic secret length growth.*

The proof of (I) is achieved by viewing a partial SSS as a wiretap channel and a careful analysis of its near-capacity behavior. We remark that (I) does not immediately imply (II) and its proof has more subtleties that may not be clear at a first glance (e.g., see Remark VI.4).

In Section VI-A, we review the definition of Wyner's wiretap channel and study its near-capacity behavior in Section VI-B. The proof of the theorem will be given in Section VI-C.

A. The wiretap channel

In this subsection, we recall the notion of *wiretap channel*, first introduced by Wyner [14] in 1975 and further developed by Csiszár and Körner [33] in 1978. A wiretap channel is defined in terms of a conditional probability distribution function. Here, we start with a joint distribution and study its associated wiretap channel. The original description was given for a single receiver and single eavesdropper. Below, we present the description for the multi-receiver multi-eavesdropper channel.

Let $\Sigma = \big(\boldsymbol{X}, (\boldsymbol{Y}_i)_{i\in\mathcal{R}}, (\boldsymbol{Z}_j)_{j\in\mathcal{E}}\big)$ be a tuple of random variables. We refer to the tuple $\mathrm{WTC}_\Sigma = \big(p, \mathcal{X}, (\mathcal{Y}_i)_{i\in\mathcal{R}}, (\mathcal{Z}_j)_{j\in\mathcal{E}}\big)$ as the wiretap channel associated to Σ where $p(\cdot,\cdot|\cdot)$ is the (conditional) probability distribution of the random variable $\big((\boldsymbol{Y}_i)_{i\in\mathcal{R}}, (\boldsymbol{Z}_j)_{j\in\mathcal{E}}\big)$ when conditioned on $\boldsymbol{X}$. That is,

$$p(\cdot,\cdot|\cdot) : \prod_{i\in\mathcal{R}} \mathcal{Y}_i \times \prod_{j\in\mathcal{E}} \mathcal{Z}_j \times \mathcal{X} \to [0,1] \ ,$$

where

$$p((y_i)_{i\in\mathcal{R}}, (z_j)_{j\in\mathcal{E}}|x) := \Pr\left[\begin{array}{c} (\boldsymbol{Y}_i)_{i\in\mathcal{R}} = (y_i)_{i\in\mathcal{R}}, \\ (\boldsymbol{Z}_j)_{j\in\mathcal{E}} = (z_j)_{j\in\mathcal{E}} \end{array} |\boldsymbol{X} = x\right] .$$

A wiretap channel models a point-to-point communication system between a sender, a set of (legitimate) receivers with index set $\mathcal{R}$ and a set of eavesdroppers with index set $\mathcal{E}$. When the sender transmits a message $x \in \mathcal{X}$ through the channel, according to the conditional distribution p, each receiver $i \in \mathcal{R}$ obtains a message $y_i \in \mathcal{Y}_i$ and each eavesdropper $j \in \mathcal{E}$ gets a message $z_j \in \mathcal{Z}_j$.

The goal of the sender is to reliably transmit a long message to the receivers (i.e., at a high rate) by using m independent instances of the channel while keeping it secret from the eavesdroppers. To this end, the sender uses a well-designed encoder and receivers use their own decoders to obtain the message (see Fig. 2).

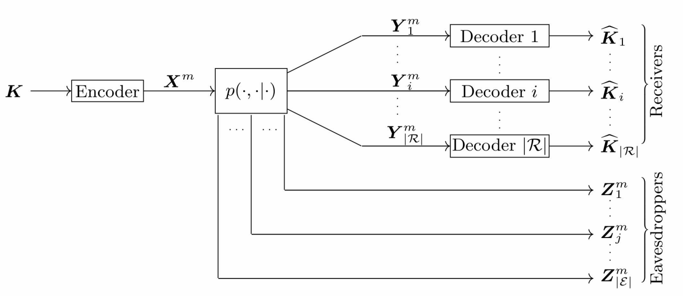


Fig. 2: A schematic of a wiretap channel with receivers $\mathcal{R} = \{1, \ldots, |\mathcal{R}|\}$ and eavesdroppers $\mathcal{E} = \{1, \ldots, |\mathcal{E}|\}$.

Formally, an encoder is a publicly-known probabilistic algorithm

$$\mathrm{Enc} : \mathcal{K} \to \mathcal{X}^m \ ,$$

and the ith decoder is a deterministic algorithm

$$\mathrm{Dec}_i : \mathcal{Y}_i^m \to \mathcal{K} \ ,$$

where $\mathcal{K}$ stands for the set of messages. To transmit a uniformly chosen message $k \in \mathcal{K}$, the sender first encodes it to obtain a tuple $x^m = (x_1, \ldots, x_m) \leftarrow \mathrm{Enc}(k)$. Then each symbol $x_k \in \mathcal{X}$ is independently transmitted through the channel. The receiver i and eavesdropper j then accordingly receive a tuple $y_i^m = (y_{i1}, \ldots, y_{im})$ and $z_j^m = (z_{j1}, \ldots, z_{jm})$, respectively. Each receiver i then uses his/her own decoder to compute a message $\widehat{k}_i \in \mathcal{K}$.

Let $\boldsymbol{K}, \boldsymbol{X}^m, \boldsymbol{Y}_i^m, \boldsymbol{Z}_j^m$ denote the random variables for the encoder's input, the encoder's output (i.e., channel's input), the ith receiver's input and the jth eavesdropper's input, respectively. In Fig. 2, the ith decoder's output is denoted by $\widehat{\boldsymbol{K}}_i$.

We say that a *rate* $R \geqslant 0$ is achievable if for every m there exist an encoder and decoders such that:

(i) **Rate.** The RV $\boldsymbol{K}$ is uniformly distributed on $\mathcal{K} = \{1, \ldots, e^{mR}\}$.

(ii) **Reliability.** For every receiver $i \in \mathcal{R}$, the (average) decoding error probability $\Pr[\mathrm{Dec}_i(\boldsymbol{K}) \neq \boldsymbol{K}]$ is negligible in m.

(iii) **Privacy.** For every eavesdropper $j \in \mathcal{E}$, the (average) statistical distance $\mathrm{SD}(p_{\boldsymbol{Z}_j^m\boldsymbol{K}}, p_{\boldsymbol{Z}_j^m}p_{\boldsymbol{K}})$ is negligible in m.

The *secrecy capacity* of the wiretap channel WTC_Σ, associated to the distribution $\Sigma = \big(\boldsymbol{X}, (\boldsymbol{Y}_i)_{i\in\mathcal{R}}, (\boldsymbol{Z}_j)_{j\in\mathcal{E}}\big)$, is defined to be the supremum of all achievable rates. Except for the case of single-receiver single-eavesdropper [33], the secrecy capacity of the wiretap channel is an open problem. However, the following lower-bound on the secrecy capacity of the wiretap channel associated with Σ is known and enough for our purpose:

$$C_\Sigma = \min_{i\in\mathcal{R}} \mathrm{I}(\boldsymbol{X} : \boldsymbol{Y}_i) - \max_{j\in\mathcal{E}} \mathrm{I}(\boldsymbol{X} : \boldsymbol{Z}_j) \ . \tag{VI.1}$$

Assuming $C_\Sigma > 0$, it can be proved that every (fixed) rate $R < C_\Sigma$ is achievable (e.g., see [20]). However, to prove the main result of this section (Theorem VI.1), we need a careful analysis of the near-capacity behavior of the wiretap channel, to be studied in Section VI-B.

Stronger reliability and privacy requirements: Notice that, similar to the definition of expected-statistical security for secret sharing (Section III-A), the reliability and privacy conditions in items (ii) and (iii) require that the error probability $\Pr[\mathrm{Dec}_i(\boldsymbol{K}) \neq \boldsymbol{K}]$ and statistical distance $\mathrm{SD}(p_{\boldsymbol{Z}_j^m \boldsymbol{K}}, p_{\boldsymbol{Z}_j^m} p_{\boldsymbol{K}})$ be negligible on the average (see relations (III.1) and (III.2)).

Similar to the definition of statistical secret sharing, we can consider the following stronger requirements:

(ii') **Strong reliability.** For every receiver $i \in \mathcal{R}$ and every message $k \in \mathcal{K}$, the decoding error probability $\Pr[\mathrm{Dec}_i(\boldsymbol{K}) \neq \boldsymbol{K} | \boldsymbol{K} = k]$ is negligible in m.

(iii') **Strong privacy.** For every eavesdropper $j \in \mathcal{E}$ and every message $k \in \mathcal{K}$, the statistical distance $\mathrm{SD}(p_{\boldsymbol{Z}_j^m|\boldsymbol{K}=k}, p_{\boldsymbol{Z}_j^m})$ is negligible in m.

It is folklore that the capacity remains invariant with respect to both definitions. Here, we present a proof for completeness. Let $R > 0$ be a fixed achievable rate with respect to requirements (ii) and (iii). We show that it is also achievable by requirements (ii') and (iii'). This can be shown by discarding the worst messages and keeping only the best $\frac{1}{e}$ fraction, for each receiver (in terms of the probability of error) and each eavesdropper (in terms of the statistical distance); hence, reducing the message size by a factor of at most $e^{-(|\mathcal{R}|+|\mathcal{E}|)}$. By using the union-bound and Markov inequality, it follows that there exists a subset $\mathcal{K}' \subseteq \{1, \ldots, e^{mR}\}$ of size at least $e^{mR-(|\mathcal{R}|+|\mathcal{E}|)}$ such that for every $k \in \mathcal{K}'$, for every receiver $i \in \mathcal{R}$, and for every eavesdropper $j \in \mathcal{E}$, we have:

$$\begin{aligned} \Pr[\mathrm{Dec}_i(\boldsymbol{K}) \neq \boldsymbol{K} | \boldsymbol{K} = k] &\leqslant 2 \Pr[\mathrm{Dec}_i(\boldsymbol{K}) \neq \boldsymbol{K}] \ , \\ \mathrm{SD}(p_{\boldsymbol{Z}_j^m|\boldsymbol{K}=k}, p_{\boldsymbol{Z}_j^m}) &\leqslant 2\mathrm{SD}(p_{\boldsymbol{Z}_j^m \boldsymbol{K}}, p_{\boldsymbol{Z}_j^m} p_{\boldsymbol{K}}) \ . \end{aligned} \tag{VI.2}$$

Consequently, the rate $\lim_{m\to\infty} \big(mR - (|\mathcal{R}|+|\mathcal{E}|)\big)/m = R$ is also achievable with requirements (ii') and (iii'). When R may depend on m, if the rate R is achievable for the weaker definition, so is the rate $R - O(\frac{1}{m})$ for the stronger definition.

B. Near-capacity behavior of the wiretap channel

In this subsection, we show that the rate $R = C_\Sigma - \Theta(\frac{1}{m^{1/4}})$ is achievable; i.e., the reliability and privacy errors are (exponentially) negligible. We remark that there is nothing special about the exponent $\frac{1}{4}$ and any positive exponent (strictly) smaller than $\frac{1}{2}$ works fine.

Let us first describe how the encoder of the wiretap channel works. To encode a message $k \in \mathcal{K} = \{1, \ldots, e^{mR}\}$, with $R < C_\Sigma$, the encoder chooses a uniform random index $\ell \in \mathcal{L} = \{1, \ldots, e^{m\tilde{R}}\}$ and outputs $h(k, l)$, where

$$h : \mathcal{K} \times \mathcal{L} \to \mathcal{X}^m$$

is a randomly chosen hash function, known to every party and $\tilde{R}$, satisfying

$$\max_{j\in\mathcal{E}} \mathrm{I}(\boldsymbol{X} : \boldsymbol{Z}_j) < \tilde{R} < \min_{i\in\mathcal{R}} \mathrm{I}(\boldsymbol{X} : \boldsymbol{Y}_i) - R \ ,$$

is some parameter that will be set at the end. Every receiver decodes using the *maximum-likelihood criterion*.

- **Reliability analysis.** Using [67, Theorem 13], for every receiver $i \in \mathcal{R}$, we have:

  $$\Pr[\mathrm{Dec}_i(\boldsymbol{K}) \neq \boldsymbol{K}] \leqslant \exp\left(-m\rho\big(\mathrm{I}_{\frac{1}{1+\rho}}(\boldsymbol{X} : \boldsymbol{Y}_i) - R - \tilde{R}\big)\right) ,$$

  for every $\rho \in (0,1)$, which may be considered as a function of m too. Here, I_α is the α-Rényi mutual information according to Csiszár's proposal (see [67, Eq. 29]). The following Taylor expansion holds

  $$\mathrm{I}_{\frac{1}{1+\rho}}(\boldsymbol{X} : \boldsymbol{Y}_i) = \mathrm{I}(\boldsymbol{X} : \boldsymbol{Y}_i) - \rho \mathrm{I}_1'(\boldsymbol{X} : \boldsymbol{Y}_i) + \mathrm{O}(\rho^2) \ ,$$

  where I_1' is the derivative of I_α at $\alpha = 1$ whose value is irrelevant for us. It can be shown that I_α is non-decreasing and differentiable for discrete random variables with finite supports.
  If we let $R + \tilde{R} = \min_{i\in\mathcal{R}} \mathrm{I}_{\frac{1}{1+\rho}}(\boldsymbol{X} : \boldsymbol{Y}_i) - \rho$, for every receiver $i \in \mathcal{R}$, we get $\Pr[\mathrm{Dec}_i(\boldsymbol{K}) \neq \boldsymbol{K}] \leqslant \exp(-m\rho^2)$. In particular, letting $\rho = m^{-\frac{1}{4}}$, we have $\Pr[\mathrm{Dec}_i(\boldsymbol{K}) \neq \boldsymbol{K}] \leqslant \exp(-\sqrt{m})$, for

  $$R + \tilde{R} = \min_{i\in\mathcal{R}} \mathrm{I}(\boldsymbol{X} : \boldsymbol{Y}_i) - \Theta(m^{-\frac{1}{4}}) \ . \tag{VI.3}$$

- **Privacy analysis.** By [68, Theorem 1], for every eavesdropper $j \in \mathcal{E}$, we have

  $$\mathrm{SD}(p_{\boldsymbol{Z}_j^m \boldsymbol{K}}, p_{\boldsymbol{Z}_j^m} p_{\boldsymbol{K}}) \leqslant \frac{3}{2} \exp\left(-m\rho\big(\tilde{R} - \mathrm{I}_{\frac{1}{1-\rho}}(\boldsymbol{X} : \boldsymbol{Z}_j)\big)\right) ,$$

  for every $\rho \in (0, \frac{1}{2})$, which may be considered as a function of m too. Since

  $$\mathrm{I}_{\frac{1}{1-\rho}}(\boldsymbol{X} : \boldsymbol{Z}_j) = \mathrm{I}(\boldsymbol{X} : \boldsymbol{Z}_j) + \rho \mathrm{I}_1'(\boldsymbol{X} : \boldsymbol{Z}_j) + \mathrm{O}(\rho^2) \ ,$$

  by letting $\tilde{R} = \max_{j\in\mathcal{E}} \mathrm{I}_{\frac{1}{1-\rho}}(\boldsymbol{X} : \boldsymbol{Z}_j) + \rho$, for every eavesdropper $j \in \mathcal{E}$, we get $\mathrm{SD}(p_{\boldsymbol{Z}_j^m \boldsymbol{K}}, p_{\boldsymbol{Z}_j^m} p_{\boldsymbol{K}}) \leqslant \frac{3}{2} \exp(-m\rho^2)$. In particular, letting $\rho = m^{-\frac{1}{4}}$, we have $\mathrm{SD}(p_{\boldsymbol{Z}_j^m \boldsymbol{K}}, p_{\boldsymbol{Z}_j^m} p_{\boldsymbol{K}}) \leqslant \frac{3}{2} \exp(-\sqrt{m})$, for

  $$\tilde{R} = \max_{j\in\mathcal{R}} \mathrm{I}(\boldsymbol{X} : \boldsymbol{Z}_j) + \Theta(m^{-\frac{1}{4}}) \ . \tag{VI.4}$$

We remark that in the analysis, we assumed that the hash function is random and known to every party. Indeed, it can be shown that there is a fixed choice for the hash function with exponentially negligible reliability and privacy errors.

To summarize, by relations (VI.3) and (VI.4) and our discussion at the end of Section VI-A (see relation VI.2), we have the following result.

Theorem VI.2 *For every wiretap channel with strong reliability and privacy requirements (i.e., requirements (ii') and (iii')), the rate $R = C_\Sigma - \Theta(\frac{1}{m^{1/4}})$ is achievable with the upper-bound $3\exp(-\sqrt{m})$ for both the reliability and privacy errors.*

Notice that our upper-bound on the reliability and privacy errors is independent of the channel parameters. This turns out crucial in the next subsection (see Remark VI.4).

C. Proof of Theorem VI.1

We first present an overview of the proof of part (I). Given the partial SSS Π for Γ, we construct a statistical family for it as follows. When a secret is shared using Π among the participants, it can be viewed as transmitting the secret through a wiretap channel in which, each qualified subset of participants is considered a receiver, and each unqualified subset of participants can be treated as an eavesdropper. The sender (dealer) can use this channel to send reliably a secret that can be recovered by the receivers (i.e., qualified sets) and remains hidden from the eavesdroppers (i.e., unqualified sets). It is then easy to verify that all the requirements for statistical realization are satisfied.

Proof of part (I): from a partial scheme to a statistical family: Given a partial SSS $\Pi = (\boldsymbol{S}_0, \boldsymbol{S}_1, \ldots, \boldsymbol{S}_n)$ with nominal capacity C_Π, we construct a statistical family $\{\Pi^m\}_{m\in\mathbb{N}}$ for Γ with convec $\operatorname{pcv}(\Pi) = \frac{\operatorname{cv}(\Pi)}{C_\Pi}$, where $\Pi^m = (\boldsymbol{T}_0^m, \boldsymbol{T}_1^m, \ldots, \boldsymbol{T}_n^m)$. Let

$$\Sigma = \big(\boldsymbol{X}, (\boldsymbol{Y}_i)_{i\in\Gamma}, (\boldsymbol{Z}_j)_{j\in\Gamma^c}\big) := \big(\boldsymbol{S}_0, (\boldsymbol{S}_A)_{A\in\Gamma}, (\boldsymbol{S}_B)_{B\in\Gamma^c}\big) \ ,$$

and consider the associated wiretap channel. By (IV.2) and (VI.1), $C_\Sigma = C_\Pi$ and therefore, by Theorem VI.2, the rate $R = C_\Pi - \Theta(m^{-\frac{1}{4}})$, is achievable. Let $\boldsymbol{K}$ be a uniform random variable on $\{1, \ldots, e^{mR}\}$ and

$$\operatorname{Enc} : \mathcal{K} \to \mathcal{X}^m = \big(\operatorname{supp}(\boldsymbol{S}_0)\big)^m \ ,$$

be the encoder mentioned in Section VI-A.

The secret random variable of the scheme Π^m is $\boldsymbol{T}_0^m = \boldsymbol{K}$. To share a secret $s \in \operatorname{supp}(\boldsymbol{K})$, we first compute a random encoding $(s_1, \ldots, s_m) \leftarrow \operatorname{Enc}(s)$ and then share every secret $s_k \in \operatorname{supp}(\boldsymbol{S}_0)$, $k \in [m]$, independently using Π. The share of the ith participant is the collection of all shares that he receives from each scheme, which we denote by the random variable $\boldsymbol{T}_i^m$. It is easy to verify that all the requirements for statistical security hold (see Section III-A). In particular, the linear secret length growth holds because:

$$\log|\operatorname{supp}(\boldsymbol{T}_0^m)| \leqslant C_\Pi m \ . \tag{VI.5}$$

The proof of the claim on the information ratio follows by the following relations, where $i \in [n]$ is some participant such that $\{i\}$ is a qualified set (the unqualified case is similar):

$$\begin{aligned}
\lim_{m\to\infty} \frac{\mathrm{H}(\boldsymbol{T}_i^m)}{\mathrm{H}(\boldsymbol{T}_0^m)} &= \lim_{m\to\infty} \frac{\mathrm{H}(\boldsymbol{Y}_i^m)}{\mathrm{H}(\boldsymbol{K})} \\
&= \lim_{m\to\infty} \frac{\mathrm{H}(\boldsymbol{Y}_i^m)}{m\big(C_\Pi - \Theta(m^{-\frac{1}{4}})\big)} = \frac{\mathrm{H}(\boldsymbol{Y}_i)}{C_\Pi} \\
&= \frac{\mathrm{H}(\boldsymbol{S}_i)}{C_\Pi} \ .
\end{aligned} \tag{VI.6}$$

Here we have used the relation $\lim_{m\to\infty} \dfrac{1}{m}\mathrm{H}(\boldsymbol{Y}_i^m) = \mathrm{H}(\boldsymbol{Y}_i)$, which is known to hold for a wiretap channel.

Finlay, by Theorem VI.2,

$$\delta(m) = 3\exp(-\sqrt{m}) \ , \tag{VI.7}$$

is an upper-bound on both the reconstruction probability of error and the statistical distance of the constructed family $\{\Pi^m\}_{m\in\mathbb{N}}$. ■

Proof of part (II): from a partial family to a statistical family: The following lemma is useful for proving the second part.

Lemma VI.3 *Let $\{\sigma_k\}_{k\in\mathbb{N}}$ and $\{c_k\}_{k\in\mathbb{N}}$ be a sequences of non-negative real numbers such that $\lim\limits_{k\to\infty} \sigma_k = \sigma$. Let $\{\sigma_{k,m}\}_{m\in\mathbb{N}}$, $\{\ell_{k,m}\}_{m\in\mathbb{N}}$, $\{\varepsilon_{k,m}\}_{m\in\mathbb{N}}$ be sequences and $\delta(m)$ be a negligible function such that for each k we have*

$$\lim_{m\to\infty} \sigma_{k,m} = \sigma_k \ ,$$

$$\ell_{k,m} \leqslant c_k m \ ,$$

$$\varepsilon_{k,m} \leqslant \delta(m) \ .$$

Then, there exists $\mu : \mathbb{N} \mapsto \mathbb{N}$ such that:

$$\lim_{m\to\infty} \sigma_{\mu(m),m} = \sigma \ ,$$

$$\ell_{\mu(m),m} < m^2 \ ,$$

and $\varepsilon_{\mu(m),m}$ is negligible.

Proof: Since $\lim\limits_{m\to\infty} \sigma_{k,m} = \sigma_k$, there exists M_k such that for all $m \geqslant M_k$ it holds that $|\sigma_{k,m} - \sigma_k| < \frac{1}{k}$. Let

$$d_k = \max\{c_1, \ldots, c_k, M_1, \ldots, M_k\} + k \ .$$

Then $\{d_k\}_{k\in\mathbb{N}}$ is increasing and it goes to infinity as $k \to \infty$. Define

$$\mu(m) = i \text{ if } d_i \leqslant m < d_{i+1}$$

and define $\mu(m) = 1$ if $m < d_1$. Then, $\{\mu(m)\}_{m\in\mathbb{N}}$ is non-decreasing and it goes to infinity as $m \to \infty$. Note that $m \geqslant d_{\mu(m)} > c_{\mu(m)}$ and, therefore, $\ell_{\mu(m),m} < m^2$. Also, for every $m \geqslant d_{\mu(m)} > M_{\mu(m)}$, we have $|\sigma_{\mu(m),m} - \sigma_{\mu(m)}| < \frac{1}{\mu(m)}$. This implies that $\lim\limits_{m\to\infty} \sigma_{\mu(m),m} = \lim\limits_{m\to\infty} \sigma_{\mu(m)} = \sigma$ since $\mu(m) \to \infty$ as $m \to \infty$. It is trivial that $\varepsilon_{\mu(m),m}$ is negligible. ■

Now let us prove part (II). Let $\{\Pi_k\}_{k\in\mathbb{N}}$ be a family of partial schemes for Γ. Denote the partial information ratio of Π_k by σ_k and let $\lim\limits_{k\to\infty} \sigma_k = \sigma$.

Let $\{\Pi_k^m\}_{m\in\mathbb{N}}$ be the statistical family which by part (I) is promised to exist for the partial scheme Π_k. Denote the information ratio of Π_k^m by $\sigma_{k,m}$, and thus $\lim\limits_{m\to\infty} \sigma_{k,m} = \sigma_k$.

Let $c_k = C_{\Pi_k}$ and denote the secret length of Π_k^m by $\ell_{k,m}$. Thus by relation (VI.5), we have $\ell_{k,m} \leqslant c_k m$.

Let $\varepsilon_{k,m}$ be the maximum of these two values: the reconstruction probability of error and the statistical distance of the family $\{\Pi_k^m\}_{m\in\mathbb{N}}$. Notice that by relation (VI.7), $\varepsilon_{k,m} \leqslant \delta(m) = 3\exp(-\sqrt{m})$.

Now, the conditions of Lemma VI.3 (with the same notations) are satisfied. Let μ be the function whose existence is guaranteed by the lemma. It then follows that $\{\Pi_{\mu(m)}^m\}_{m\in\mathbb{N}}$ is a statistical family for Γ with quadratic secret length growth and information ratio σ. ■

Remark VI.4 (On the subtleties of proving part II) *We were lucky to achieve an exponentially negligible upper-bound* *for the reliability and privacy errors of a wiretap channel, which is independent of the parameters of the channel (Theorem VI.2). If this would not be the case, then we could have been in trouble proving part (II) of the theorem. The reason is that Lemma VI.3 does not hold if we replace $\delta(m)$ with $\delta_k(m)$, where $\{\delta_k(m)\}_{k\in\mathbb{N}}$ is a family of negligible functions.*

VII. Separating almost-perfect and partial mixed-linear information ratios

The equality of perfect and partial linear information ratios was proved in Section V. In this section, we show that for the $\mathcal{F}+\mathcal{N}$ access structure, introduced in [69] and further studied in [7], the partial and perfect information ratios do not necessarily match for the class of mixed-linear schemes. By relation (I.1), it then follows that the almost-perfect and partial information ratios are separated for this class.

A. The access structure $\mathcal{F}+\mathcal{N}$

We study $\mathcal{F}+\mathcal{N}$, a well-known access structure [69, page 2641] with 12 participants which has both Fano ($\mathcal{F}$) and non-Fano ($\mathcal{N}$) access structures as minors. Both $\mathcal{F}$ and $\mathcal{N}$ have six participants. The Fano access structure has the following seven minimal qualified sets:

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

and the non-Fano access structure has the following eight minimal qualified sets:

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

The access structure $\mathcal{F}$ (resp. $\mathcal{N}$) is the port of the Fano (resp. non-Fano) matroid and it is known [70] 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:

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

where s, r_1, r_2 are all uniformly and independently 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, it realizes $\mathcal{N}$.

The minimal qualified sets of the access structure $\mathcal{F}+\mathcal{N}$, with 12 participants, is the union of the minimal qualified sets of $\mathcal{F}$ and $\mathcal{N}$ (the parties in $\mathcal{N}$ are renamed from $p_1,\ldots,p_6$ 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* [69]. Recently, in [7], 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 linear ones.

Below, we construct a family of partially-correct mixed-linear schemes for this access structure with partial information ratio one. Table I summarizes the known results about the $\mathcal{F}+\mathcal{N}$ access structure. For completeness, we also include the result for other non-perfect security notions.

B. A nearly-ideal partially-correct mixed-linear scheme for $\mathcal{F}+\mathcal{N}$

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

The secret space of the m'th scheme is $\mathbb{F}_{2^m}\times\mathbb{F}_{q_1}\times\cdots\times\mathbb{F}_{q_\ell}$. We share a secret $(s',s_1,\cdots,s_\ell)$, where $s'\in\mathbb{F}_{2^m}$ 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 partially-correct with the advantage $\delta=\frac{\log 2^m}{\log 2^m+\log(2^m+1)}$. 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 $\frac{\log(2^m+1)}{\log 2^m}$. That is, the m'th scheme is partially-correct for $\mathcal{F}+\mathcal{N}$ and its partial information ratio approaches one as $m\to\infty$.

TABLE I: 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).

		almost-perfect statistical	quasi-perfect	partial	reference
general	max	1			[69]
	avg				
mixed-linear	max	7/6	$1\leqslant\cdot\leqslant\frac{7}{6}$	1	[7] Eq. (I.1) Sect. VII-B
	avg	41/36	$1\leqslant\cdot\leqslant\frac{41}{36}$		
linear	max	4/3			Eq. (I.1), Eq. (I.4) [7]
	avg	41/36			

It remains open to prove the separation or coincidence of "partial and quasi-perfect" or "quasi-perfect and almost-perfect" information ratios for the class of mixed-linear schemes. However, the result of this section shows that there is at least one case of separation.

VIII. On decomposition techniques

Decomposition techniques are useful to construct SSSs for a given access structure by combining several (usually simple) schemes. For example, the optimal linear schemes for several graph access structures on six participants, which had remained an open problem for a long time, were constructed using these methods in [22]. Suitable decompositions can be found using *linear programming techniques* (see [34], [39]). In [44], a recursive method has been used to systemically find all optimal linear schemes for all access structures on five participants and all graph access structures on six participants.

Decomposition techniques have two varieties. Weighted decompositions [21], [22] allow non-perfect subschemes but require them to be linear. One caveat of the constructions in [21], [22] is that they need the linear subschemes to satisfy an additional requirement but, in Section VIII-A, we will show that it can be relaxed. Non-weighted-decompositions [34], [35] allow non-linear subschemes but require them to be perfect.

In Section VIII-B, we present a unified decomposition theorem, that we refer to as the δ-decomposition, which incorporates both weighted and non-weighted decompositions.

The existence of a more general decomposition theorem for perfect security that allows general subschemes (i.e., linear or non-linear, perfect or non-perfect) remains an open problem. However, we will present a general decomposition theorem for statistical security in Section VIII-C.

A. Weighted-(λ,ω)-decomposition revisited

The following definition is a restatement of Definition 3.4 in [22].

Definition VIII.1 ($(\boldsymbol{\lambda},\boldsymbol{\omega})$–weighted decomposition) *Let $\lambda,\omega,N,m_1,\cdots,m_N$, be non-negative integers, with $0\leqslant\omega<\lambda$. Let Γ be an access structure and $\Phi_1,\dots,\Phi_N$ be (rational-valued) access functions all defined on the same set of participants and further assume that $m_j\Phi_j$ is an integer-valued function for every $j\in[N]$. We call $(m_1,\Phi_1),\dots,(m_N,\Phi_N)$ a weighted-(λ,ω)-decomposition for Γ 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-(λ,ω)-decomposition theorem of [22, Theorem 3.2] (as well as its predecessor [21]) has the following limitation. It requires that in the linear subschemes 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 achieved using a ramp SSS. In the following theorem, we remove this strong requirement. Its proof uses the notion of partial secret sharing and the result of Section V on the equality of partial and perfect linear information ratios.

Theorem VIII.2 ($(\boldsymbol{\lambda},\boldsymbol{\omega})$–weighted-decomposition theorem) *Let Γ be an access structure and $(m_1,\Phi_1),\dots,(m_N,\Phi_N)$ be a weighted-(λ,ω)-decomposition for it. If for each $j\in[N]$, the access function Φ_j has a linear SSS with convec σ_j, such that their field characteristics are all the same, then Γ has a linear scheme with convec $\frac{1}{\lambda-\omega}\sum_{j=1}^N m_j\sigma_j$.*

Proof: Let $\Pi_j=(T_{i,j})_{i\in P\cup\{0\}}$ be a linear SSS for Φ_j with convec σ_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 $T'_i=\oplus_{j\in[N]}T_{i,j}$ and denote $\Pi'=(T'_i)_{i\in P\cup\{0\}}$. We have $\dim T'_i=\sum_{j\in[N]}\dim T_{i,j}$ 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 (λ,ω)–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, Π' is an $\mathbb{F}$-linear partial SSS for Γ with the following partial convec:

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

Then, by Proposition V.4, there exists a finite extension $\mathbb{K}$ of $\mathbb{F}$, such that Γ has a perfect $\mathbb{K}$-linear scheme Π with the above convec. It is straightforward to modify the scheme, by adding dummy shares, to have a scheme with convec $\frac{1}{\lambda-\omega}\sum_{j=1}^N m_j\sigma_j$. ■

B. δ-decomposition for perfect security

We present the notion of δ-decomposition, which incorporates all weighted and non-weighted decompositions [21], [22], [34], [35], simultaneously (even in a more general form since we allow the coefficients to be real numbers).

Definition VIII.3 ($\boldsymbol{\delta}$-decomposition) *Let N be an integer and $h_1,\dots,h_N$ be non-negative real numbers. Let Γ be an access structure and $\Phi_1,\dots,\Phi_N$ be access functions all on the same set of participants. We say that $(h_1,\Phi_1),\dots,(h_N,\Phi_N)$ is a δ–decomposition for Γ 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 subschemes in (λ,ω)-weighted decomposition need to be linear and, consequently, the subaccess functions Φ_j's must be *rational-valued*. In the (non-weighted) (λ,ω)-decomposition [35], however, the subschemes can be linear or non-linear but they must be perfect. Consequently, the subaccess functions must be *all-or-nothing* (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 straightforward and, hence, omitted.

Theorem VIII.4 ($\boldsymbol{\delta}$-decomposition for perfect security) *Let Γ be an access structure and $(h_1,\Phi_1),\dots,(h_N,\Phi_N)$ be a δ–decomposition for it. Then:*

(i) ***(Rational/Linear)*** *If each Φ_j is a rational-valued access function and realizable by a linear SSSs with convec σ_j, such that all the underlying finite fields have the same*

characteristic, then Γ is realizable by a family of linear schemes with convec $\frac{1}{\delta}\sum_{j=1}^{N} h_j\sigma_j$.

(ii) ***(All-or-nothing/Non-linear)*** *If each Φ_j is all-or-nothing (i.e., 0-1-valued) and realizable by a (linear or non-linear) SSSs with convec σ_j, then Γ is realizable by a family of SSSs with convec $\frac{1}{\delta}\sum_{j=1}^{N} h_j\sigma_j$.*

It remains unknown if there exists a general decomposition theorem with the advantages of both weighted and non-weighted decompositions. In the next subsection, we present such a decomposition for all non-perfect security notions.

C. δ-decomposition for non-perfect security notions

The δ-decomposition for perfect security only allows two restricted classes of subschemes. The following decomposition theorem for partial security does not impose any restriction on the subschemes (i.e., they can be linear or non-linear, perfect or non-perfect).

Theorem VIII.5 (δ-decomposition for partial security) *Let Γ be an access structure and $(h_1,\Phi_1),\dots,(h_N,\Phi_N)$ be a δ–decomposition for it. If each Φ_j is realizable by a SSS with convec σ_j, then Γ is realizable by a family of partial SSSs with partial convec $\frac{1}{\delta}\sum_{j=1}^{N} h_j\sigma_j$.*

Proof: Let $\Pi_j = (\boldsymbol{S}_i^j)_{i\in Q}$ be a SSS for Φ_j. We first prove the theorem under the assumption that $h_j/\mathrm{H}(\boldsymbol{S}_0^j)$ is a rational number for every $j \in [N]$. The general case then follows by standard techniques (i.e., considering a converging sequence of rational numbers to each value). Let L be an integer such that for every $j \in [N]$, the number $M_j := \frac{Lh_j}{\mathrm{H}(\boldsymbol{S}_0^j)}$ is an integer.

For every $j \in [N]$ and every $k \in [M_j]$, let $\Pi_{j,k} = (\boldsymbol{S}_i^{j,k})_{i\in Q}$ be an independent instance of Π_j. Consider the SSS

$$\Pi = (\boldsymbol{S}_i)_{i\in Q} \quad \text{with} \quad \boldsymbol{S}_i = \left(\boldsymbol{S}_i^{j,k}\right)_{j\in[N],k\in[M_j]} \ .$$

By independence of different instances of SSSs, for every $i \in Q$ we have

$$\mathrm{H}(\boldsymbol{S}_i) = \textstyle\sum_{j=1}^{N} M_j \mathrm{H}(\boldsymbol{S}_i^j) = \sum_{j=1}^{N} \frac{Lh_j}{\mathrm{H}(\boldsymbol{S}_0^j)}\mathrm{H}(\boldsymbol{S}_i^j) \quad .$$

In particular, $\mathrm{H}(\boldsymbol{S}_0) = L\sum_{j=1}^{N} h_j$. It then follows that

$$\mathrm{cv}(\Pi) = \frac{1}{\sum_{j=1}^{N} h_j}\sum_{j=1}^{N} h_j \mathrm{cv}(\Pi_j) \ .$$

and

$$\begin{array}{rcl} \mathrm{I}(\boldsymbol{S}_0 : \boldsymbol{S}_A) & = & \sum_{j=1}^{N} M_j \mathrm{I}(\boldsymbol{S}_0^j : \boldsymbol{S}_A^j) \\ & = & \sum_{j=1}^{N} \frac{Lh_j}{\mathrm{H}(\boldsymbol{S}_0^j)}\mathrm{I}(\boldsymbol{S}_0^j : \boldsymbol{S}_A^j) \\ & = & L\sum_{j=1}^{N} h_j \Phi_{\Pi_j}(A) \\ & = & L\sum_{j=1}^{N} h_j \Phi_j(A) \ . \end{array} \ .$$

Consequently,

$$\Phi_\Pi(A) = \frac{1}{\sum_{j=1}^{N} h_j}\sum_{j=1}^{N} h_j \Phi_j(A) \ .$$

Since $(h_1,\Phi_1),\dots,(h_N,\Phi_N)$ is a δ–decomposition for Γ, by definition, it then follows that Π is a partial scheme for it with advantage $\delta' = \frac{\delta}{\sum_{j=1}^{N} h_j}$. Therefore, we have $\mathrm{pcv}(\Pi) = \frac{1}{\delta'}\mathrm{cv}(\Pi) = \frac{1}{\delta}\sum_{j=1}^{N} h_j \mathrm{cv}(\Pi_j)$

When $h_j/\mathrm{H}(\boldsymbol{S}_0^j)$ is not a rational number for every $j \in [N]$, by considering a converging sequence of rational numbers to each value, a family of partial schemes can be constructed whose partial information ratio converges to $\frac{1}{\delta}\sum_{j=1}^{N} h_j \mathrm{cv}(\Pi_j)$. ■

It is not clear how one can extend the notion of partial and statistical security to access functions. In Section III-B, we defined the notion of quasi-perfect realization for an access structure by a family of schemes. The definition straightforwardly extends to access functions. We say that a family $\{\Pi_m\}_{m\in\mathbb{N}}$ of SSSs *quasi-perfectly realizes an access function* Φ if $\lim\limits_{m\to\infty} \Phi_{\Pi_m} = \Phi$ (this definition is equivalent to realization by *almost-entropic polymatroid*; see [11], [12] and also Appendix A).

Theorem VIII.6, together with Theorem VI.1, leads to a general decomposition theorem for all non-perfect (i.e., quasi-perfect, almost-perfect, and statistical) security notions. Below, we present the statement for the strongest, i.e., statistical security. On the other hand, we consider the weakest security notion for the subschemes; i.e., quasi-perfect security.

Theorem VIII.6 (δ-decomposition for statistical security) *Let Γ be an access structure and $(h_1,\Phi_1),\dots,(h_N,\Phi_N)$ be a δ–decomposition for it. If each Φ_j is quasi-perfectly realizable by a family of SSSs with convec σ_j, then Γ is statistically realizable by a family of SSSs with convec $\frac{1}{\delta}\sum_{j=1}^{N} h_j\sigma_j$.*

IX. Conclusion

In this paper, we introduced a new relaxed security notion for SSSs, called partial security. The partially-private and partially-correct variants are more relaxed than weakly-private [31] and weakly-correct security [32] notions, respectively. However, unlike the latter two security notions, which consider the standard information ratio as a criterion for efficiency, we introduced a new parameter called partial information ratio. We proved that, in terms of partial information ratio, partial security coincides with perfect security for linear schemes and with statistical security for general schemes. The first result helped us remove a strong requirement for linear subschemes in weighted decompositions [21], [22]. More interestingly, the second result leads to a very strong decomposition theorem for statistical security.

Our third result was a rare example demonstrating the superiority of partial schemes to perfect schemes for the particular class of mixed-linear schemes (recently introduced in [7]). Nevertheless, currently, there is no proof for the superiority of non-perfect SSSs to perfect ones for general schemes (however, some evidence was presented by Beimel and Ishai in [10] for short secrets). Beimel and Franklin made an attempt in [31], by presenting a weakly-private SSS with the standard information ratio equal to one for every access structure. However, we showed that the partial information ratio of their construction is exponential for almost all access structures. Nevertheless, the existence of partial schemes with sub-exponential partial information ratio is not ruled out (unless Beimel's conjecture [55] turns out to be true for both perfect and statistical security notions).

Applebaum and Vasudevan's result [47] on non-perfect CDS shows that for one-bit secrets, partially-correct schemes outperform partially-private (and hence perfect) schemes and they achieved a $\Theta(\log n)$ separation for share size. It remains open if such a result holds for information ratio too (i.e., for arbitrarily-long secrets including exponentially-long ones). It is also an interesting question to see if a super-logarithmic separation can be achieved for one-bit secrets.

Finally, it is also an interesting question to see if a super-constant separation can be achieved for one-bit secrets between partially-private and perfect schemes. Again, Beimel and Ishai's result on statistical secret sharing with perfect correctness [10, Section 4.1.] provides some support that it might even be possible to achieve an exponential separation.

Appendix A
Csirmaz's proof for "quasi-perfect = almost-perfect"

As we mentioned in the introduction, in the context of the secret key agreement, advanced concepts (such as privacy amplification) are used to attain strong security from weak security (the counterparts of almost-perfect and quasi-perfect security in secret sharing). Here, we present a simple argument, suggested by Laszlo Csirmaz, for the equality of quasi-perfect and almost-perfect information ratios.

Let Q be a finite set called the *ground set*. A *polymatroid* on the ground set Q is a mapping $f : 2^Q \to \mathbb{R}$ that satisfies: i) $f(\varnothing) = 0$, ii) monotonicity, i.e., $f(A) \leqslant f(B)$ for every $A \subseteq B \subseteq Q$ and iii) submodularity; i.e., $f(A \cup B) \leqslant f(A) + f(B) - f(A \cap B)$, for every $A, B \subseteq Q$.

A polymatroid is called *entropic* if there exists a vector of random variables $(\boldsymbol{S}_i)_{i \in Q}$ such that $f(A) = \mathrm{H}(\boldsymbol{S}_A)$ for every subset $A \subseteq Q$. Ignoring the empty-set, a polymatroid can be identified by a $(2^{|Q|} - 1)$-dimensional point in the Euclidean space.

The set of all entropic polymatroids is called the *entropy region* [25]. The following facts are known about this set. First, its closure (in the usual Euclidean topology) is convex. Second, the interior points of the closure are entropic, meaning that the closure adds only boundary points (in other words there is no "holes" inside the entropy region). Third, the closure is a cone: one can multiply all coordinates by any positive number and remain in the closure; in other words, a multiple of an interior point is also an interior point. The first result was proved by Zhang and Yeung [25] and the latter two by Matús [71].

A SSS on participants set P can be identified with an entropic polymatroid on the ground set $Q = P \cup \{0\}$. The notion of realization of an access structure, or more generally an access function, by SSSs extends to polymatroids in a straightforward way [30]. A polymatroid f with ground set $P \cup \{0\}$ is said to realize an access function Φ on participants set P if $\Phi(A) = \big(f(\{0\}) + f(A) - f(A \cup \{0\})\big)/f(\{0\})$, for every $A \subseteq P$. The information ratio of f is defined to be $\max_{i \in P} f(\{i\})/f(\{0\})$.

Here we informally explain why almost-perfect and quasi-perfect information ratios are equal. For almost-perfect realization, we require realization by a point (polymatroid) inside or on the boundary of the entropy region. Such points are called *almost-entropic*. By the second property of the entropy region, in every neighborhood of an almost-entropic polymatroid, there is an entropic point (i.e., a genuine SSS). If the distance (in the usual Euclidean L_2 norm) between an almost-entropic and an entropic polymatroid is sufficiently small, they realize almost the same access function and have almost equal information ratios. For quasi-perfect security, we consider the normalization of the point by the secret entropy and we require that a normalized point lies inside or on the boundary. By the third property of the entropy region (i.e. the closure is a cone), normalization does not matter; thus, this notion is equivalent to almost-perfect security with respect to the information ratio.

Acknowledgment

The authors would like to thank anonymous reviewers for their constructive feedback that substantially helped shape our work. We are grateful to Mohammad Hossein Yassaee, Amin A. Gohari, and Laszlo Csirmaz for useful discussions. The second author has been supported by Iran National Science Foundation (INSF) Grant No. 99025148.

References

[1] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979. [Online]. Available: http://doi.acm.org/10.1145/359168.359176

[2] G. R. Blakley, "Safeguarding cryptographic keys," *Proc. of the National Computer Conference1979*, vol. 48, pp. 313–317, 1979.

[3] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, vol. 72, no. 9, pp. 56–64, 1989.

[4] E. F. Brickell and D. R. Stinson, "Some improved bounds on the information rate of perfect secret sharing schemes," *J. Cryptology*, vol. 5, no. 3, pp. 153–166, 1992. [Online]. Available: http://dx.doi.org/10.1007/BF02451112

[5] C. Blundo, A. D. Santis, D. R. Stinson, and U. Vaccaro, "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*, 1992, pp. 1–24. [Online]. Available: http://dx.doi.org/10.1007/3-540-47555-9_1

[6] K. M. Martin, "New secret sharing schemes from old," *J. Combin. Math. Combin. Comput*, vol. 14, pp. 65–77, 1993.

[7] A. Jafari and S. Khazaei, "On abelian and homomorphic secret sharing schemes," *J. Cryptol.*, vol. 34, no. 4, p. 43, 2021. [Online]. Available: https://doi.org/10.1007/s00145-021-09410-2

[8] T. H. Chan and R. W. Yeung, "On a relation between information inequalities and group theory," *IEEE Trans. Information Theory*, vol. 48, no. 7, pp. 1992–1995, 2002. [Online]. Available: https://doi.org/10.1109/TIT.2002.1013138

[9] R. Kaboli, S. Khazaei, and M. Parviz, "On group-characterizability of homomorphic secret sharing schemes," *Theor. Comput. Sci.*, vol. 891, pp. 116–130, 2021. [Online]. Available: https://doi.org/10.1016/j.tcs.2021.08.032

[10] A. Beimel and Y. Ishai, "On the power of nonlinear secret-sharing," in *Proceedings of the 16th Annual IEEE Conference on Computational Complexity, Chicago, Illinois, USA, June 18-21, 2001*, 2001, pp. 188–202. [Online]. Available: https://doi.org/10.1109/CCC.2001.933886

[11] T. Kaced, "Information inequalities are not closed under polymatroid duality," *IEEE Trans. Information Theory*, vol. 64, no. 6, pp. 4379–4381, 2018. [Online]. Available: https://doi.org/10.1109/TIT.2018.2823328

[12] L. Csirmaz, "Secret sharing and duality," *CoRR*, vol. abs/1909.13663, 2019. [Online]. Available: http://arxiv.org/abs/1909.13663

[13] T. Kaced, "Secret sharing and algorithmic information theory. (partage de secret et the'orie algorithmique de l'information)," Ph.D. dissertation, Montpellier 2 University, France, 2012. [Online]. Available: https://tel.archives-ouvertes.fr/tel-00763117

[14] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975. [Online]. Available: https://doi.org/10.1002/j.1538-7305.1975.tb02040.x

[15] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, 1993. [Online]. Available: https://doi.org/10.1109/18.256484

[16] ——, "The strong secret key rate of discrete random triples," in *Communications and Cryptography*. Springer, 1994, pp. 271–285.

[17] I. Csiszár, "Almost independence and secrecy capacity," *Problemy Peredachi Informatsii*, vol. 32, no. 1, pp. 48–57, 1996.

[18] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, 2000. [Online]. Available: https://doi.org/10.1109/18.825796

[19] U. M. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, 2000, pp. 351–368. [Online]. Available: https://doi.org/10.1007/3-540-45539-6_24

[20] M. H. Yassaee, M. R. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6760–6786, 2014. [Online]. Available: https://doi.org/10.1109/TIT.2014.2351812

[21] H.-M. Sun and B.-L. Chen, "Weighted decomposition construction for perfect secret sharing schemes," *Computers & Mathematics with Applications*, vol. 43, no. 6, pp. 877–887, 2002.

[22] M. Gharahi and S. Khazaei, "Optimal linear secret sharing schemes for graph access structures on six participants," *Theoretical Computer Science*, 2018. [Online]. Available: https://doi.org/10.1016/j.tcs.2018.11.007

[23] R. M. Capocelli, A. D. Santis, L. Gargano, and U. Vaccaro, "On the size of shares for secret sharing schemes," *J. Cryptology*, vol. 6, no. 3, pp. 157–167, 1993. [Online]. Available: https://doi.org/10.1007/BF00198463

[24] L. Csirmaz, "The size of a share must be large," *J. Cryptology*, vol. 10, no. 4, pp. 223–231, 1997. [Online]. Available: https://doi.org/10.1007/s001459900029

[25] Z. Zhang and R. W. Yeung, "A non-shannon-type conditional inequality of information quantities," *IEEE Trans. Information Theory*, vol. 43, no. 6, pp. 1982–1986, 1997. [Online]. Available: https://doi.org/10.1109/18.641561

[26] A. Beimel, N. Livne, and C. Padró, "Matroids can be far from ideal secret sharing," in *Theory of Cryptography, Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008.*, 2008, pp. 194–212. [Online]. Available: https://doi.org/10.1007/978-3-540-78524-8_12

[27] O. Farràs, T. Kaced, S. M. Molleví, and C. Padró, "Improving the linear programming technique in the search for lower bounds in secret sharing," in *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*, 2018, pp. 597–621. [Online]. Available: https://doi.org/10.1007/978-3-319-78381-9_22

[28] E. Gürpinar and A. E. Romashchenko, "How to use undiscovered information inequalities: Direct applications of the copy lemma," in *IEEE International Symposium on Information Theory, ISIT 2019, Paris, France, July 7-12, 2019*. IEEE, 2019, pp. 1377–1381. [Online]. Available: https://doi.org/10.1109/ISIT.2019.8849309

[29] W. Jackson and K. M. Martin, "Geometric secret sharing schemes and their duals," *Des. Codes Cryptography*, vol. 4, no. 1, pp. 83–95, 1994. [Online]. Available: https://doi.org/10.1007/BF01388562

[30] O. Farràs, T. B. Hansen, T. Kaced, and C. Padró, "On the information ratio of non-perfect secret sharing schemes," *Algorithmica*, vol. 79, no. 4, pp. 987–1013, 2017. [Online]. Available: https://doi.org/10.1007/s00453-016-0217-9

[31] A. Beimel and M. K. Franklin, "Weakly-private secret sharing schemes," in *Theory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007, Proceedings*, 2007, pp. 253–272. [Online]. Available: https://doi.org/10.1007/978-3-540-70936-7_14

[32] P. D'Arco, R. D. Prisco, A. D. Santis, A. L. P. del Pozo, and U. Vaccaro, "Probabilistic secret sharing," in *43rd International Symposium on Mathematical Foundations of Computer Science, MFCS 2018, August 27-31, 2018, Liverpool, UK*, 2018, pp. 64:1–64:16. [Online]. Available: https://doi.org/10.4230/LIPIcs.MFCS.2018.64

[33] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978. [Online]. Available: https://doi.org/10.1109/TIT.1978.1055892

[34] D. R. Stinson, "Decomposition constructions for secret-sharing schemes," *IEEE Transactions on Information Theory*, vol. 40, no. 1, pp. 118–125, 1994.

[35] M. van Dijk, W. Jackson, and K. M. Martin, "A general decomposition construction for incomplete secret sharing schemes," *Des. Codes Cryptography*, vol. 15, no. 3, pp. 301–321, 1998. [Online]. Available: https://doi.org/10.1023/A:1008381427667

[36] L. Lai, Y. Liang, W. Du, and S. Shamai, "Secret sharing via noisy broadcast channels," in *2011 IEEE International Symposium on Information Theory Proceedings, ISIT 2011, St. Petersburg, Russia, July 31 - August 5, 2011*, 2011, pp. 1955–1959. [Online]. Available: https://doi.org/10.1109/ISIT.2011.6033894

[37] S. Zou, Y. Liang, L. Lai, and S. Shamai, "An information theoretic approach to secret sharing," *IEEE Trans. Inf. Theory*, vol. 61, no. 6, pp. 3121–3136, 2015. [Online]. Available: https://doi.org/10.1109/TIT.2015.2421905

[38] A. Beimel and N. Livne, "On matroids and non-ideal secret sharing," in *Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006, Proceedings*, 2006, pp. 482–501. [Online]. Available: https://doi.org/10.1007/11681878_25

[39] M. Van Dijk, W.-A. Jackson, and K. M. Martin, "A general decomposition construction for incomplete secret sharing schemes," *Designs, Codes and Cryptography*, vol. 15, no. 3, pp. 301–321, 1998.

[40] M. van Dijk, T. A. M. Kevenaar, G. J. Schrijen, and P. Tuyls, "Improved constructions of secret sharing schemes by applying (lambda, omega)-decompositions," *Inf. Process. Lett.*, vol. 99, no. 4, pp. 154–157, 2006. [Online]. Available: https://doi.org/10.1016/j.ipl.2006.01.016

[41] M. Gharahi and M. Hadian Dehkordi, "Perfect secret sharing schemes for graph access structures on six participants," *Journal of Mathematical Cryptology*, vol. 7, no. 2, pp. 143–146, 2013.

[42] M. Gharahi, "On the complexity of perfect secret sharing schemes," *Ph. D. Thesis (in Persian)*, 2013.

[43] M. Gharahi and S. Khazaei, "Reduced access structures with four minimal qualified subsets on six participants," *Advances in Mathematics of Communications*, vol. 12, no. 1, pp. 199–214, 2018.

[44] S. Bahariyan, "A systematic approach for determining the linear convec set of small access structures (in persian)." Master's thesis, Sharif University of Technology, 2019.

[45] M. Van Dijk, "On the information rate of perfect secret sharing schemes," *Designs, Codes and Cryptography*, vol. 6, no. 2, pp. 143–169, 1995.

[46] W.-A. Jackson and K. M. Martin, "Perfect secret sharing schemes on five participants," *Designs, Codes and Cryptography*, vol. 9, no. 3, pp. 267–286, 1996.

[47] B. Applebaum and P. N. Vasudevan, "Placing conditional disclosure of secrets in the communication complexity universe," in *10th Innovations in Theoretical Computer Science Conference, ITCS 2019, January 10-12, 2019, San Diego, California, USA*, ser. LIPIcs, A. Blum, Ed., vol. 124. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019, pp. 4:1–4:14. [Online]. Available: https://doi.org/10.4230/LIPIcs.ITCS.2019.4

[48] B. Applebaum and O. Nir, "Upslices, downslices, and secret-sharing with complexity of 1.5^{n}," in *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part III*, ser. Lecture Notes in Computer Science, T. Malkin and C. Peikert, Eds., vol. 12827. Springer, 2021, pp. 627–655. [Online]. Available: https://doi.org/10.1007/978-3-030-84252-9_21

[49] T. Liu, V. Vaikuntanathan, and H. Wee, "Towards breaking the exponential barrier for general secret sharing," in *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*, ser. Lecture Notes in Computer Science, J. B. Nielsen and V. Rijmen, Eds., vol. 10820. Springer, 2018, pp. 567–596. [Online]. Available: https://doi.org/10.1007/978-3-319-78381-9_21

[50] B. Applebaum, A. Beimel, O. Farràs, O. Nir, and N. Peter, "Secret-sharing schemes for general and uniform

access structures," in *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, ser. Lecture Notes in Computer Science, Y. Ishai and V. Rijmen, Eds., vol. 11478. Springer, 2019, pp. 441–471. [Online]. Available: https://doi.org/10.1007/978-3-030-17659-4_15

[51] B. Applebaum, A. Beimel, O. Nir, and N. Peter, "Better secret-sharing via robust conditional disclosure of secrets," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 27, p. 8, 2020. [Online]. Available: https://eccc.weizmann.ac.il/report/2020/008

[52] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography - I: secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993. [Online]. Available: https://doi.org/10.1109/18.243431

[53] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, "Protecting data privacy in private information retrieval schemes," *J. Comput. Syst. Sci.*, vol. 60, no. 3, pp. 592–629, 2000. [Online]. Available: https://doi.org/10.1006/jcss.1999.1689

[54] B. Applebaum and B. Arkis, "On the power of amortization in secret sharing: d-uniform secret sharing and CDS with constant information rate," in *Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part I*, 2018, pp. 317–344. [Online]. Available: https://doi.org/10.1007/978-3-030-03807-6_12

[55] A. Beimel, "Secret-sharing schemes: A survey," in *Coding and Cryptology - Third International Workshop, IWCC 2011, Qingdao, China, May 30-June 3, 2011. Proceedings*, 2011, pp. 11–46. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-20901-7_2

[56] G. R. Blakley and C. Meadows, "Security of ramp schemes," in *Workshop on the Theory and Application of Cryptographic Techniques*. Springer, 1984, pp. 242–268.

[57] K. Kurosawa, K. Okada, K. Sakano, W. Ogata, and S. Tsujii, "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*, 1993, pp. 126–141. [Online]. Available: https://doi.org/10.1007/3-540-48285-7_11

[58] M. Karchmer and A. Wigderson, "On span programs," in *Proceedings of the Eigth Annual Structure in Complexity Theory Conference, San Diego, CA, USA, May 18-21, 1993*, 1993, pp. 102–111. [Online]. Available: https://doi.org/10.1109/SCT.1993.336536

[59] A. Beimel, A. Ben-Efraim, C. Padró, and I. Tyomkin, "Multi-linear secret-sharing schemes," in *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings*, 2014, pp. 394–418. [Online]. Available: https://doi.org/10.1007/978-3-642-54242-8_17

[60] D. Hammer, A. E. Romashchenko, A. Shen, and N. K. Vereshchagin, "Inequalities for shannon entropy and kolmogorov complexity," *J. Comput. Syst. Sci.*, vol. 60, no. 2, pp. 442–464, 2000. [Online]. Available: https://doi.org/10.1006/jcss.1999.1677

[61] M. Bertilsson and I. Ingemarsson, "A construction of practical secret sharing schemes using linear block codes," in *Advances in Cryptology - AUSCRYPT '92, Workshop on the Theory and Application of Cryptographic Techniques, Gold Coast, Queensland, Australia, December 13-16, 1992, Proceedings*, 1992, pp. 67–79. [Online]. Available: https://doi.org/10.1007/3-540-57220-1_53

[62] T. M. Cover and J. A. Thomas, *Elements of information theory (2. ed.)*. Wiley, 2006.

[63] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, 2004. [Online]. Available: https://doi.org/10.1109/TIT.2004.838380

[64] E. F. Brickell and D. M. Davenport, "On the classification of ideal secret sharing schemes," *J. Cryptology*, vol. 4, no. 2, pp. 123–134, 1991. [Online]. Available: https://doi.org/10.1007/BF00196772

[65] P. D. Seymour, "On secret-sharing matroids," *J. Comb. Theory, Ser. B*, vol. 56, no. 1, pp. 69–73, 1992. [Online]. Available: https://doi.org/10.1016/0095-8956(92)90007-K

[66] W.-A. Jackson and K. M. Martin, "Combinatorial models for perfect secret sharing schemes," *Journal of Combinatorial Mathematics and Combinatorial Computing*, vol. 28, pp. 249–266, 1998.

[67] S. Ho and S. Verdú, "Convexity/concavity of renyi entropy and α-mutual information," in *IEEE International Symposium on Information Theory, ISIT 2015, Hong Kong, China, June 14-19, 2015*. IEEE, 2015, pp. 745–749. [Online]. Available: https://doi.org/10.1109/ISIT.2015.7282554

[68] M. H. Yassaee, "Almost exact analysis of soft covering lemma via large deviation," in *IEEE International Symposium on Information Theory, ISIT 2019, Paris, France, July 7-12, 2019*. IEEE, 2019, pp. 1387–1391. [Online]. Available: https://doi.org/10.1109/ISIT.2019.8849341

[69] A. Beimel and N. Livne, "On matroids and nonideal secret sharing," *IEEE Trans. Information Theory*, vol. 54, no. 6, pp. 2626–2643, 2008. [Online]. Available: https://doi.org/10.1109/TIT.2008.921708

[70] F. Matús, "Matroid representations by partitions," *Discrete Mathematics*, vol. 203, no. 1-3, pp. 169–194, 1999. [Online]. Available: https://doi.org/10.1016/S0012-365X(99)00004-7

[71] ——, "Two constructions on limits of entropy functions," *IEEE Trans. Information Theory*, vol. 53, no. 1, pp. 320–330, 2007. [Online]. Available: https://doi.org/10.1109/TIT.2006.887090

Amir Jafari is an assistant professor at the Department of Mathematical Sciences at the Sharif University of Technology, Tehran, Iran. He received an M.Sc. in computer science and a Ph.D. in mathematics from Brown University in 2003. He has interests in algebraic geometry, combinatorics, and theoretical computer science.

Shahram Khazaei is an associate professor at the Department of Mathematical Sciences at the Sharif University of Technology, Tehran, Iran. He received a Ph.D. in computer science from EPFL, Switzerland, in 2011. After one year of postdoctoral research at KTH, Sweden, he joined the Sharif University of Technology as a faculty member in 2012. His principal interest and expertise are cryptography.