Almost-perfect secret sharing

Abstract

Splitting a secret s between several participants, we generate (for each value of s) shares for all participants. The goal: authorized groups of participants should be able to reconstruct the secret but forbidden ones get no information about it. In this paper we introduce several notions of *non-perfect* secret sharing, where some small information leak is permitted. We study its relation to the Kolmogorov complexity version of secret sharing (establishing some connection in both directions) and the effects of changing the secret size (showing that we can decrease the size of the secret and the information leak at the same time).

1 Secret sharing: a reminder

Assume that we want to share a secret – say, a bit string x of length n – between two people in such a way that they can reconstruct it together but none of them can do this in isolation. This is simple, choose a random string r of length n and give r and $r \oplus x$ to the participants ($r \oplus x$ is a bitwise XOR of x and r.) Both r and $r \oplus x$ in isolation are uniformly distributed among all n-bit strings, so they have no information about x.

The general setting for secret sharing can be described as follows. We consider some finite set $\mathcal{K}$ whose elements are called *secrets*. We also have a finite set $\mathcal{P}$ of *participants*. An *access structure* is a non-empty set Γ whose elements are groups of participants, i.e., a non-empty subset of $2^{\mathcal{P}}$. Elements of Γ are called *authorized* groups of participants (that should be able to reconstruct the secret). Other subsets of $\mathcal{P}$ are called *forbidden* groups (that should get no information about the secret). We always assume that Γ is upward-closed (it is natural since a bigger group knows more)[1].

In our initial example $\mathcal{K} = \mathbb{B}^n$ (the set of n-bit strings), $\mathcal{P} = \{1, 2\}$ (we have two participants labeled 1 and 2), and Γ consists of the set $\{1, 2\}$ only.

In general, *perfect secret sharing* can be defined as follows. For every participant $p \in \mathcal{P}$ a set $\mathcal{S}_p$ is fixed; its elements are p's *shares*. For every $k \in \mathcal{K}$ we have a tuple of $\#\mathcal{P}$ dependent random variables $\sigma_p \in \mathcal{S}_p$. There are two conditions:

- for every authorized set $A \in \Gamma$ it is possible to reconstruct uniquely the secret k from the shares given to participants in A (i.e., for different secrets k and k' the projections of the corresponding random tuples onto the A-coordinates have disjoint ranges);

- for every forbidden set $B \notin \Gamma$ the participants in B get no information about the secret (i.e., for different secrets k and k' the projections of the corresponding random tuples onto B-coordinates are identically distributed).

Various versions of combinatorial schemes were introduced in [5] and [6]. Note that in this definition we have no probability distribution on the set of secrets. It is natural for the setting when somebody gives us the secret (i.e., the user chooses her password) and we have to share whatever is given to us.

We consider another setting (as, first in [11] and further developed in [7]) where secret is also a random variable. Consider a family of random variables: one ($\varkappa$) for the secret and one (σ_p) for each participant p. This family is a perfect secret sharing scheme if

- for every authorized set A the projection $\sigma_A = \{\sigma_p, p \in A\}$ determines $\varkappa$;

- for every forbidden set B the projection σ_B is independent with $\varkappa$.

---

[1]One can also consider a more general setting where some groups are neither allowed nor forbidden (so there is no restriction on the information they may get about the secret.) We do not consider this more general setting here.

These conditions can be rewritten using Shannon information theory: the first condition says that $H(\varkappa|\sigma_A) = 0$, and the second says that $I(\sigma_B : \varkappa) = 0$. Here $H(\cdot|\cdot)$ stands for conditional Shannon entropy and $I(\cdot : \cdot)$ stands for mutual information. (To be exact, we should ignore events of probability zero when saying that σ_A determines $\varkappa$. To avoid these technicalities, let us agree that our probability space is finite and all non-empty events have positive probabilities.)

These definitions are closely related. Namely, it is easy to see that:

- Assume that a perfect secret sharing scheme in the sense of the first definition is given. Then for every distribution on secrets (random variable $\varkappa \in \mathcal{K}$) we get a scheme in the sense of the second definition as follows. For each secret $k \in \mathcal{K}$ we have a family of dependent random variables σ_p, and we use them as conditional distribution of participants' shares if $\varkappa = k$.

- Assume that a perfect secret sharing scheme in the sense of the second definition is given, and all secrets have positive probability according to $\varkappa$. Then the conditional distributions of σ_p with the condition $\varkappa = k$ form a scheme in the sense of the first definition.

This equivalence shows that in the second version of the definition the distribution on secrets is irrelevant (as far as all element in $\mathcal{K}$ have positive probability): we can change $\varkappa$ keeping the conditional distributions, and still have a perfect secret sharing scheme. The advantage of the second definition is that we can use standard techniques from Shannon information theory (e.g., information inequalities).

The general task of secret sharing can now be described as follows: given a set of secrets $\mathcal{K}$ and an access structure Γ construct a secret sharing scheme. This is always possible (see [4, 10]). However, the problem becomes much more difficult if we limit the size of shares. It is known (see [7]) that in the non-degenerate case shares should be at least of the same size as the secret: $\#\mathcal{S}_p \geq \#\mathcal{K}$ for every essential participant p. (A participant is *essential* if we remove it from some authorized group and get a forbidden group. Evidently, non-essential participants can be just ignored.) This motivates the notion of *ideal* secret sharing scheme where $\#\mathcal{S}_p = \#K$ for every essential participant p.

Historically, the motivating example for secret sharing was Shamir's scheme (see [17]). It has n participants, authorized groups are groups of t or more participants (where t is an arbitrary threshold). Secrets are elements of a finite field $\mathbb{F}$ of size greater than n. To share a secret k, we construct a polynomial

$$P_k(x) = k + r_1 x + r_2 x^2 + \ldots + r_{t-1} x^{t-1}$$

where the r_i are chosen independently and uniformly. The shares are the values $P(x_1), \ldots, P(x_n)$ for distinct nonzero field elements $x_1, \ldots, x_n$ (for each participant a non-zero element of the field is fixed). Any t participants together can reconstruct the polynomial while for any $t - 1$ participants all combinations of shares are equally probable (for every k). This scheme is ideal.

Not every access structure allows an ideal secret sharing scheme. For example, no ideal scheme exists for four participants a, b, c, d where the authorized groups are $\{a, b\}$, $\{b, c\}$ and $\{c, d\}$ and all their supersets (see [4, 12]; it is shown there that every secret sharing scheme for this access structure satisfies $\log \#S_b + \log \#S_c \geq 3 \log \#\mathcal{K}$).

It is therefore natural to weaken the requirements a bit and to allow non-ideal secret sharing schemes still having shares of reasonable size. For example, we may fix some $\rho \geq 1$ and ask whether for a given access structure there exists a perfect secret sharing scheme where $\max_{p \in \mathcal{P}} \log \#S_p \leq \rho \log \#\mathcal{K}$. (The answer may depend on the size of $\mathcal{K}$.)

Unfortunately, not much is known about this. There are quite intricate lower bounds for different specific access structures (some proofs are based on non-Shannon inequalities for entropies of tuples of random variables, see [3, 15]). The best known lower bounds for sharing m-bit secrets (for some fixed access scheme) are still rather weak, like $\frac{n}{\log n} m$ (see [8]). On the other hand, the known upper bounds for general access structures are exponential in the number of participants (and rather simple, see [4, 10]).

2 Nonperfect secret sharing

In this paper we consider other possible relaxations of the requirements and introduce several versions of *almost-perfect* secret sharing. By this we mean that we allow limited "leaks" of information to forbidden groups of participants. We also consider schemes where authorized groups need some (small) additional information to reconstruct the secret. Such approximately-perfect schemes look quite natural from the

practical point of view. Also, the gain in flexibility may help overcome the difficulty of constructing efficient perfect schemes which seems related to difficult problems of combinatorial or algebraic nature.

Let us discuss possible definitions for almost-perfect schemes. Now we want to measure the leak of information (or the amount of missing information), and the most natural way is to replace the equations $H(\varkappa|\sigma_A) = 0$ and $I(\sigma_B : \varkappa) = 0$ by inequalities $H(\ldots) < \varepsilon_1$ and $I(\ldots) < \varepsilon_2$, for some bounds ε_1 and ε_2 (normally, a small fraction of the amount of information in the secret itself).

The problem here is that measuring the information leak and missing information in this way, we need to fix some distribution on secrets, and this looks unavoidable even from the intuitive point of view. Imagine that we have 1000-bit secrets, and the sharing scheme works badly for secrets with 900 trailing zeros (e.g., discloses them to all participants). For the uniform distribution on secrets this does not mean a big information leak, since 100 leaked bits are multiplied by 2^{-900} probability to have 900 trailing zeros. However, if the secret is not chosen uniformly, e.g. the user chooses a short password padded with trailing zeros, the leak can become significant.

An interesting question (that we postpone for now) is how significant could be this dependence. One may expect that a good secret sharing scheme remains almost as good if we change slightly the distribution, but we cannot prove any natural statement of this kind. So we have to include the distribution on secrets in all the definitions.

Let Γ be an access structure. Let $\varkappa$ and σ_p (for all participants p) be some random variables (on the same probability space, so we may consider their joint distribution). Such a family is called a (not necessarily perfect) secret sharing scheme, and its parameters are:

- distribution on secrets (in particular, the entropy of $\varkappa$ is important);

- *information rate*, the maximal entropy of a single share divided by $H(\varkappa)$, the entropy of the secret;

- *missing information ratio*, the maximal value of $H(\varkappa|\sigma_A)$ for all authorized A, divided by $H(\varkappa)$;

- *information leak ratio*, the maximal value of $I(\sigma_B : \varkappa)$ for all forbidden B, divided by $H(\varkappa)$.

To simplify our statements, we consider asymptotic behaviors and give the following template definition of almost-perfect secret sharing:

Definition 2.1. *An access structure Γ on the set P of participants can be almost-perfectly implemented with parameters $(\rho, \varepsilon_1, \varepsilon_2)$ if there exists a sequence of secret sharing schemes for the secret variable $\varkappa_n$, such that*

- $H(\varkappa_n) \to \infty$;

- *the* $\limsup$ *of the information rates does not exceed ρ;*

- *the missing information ratio converges to ε_1 as $n \to \infty$;*

- *the information leak ratio converges to ε_2 as $n \to \infty$.*

In the present paper we show that a stronger definition where we require no missing information, gives the same notion. We formulate and prove an equivalent definition in the framework Kolmogorov complexity (see Section 3). In addition to these asymptotic results, we consider the following question. Imagine we have a secret sharing scheme with some leak information ratio (and some share sets). Can we transform it into a secret sharing scheme (for the same access structure) for a smaller set of secrets, say, a 1-bit secret? (Note that we want to keep a small information leak ratio, where $H(\varkappa)$ is in the denominator, so the absolute leak should be much smaller now). In Section 4 we show how such a transformation is possible in some cases.

2.1 Definitions

We consider two different versions of the definition of approximately-perfect secret sharing schemes. In the first one, non-perfect secret sharing schemes are allowed to give some information to forbidden groups and/or not give authorized groups the entire secret:

Definition 2.2. *Let $\mathcal{K}$ be a finite set of secrets, a $(\varepsilon_1, \varepsilon_2)$-nonperfect secret sharing scheme for secrets in $\mathcal{K}$ implementing an access structure Γ is a tuple of jointly distributed discrete random variables $(\varkappa, \sigma_1, \ldots, \sigma_n)$ such that*

- *if $A \in \Gamma$ then $H(\varkappa | \sigma_A) \le \varepsilon_1 H(\varkappa)$*

- *if $B \notin \Gamma$ then $I(\varkappa : \sigma_B) \le \varepsilon_2 H(\varkappa)$*

In this definition, authorized groups may fail to recover at most ε_1 bits of the secret while forbidden groups can not learn more than ε_2 bits. A probably more natural version of a non-perfect scheme is asymmetric: authorized groups know everything about the secret, while forbidden groups can keep not more than ε bits of information about the secret:

Definition 2.3. *Let $\mathcal{K}$ be a finite set of secrets, a ε-nonperfect secret sharing scheme for secrets in $\mathcal{K}$ implementing an access structure Γ is a tuple of jointly distributed discrete random variables $(\varkappa, \sigma_1, \ldots, \sigma_n)$ such that*

- *if $A \in \Gamma$ then $H(\varkappa | \sigma_A) = 0$*

- *if $B \notin \Gamma$ then $I(\varkappa : \sigma_B) \le \varepsilon H(\varkappa)$*

By ε-**NPS**(Γ, N, S), resp. $(\varepsilon_1, \varepsilon_2)$-**NPS**$(\Gamma, N, S)$, we refer to a ε-nonperfect, resp. $(\varepsilon_1, \varepsilon_2)$-nonperfect, secret sharing scheme implementing access structure Γ for N-bit secrets with single shares of entropy at most S. We use **PS**(Γ, N, S) for perfect schemes, i.e., when it is the case that ε_1 and ε_2 are null.

We now introduce the *almost-perfect* versions of secret sharing, that denotes an asymptotic sequence of nonperfect schemes for a fixed access structure where the leak can be made negligible as the size of the secret grows.

Definition 2.4. *We say that an access structure Γ can be almost-perfectly implemented, with parameters $(\rho, \varepsilon_1, \varepsilon_2)$, if there exists a sequence of nonperfect schemes in the sense of Definition 2.2 such that parameters converge to $(\rho, \varepsilon_1, \varepsilon_2)$. i.e., if*

$$\exists ((\varepsilon_m^1, \varepsilon_m^2)\text{-}\mathbf{NPS}(\Gamma, N_m, S_m))_{m \in \mathbb{N}} \ s.t. \ (\varepsilon_m^1, \varepsilon_m^2) \to (\varepsilon_1, \varepsilon_2) \ and \ \frac{N_m}{S_m} \to \rho \ as \ m \to \infty$$

Moreover, we say that Γ can be almost-perfectly implemented without missing information when the nonperfect schemes are in the sense of Definition 2.3.

In fact, as the following proposition shows, it does not matter in which sense of non-perfectness (with or without missing information) one defines the notion of almost-perfect secret sharing for they are equivalent.

Proposition 2.5. *Let Γ be an access structure and ρ be a positive real, the following are equivalement*

- *Γ can be almost-perfectly implemented*

- *Γ can be almost-perfectly implemented without missing information.*

This proposition is a corollary of the following result: one can transform a scheme with some missing information into a scheme without missing information by increasing the size of shares.

Proposition 2.6. *If Γ is an access structure on n participants, then*

$$\exists (\varepsilon_1, \varepsilon_2)\text{-}\mathbf{NPS}(\Gamma, N, S) \Rightarrow \exists (\varepsilon_2 + O(\varepsilon_1 N 2^n))\text{-}\mathbf{NPS}(\Gamma, N, S + O(\varepsilon_1 N 2^n))$$

Proof. Assume there is a $(\varepsilon_1, \varepsilon_2)$-**NPS**$(\Gamma, N, S)$, let us transform it as follows. Take a minimal authorized set $A \in \Gamma^-$, by definition it holds that $H(\varkappa | \sigma_A) \le \varepsilon_1 N$. Informally, it means that A lacks $\varepsilon_1 N$ bits of information about the secret. We materialize this information and add it to A. More precisely, we use the following lemma about conditional descriptions:

Lemma 2.7. *Let α and β be two random variables defined on the same space. Then there exists a variable γ (defined on the same space) such that $H(\alpha | \beta, \gamma) = 0$ and $H(\gamma) \le 2H(\alpha | \beta) + O(1)$.*

Proof. Let β be distributed on a set $\{b_1, \ldots, b_s\}$. For each fixed value b_j, we have a conditional distribution on values of α given the condition $\beta = b_j$. We can construct for this conditional distribution on values of α a prefix-free binary code $c_{1j}, \ldots, c_{mj}$ such that the average length of codewords is at most $H(\alpha|\beta = b_j) + 1$ (e.g., we can take Huffman's code).

Let γ be the corresponding codeword: if $\beta = b_j$ and $\alpha = a_i$ then $\gamma = c_{ij}$ (the i-th codeword from the code constructed for the distribution of α under condition $\beta = b_j$).

Given a value b_j of β and a codeword c_{ij} from the corresponding code, we can uniquely determine the corresponding value of α. Hence, we get $H(\alpha|\beta, \gamma) = 0$. It remains to estimate entropy of γ.

The defined above γ ranges over the union of all codewords c_{ij} (from all codes constructed for all possible values of β). The average length of bit strings c_{ij}

$$\mathbb{E}_{ij} |c_{ij}| = \mathbb{E}_i(\mathbb{E}_j |c_{ij}|) < \mathbb{E}_i(H(\alpha|\beta = b_j) + 1) = H(\alpha|\beta = b_j) + 1.$$

This observation is enough to estimate the entropy of γ.

The union of all codewords c_{ij} is not necessarily prefix-free even if the codes $\{c_{1j}, \ldots, c_{mj}\}$ were prefix-free for each value of β. However, we can convert any set of bit strings into a prefix-free code by a simple transformation: we double each bit in each string, and add at the end of each string the pair of bits 01. E.g., a string 00101 is converted into 000011001101. This simple trick converts the set of c_{ij} into a prefix-free set c'_{ij} such that

$$\mathbb{E}_{ij} |c'_{ij}| = 2 \, \mathbb{E}_{ij} |c_{ij}| + 2$$

Thus, random variable γ can be considered as a distribution on this prefix-free set c'_{ij}. It is well known that for any distribution on a prefix-free set, the entropy is not greater than the average length of codewords (it follows from Kraft's inequality). Hence, entropy of γ is not greater than the average length of c'_{ij}, i.e., not greater than $2H(\alpha|\beta) + O(1)$. $\qquad\square$

We apply lemma 2.7 to encode the secret k conditional to the shares of A. Since this random variable has entropy at most $\varepsilon_1 N$, the encoding can be done by strings of size at most $O(\varepsilon_1 N) + O(1)$. We add this "conditional description" to any participant of A. Now the participants of A can together determine the secret uniquely. We do the same for all minimal authorized groups in Γ^-. So, now all authorized groups have all information about the secret.

We added some additional data to several participants (some participants can obtain several different "conditional descriptions" since one participant can belong to several minimal authorized groups). However all additional information given to participants is of size only $O(\varepsilon_1 N 2^n)$, hence, the extra information is given to forbidden groups is at most $O(\varepsilon_1 N 2^n)$. The size of the shares in the new schemes is at most $S + O(\varepsilon_1 N 2^n)$, and we are done. $\qquad\square$

An interesting open question about almost-perfect secret sharing is to settle whether it is equivalent to perfect secret sharing or not:

Question 2.8. *Can we achieve essentially better information rates with almost-perfect schemes than with perfect schemes ?*

A weaker form of this question where leaks are exactly zero has been answered by Beimel et al in [2] (using a result of Matúš [14]) where they construct a *nearly-ideal* access structure, i.e. access structure that can be implemented perfectly with an information rate as close to 1 as we want but not equal. In fact, with the same kind of arguments we can construct an almost-perfect scheme for the same access structure with small leaks but information rate exactly one.

Proposition 2.9. *There is an access structure which can be implemented by an almost-perfect scheme with parameters $(1, 0, 0)$ and rate exactly one but has no ideal perfect scheme.*

Proof. An access structure Γ is induced by a matroid $M = (\mathcal{Q}, \mathcal{C})$ through $s \in \mathcal{Q}$ if Γ is defined on the set of participants $\mathcal{P} = \mathcal{Q} \setminus \{s\}$ by the upper closure of the collection of subsets $A \subseteq \mathcal{P}$ such that $A \cup \{s\} \in \mathcal{C}$ (here $\mathcal{C}$ is the set of circuits of the matroid $\mathcal{M}$.) Let $\mathcal{F}$ and $\mathcal{F}^-$ be respectively the access structures induced by the Fano and by the non-Fano matroids (through any point). In [14], Matúš proved that there exist perfect ideal schemes for $\mathcal{F}$, resp. $\mathcal{F}^-$ if and only if $\#\mathcal{K}$ is even, resp. odd.

Consider an access stucture Γ consisting of disjoint copies of $\mathcal{F}$ and $\mathcal{F}^-$. From Matúš argument, Γ cannot be implemented ideally by a perfect scheme. Construct a scheme Σ consisting of the concatenation of two independent schemes:

- a $\mathbf{PS}(\mathcal{F}, N, N)$, and

- a $\mathbf{PS}(\mathcal{F}^-, N, M)$, constructed from a $\mathbf{PS}(\mathcal{F}^-, M, M)$ for $\#\mathcal{K} = 2^N + 1$ (i.e., $M = \log(2^N + 1)$) where we removed one possible value of the secret.

Σ is a perfect scheme for Γ with rate $\frac{N}{\log(2^N+1)}$. Now instead of using a $\mathbf{PS}(\mathcal{F}^-, N, M)$ as second scheme, we modify it into a nonperfect scheme by substituting the value of the share "$2^N + 1$" by any other possible value. Now there are exactly 2^N shares. It is not difficult to show that Σ' is, at most, a $(\frac{3}{N}, 0)$-$\mathbf{NPS}(\Gamma, N, N)$ i.e., with information rate exactly one. $\qquad\square$

3   Kolmogorov secret sharing

We denote "the" Kolmogorov complexity function by the letter K. Since most variants are equal up to a logarithmic term and our results are asymptotic. For a complete introduction to Kolmogorov complexity and to some techniques used here, we refer the reader to the book [13] and to [18].

The problem of secret sharing could be studied also in the framework of the algorithmic information theory. The idea is that now a secret sharing scheme is not a distribution on binary strings but an individual tuple of binary strings with corresponding properties of "secrecy". To define these "secrecy" properties for individual strings, we substitute Shannon's entropy by Kolmogorov complexity and get algorithmic counterparts of the definition of secret sharing schemes. A similar idea was realized in Definition 21 (part 1) in [1] for a special case (for threshold access structures).

For Kolmogorov complexity there is no natural way to define an "absolutely" perfect version of secret sharing scheme. Thus, in the framework of Kolmogorov complexity we can deal only with "approximately-perfect" versions of the definition. We define approximately-perfect secret sharing schemes for Kolmogorov complexity just in the same way as we defined $(\varepsilon_1, \varepsilon_2)$-nonperfect schemes for Shannon's entropy (similarly to Definition 2.2):

Definition 3.1. *For an access structure Γ we say that a tuple of binary strings $(s, a_1, \ldots, a_n)$ is a Kolmogorov $(\varepsilon_1, \varepsilon_2)$-perfect secret sharing scheme for secrets of size N if*

- $K(s) = N$

- *for $A \in \Gamma, K(s|a_A) \leq \varepsilon_1 N$*

- *for $B \notin \Gamma, K(s) - K(s|a_B) = I(s : a_B) \leq \varepsilon_2 N$*

We reuse the template of almost-perfect secret sharing, this time in the Kolmogorov setting using the above version of secret sharing scheme. Thus, it should make sense to talk about almost-perfect secret sharing in the sense of Kolmogorov.

It turns out that problems of constructing approximately perfect secret sharing schemes in Shannon's and Kolmogorov's frameworks are closely related. For every access structure, in both frameworks the asymptotically optimal rates are equal to each other. More precisely, we have the following equivalence:

Theorem 3.2. *Let Γ be an access structure over n participants and ρ be a positive real, then the following are equivalent:*

- *Γ can be almost-perfectly implemented with parameters $(\rho, \varepsilon_1, \varepsilon_2)$ in the sense of Shannon.*

- *Γ can be almost-perfectly implemented with parameters $(\rho, \varepsilon_1, \varepsilon_2)$ in the sense of Kolmogorov.*

This theorem follows from a more general parallelism between Shannon entropy and Kolmogorov complexity. Below we explain this parallelism in terms of realizable complexity and entropy profiles.

The Kolmogorov complexity profile of a tuple $[a] = (a_1, \ldots, a_n)$ of a binary string is defined by the vector $\vec{K}([a])$ of Kolmogorov complexities of all pairs, triples . . . of strings a_i. So, it consists consists of

$2^n - 1$ (integer) complexity values, one for each non-empty subset of n strings a_i. In the same way we define the entropy profile $\vec{H}([s])$ of a tuple $[s] = (s_1, \ldots, s_n)$ of random variables by replacing $K(\cdot)$ by $H(\cdot)$.

Next theorem explains that the class of realizable complexity profiles and the class of entropy profiles are in some sense very similar:

Theorem 3.3. *For every $\vec{v} \in \mathbb{R}_+^{2^n-1}$ the following conditions are equivalent:*

- *there is a sequence $([s_m])_{m \in \mathbb{N}}$ of n-tuple of random variables s.t. $\frac{1}{m}\vec{H}([s_m]) \to \vec{v}$*

- *there is a sequence $([a_m])_{m \in \mathbb{N}}$ of n-tuple of binary strings s.t. $\frac{1}{m}\vec{K}([a_m]) \to \vec{v}$*

Note that Theorem 3.2 follows immediately from Theorem 3.3.

Proof. To prove this result, we convert a sequence of n-tuple of random variables into a sequence of n-tuple of binary strings and visa-versa; these conversions will preserve complexity/entropy profiles: corresponding tuples of random variables and strings will have similar values in their profiles.

The main technical tools are the Kolmogorov–Levin theorem

$$K(a, b) = K(a) + K(b|a) + O(\log |ab|)$$

and the "typization" trick for entropy and Kolmogorov complexity (the same technique as in [9, 16]).

[Kolmogorov $\to$ Shannon] Let $[a] = (a_1, \ldots, a_n)$ be an n-tuple of binary strings. For a non-negative integer c (to be fixed below) we consider the following set:

$$T_c([a]) = \{[a'] = (a_1', \ldots, a_n') : \forall U \subseteq [1, \ldots, n], K(a_U) - c \log |a| \leq K(a_U') \leq K(a_U)\},$$

which is the set of n-tuples of binary strings whose complexity profile is close to the one of $[a]$ up to a logarithmic term. Further we formulate several properties of $T_c([a])$.

Claim 3.4. $\log \#T_c([a]) = 2^{K(a) - O(\log K(a))}$ *for all large enough c.*

Proof. See Lemma 2 in [9] and Proposition 1 in [16]. We fix value c so that Claim 3.4 holds (c depends on the size n of the tuple but not on $K(a)$). $\square$

Claim 3.5. $\forall a' \in T_c(a), \forall U, V \subseteq [1, \ldots, n], K(a_U'|a_V') = K(a_U|a_V) - O(\log |a|)$

Proof. Follows from the definition of $T_c(a)$ and the Kolmogorov–Levin theorem. $\square$

Now, define $[s] = (s_1, \ldots, s_n)$ as an n-tuple of random variables uniformly distributed on $T_c([a])$. From the definition of $[s]$ and Claim 3.4 it follows that entropy of all $[s]$ is close to $K(a)$. We claim that in fact all components of the entropy profile of $[s]$ are close to the corresponding components in the complexity profile of $[a]$. We prove this property in two steps. At first, we obtain /Can upper bound:

Claim 3.6. $\forall U \subseteq [1, \ldots, n], H(s_U) \leq K(a_U) + 1$

Proof. The number of possible values for s_U is the number of possible substrings a_U' for $a' \in T(a)$. Since $K(a_U') \leq K(a_U)$, there is at most $2^{K(a_U)+1} - 1$ such values for s_U. Shannon's entropy of a random variable cannot be greater than logarithm of the number of its values, and we are done. $\square$

Further, we prove the lower bound:

Claim 3.7. $\forall U \subseteq [1, \ldots, n], H(s_U) \geq K(a_U) - O(\log |a|)$

Proof. First, consider a_U' for some fixed $a' \in T(a)$. From Claim 3.5, $K(a_{\overline{U}}'|a_U') \leq K(a_{\overline{U}}|a_U) + O(\log |a|)$, thus s_U can take at most $2^{K(a_{\overline{U}}|a_U)+O(\log |a|)}$ values. This is true for all such a_U', therefore $H(s_{\overline{U}}|s_U) \leq K(a_{\overline{U}}|a_U) + O(\log |a|)$.

Then,

$$
\begin{array}{rcll}
H(\mathbf{s}_U) & = & H(\mathbf{s}) - H(\mathbf{s}_{\overline{U}}|\mathbf{s}_U) & \text{(equality for entropy)} \\
& \geq & K(a) - K(a_{\overline{U}}|a_U) - O(\log |a|) & \text{(by definition of } s) \\
& \geq & K(a_U) - O(\log |a|) & \text{(from symmetry of information)}
\end{array}
$$

□

Therefore, the random variable $[s]$ has an entropy profile close to the complexity profile of $[a]$ up to a logarithmic factor. The first part fo the theorem is proven.

[Shannon $\to$ Kolmogorov] Let $s = (s_1, \ldots, s_n)$ be a n-tuple of random variables. We fixe an integer $M > 0$ (to be specified below) and construct some $M \times n$ table

$$
\begin{array}{c}
a_1^1 a_1^2 \ldots a_1^M \\
a_2^1 a_2^2 \ldots a_2^M \\
\vdots \\
a_n^1 a_n^2 \ldots a_n^M
\end{array}
$$

satisfying the following properties:

(a) The columns of the table (each column is an n-vector) consist of possible values for the random variable $[s]$.

(b) Different n-tuples are used as columns in the matrix with different frequencies; we require that each frequency is close to the corresponding probability in the distribution of $[s]$. More precisely, for every n-tuple of letters $(\alpha_1, \ldots, \alpha_n)$

the column $\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$ should occur in the table $\mathbf{Prob}[s = (\alpha_1, \ldots, \alpha_n)] \cdot M + O(1)$ times.

(c) The table has the maximal Kolmogorov complexity among all tables satisfying (a) and (b). It implies, by a rather simple counting argument, that

$$
K(a) \geq M \cdot H(s) - O(\log M)
$$

Denote $a_i = a_i^1 \ldots a_i^M$ for all $i = 1 \ldots n$ (i.e., we set a_i to be the row i of the table.) Let us verify that the n-tuple of binary strings $a = (a_1, \ldots, a_n)$ has a complexity profile close to the entropy profile of s multiplied by M.

Claim 3.8. $\forall U \subseteq [1, \ldots, n], K(a_U) \leq M \cdot H(s_U) + O(\log M)$

Proof. We extract from the entire table the rows corresponding to U; count frequencies of different columns (of size $|U|$) that occur in this restricted table (of size $|U| \times M$). Denote these frequencies by $f_1, f_2, \ldots$ (of course, the sum of all frequencies equals 1). Let h be the entropy of the distribution with probabilities $f_1, f_2, \ldots$. By Theorem 5.1 in [18],

$$
K(a_U) \leq M \cdot h + O(\log M).
$$

Further, we use the fact that frequencies f_j are close to the corresponding probabilities of s_u:

$$
\begin{array}{rcl}
h & = & -\sum_i f_i \log f_i \\
& = & -\sum_i (p_i + O(\frac{1}{M})) \log(p_i[1 + O(\frac{1}{p_i M})]) \\
& \leq & H(s_U) + O(\frac{1}{M})
\end{array}
$$

We get the claim by combining the two inequalities. □

Claim 3.9. $\forall U, V \subseteq [1, \ldots, n], K(a_U | a_V) \leq M \cdot H(s_U | s_V) + O(\log M)$

Proof. Denote $a_V = a_V^1 \ldots a_V^M$. We split all positions $i = 1 \ldots M$ into classes corresponding to different values of a_V^i. Denote the sizes of these classes by $m_1, m_1, \ldots$ By property (c) of the table, each

m_j must be proportional to the corresponding probability: the number m_j of positions $i = 1, \ldots, M$ such that $a_V^i = \bar{\alpha}_j$ is equal to

$$\mathbf{Prob}[s_v = \bar{\alpha}_j] \cdot M + O(1).$$

Given a_V, we describe a_U by an encoding a_U^i separately for different classes of positions corresponding to different values of a_V^i. Similarly to the previous Claim, we get

$$K(a_U|a_V) \leq \sum_j \left[m_j H(s_U|s_V = \bar{\alpha}_j) + O(\log m_j) \right]$$

where m_j is the number of columns c of the table where $a_V^c = \bar{\alpha}_j$. It follows that

$$K(a_U|a_V) \leq M \sum_j \frac{m_j}{M} H(s_U|s_V = \alpha_j) + O(\log M) = M \cdot H(s_U|s_V) + O(\log M)$$

$\square$

Claim 3.10. $\forall U, V \subseteq [1, \ldots, n], K(a_U|a_V) \geq M \cdot H(\mathbf{s}_U|\mathbf{s}_V) - O(\log |a|)$

Proof.

$$
\begin{array}{rcll}
K(a_U|a_V) & = & K(a) - K(a_V) - O(\log|a|) & \text{by Kolmogorov-Levin Theorem} \\
& \geq & MH(\mathbf{s}) - MH(\mathbf{s}_V) - O(\log|a|) & \text{by (c) and previous claim} \\
& \geq & MH(\mathbf{s}_U|\mathbf{s}_V) - O(\log|a|) & \text{Shannon information equality}
\end{array}
$$

$\square$

Thus, we have constructed a n-tuple of binary strings $[a]$ whose complexity profile is close to M times the entropy profile of $[s]$, up to some logarithmic term. $\square$

4 Scaling of secret sharing schemes

Here, we attempt to show how to scale up and down any secret sharing scheme. The problem consist of, given a secret sharing for N-bit secrets, constructing new secret sharing schemes for ℓ-bit secrets where ℓ can be arbitrary large or small. While this task is easy in the perfect case, it becomes much more difficult in the non-perfect case when we are concerned with efficiency and information leak.

4.1 Scaling for perfect schemes

We present some easy construction for scaling up and down in the perfect case and state what they achieve in terms of efficiency (size of the shares).

Proposition 4.1. *Let Γ be an access structure and Σ be a $\mathbf{PS}(\Gamma, N, S)$ then*
(a) [scaling down] *For every positive integer $\ell \leq N$ there exists a $\mathbf{PS}(\Gamma, \ell, S)$*
(b) [scaling up] *For every positive integer q there exists a $\mathbf{PS}(\Gamma, qN, qS)$*

Proof.
(a) To scale down, we can reuse the same scheme. Simply restrict the support of the random variable k to 2^ℓ values and equip this support with the uniform distribution. Authorized groups can determine the secret uniquely since it was the case in the initial scheme. Forbidden have no information about the secret otherwise they they had some information in the initial perfect scheme.

(b) For scaling up, the new scheme consists of the concatenation of q independent versions of the initial scheme. Since the new scheme consists of independent copies (a serialization) of the inital scheme, every new entropy value is q times the old entropy value. $\square$

4.2 Scaling for non-perfect schemes

Scaling up for nonperfect schemes is similar to the case of perfect schemes.

Proposition 4.2. *Let Γ be an access structure and Σ be a ε-**NPS**(Γ, N, S) then for every non-negative integer q there exists a $q\varepsilon$-**NPS**(Γ, qN, qS)*

Proof. Simply reuse the construction of (b) of proposition 4.1. Then a forbidden group can have at most $q\varepsilon$ bits of information about the secret. $\square$

Scaling down of the size of the secret becomes non-trivial for non-perfect secret sharing schemes if we want to keep the same information leak and missing information. If we can ε-nonperfectly share an N-bit secret, then intuitively it seems that we should be able to share one single bit with information leak ratio of about ε. However this statement is quite non-obvious. Now we formulate and prove a slightly weaker statement (it is the most technical result of this paper):

Theorem 4.3. *For all $c \in (0, \frac{1}{4})$ there exists an integer $N_0 > 0$ such that for every access structure Γ on n participants. If for some ε there exist a ε-**NPS**(Γ, N, S) where the secret is uniformly distributed, such that*

- $nS < 2^{cN}$

- $N > N_0$

*there exists a ε'-**NPS**$(\Gamma, 1, S)$ with $\varepsilon' = 8\varepsilon^{\frac{2}{3}}$, where the secret is uniformly distributed*

Sketch of the proof: Construct a new scheme for a 1-bit secret from the initial scheme in the following way. Given a ε-**NPS**(Γ, N, S) for a uniformly distributed secret in $\mathcal{K} = \{1, \ldots, 2^N\}$, take a splitting of $\mathcal{K}$ into two equal parts, say $\mathcal{K}_0$ and $\mathcal{K}_1$. Then define a new scheme as follows: to share the bit i, take a random element of $\mathcal{K}_i$ and share it with the initial scheme. It is easy to see that this new scheme is indeed a ε'-**NPS**$(\Gamma, 1, S)$ for a uniformly distributed secret bit with some leak ε'. This leak ε' depends on the initial choice of the splitting $\mathcal{K}_0$. We will show that there exists one such splitting for which the leak is small.

We first prove a general lemma about discrete random variables.

Lemma 4.4. *Let X be a finite discrete random variable over a k-element set A (with k even) such that $H(X) \geq \log k - \delta$ for some positive δ. Let B be a random subset of A of size $k/2$ (B is chosen uniformly, i.e., each $(k/2)$-element subset of A is chosen with probability $1/\binom{k}{k/2}$). Then for every $\gamma \in (0, 1)$, with probability at least*

$$1 - 2e^{-\frac{4\tau^2}{k\gamma^2}}$$

(probability for a random choice of B) we have

$$\| \Pr[X \in B] - \frac{1}{2} \| \leq 2\tau$$

(probability for the initial distribution X), where $\tau = \frac{1+\delta}{2\log \gamma k}$.

(In applications of this lemma we will choose the most reasonable values of parameter γ.)

Proof. For each element $x \in A$, denote by ρ_x the non-negative weight (probability) that X assigns to x. Using this notation we have

$$H(X) = \sum_{x \in A} -\rho_x \log \rho_x$$

A randomly chosen B contains exactly one half of the points x from A. We need to estimate the sum of ρ_x for all $x \in B$. We do it separately for "rather large" ρ_x and for "rather small" ρ_x. To make this idea more precise, fix a threshold $\gamma > 0$ that separates "rather large" and "rather small" values of ρ_x. Denote by p_γ the total measure of all ρ_x that are greater than this threshold. More formally,

$$p_\gamma = \sum_{\rho_x > \gamma} \rho_x$$

We claim that p_γ is rather small. Indeed, if we need to identify some $x \in A$, we should specify the following information which consists of two parts:

1. We say whether $p_x > \gamma$ or not (one bit of information).

2a. If $p_x > \gamma$, we specify the ordinal number of this "large" point; there are at most $1/\gamma$ points x' such that $\rho_{x'} > \gamma$, so we need at most $\log(1/\gamma)$ bits of information;

2b. otherwise, $p_x \leq \gamma$, we simply specify the ordinal number of x in A; here we need at most $\log k$ bits of information.

From the standard coding argument we get

$$H(X) \leq 1 + p_\gamma \log(1/\gamma) + (1 - p_\gamma) \log k$$

Since $H(X) \geq \log k - \delta$, it follows that $p_\gamma \leq \frac{1+\delta}{\log(\gamma k)}$.

Thus, we may assume that total measure of "rather large" values ρ_x is quite small even in the entire set A; hence, "large" points do not affect seriously the measure of a randomly chosen B. It remains to estimate the typical impact of "small" ρ_x to the weight of B.

Technically, it is useful to forget about "large" points x (substitute weights $\rho_x > \gamma$ by 0) and denote

$$\rho'_x = \begin{cases} \rho_x & \text{if } \rho_x \leq \gamma \\ 0 & \text{otherwise} \end{cases}$$

Now we choose exactly $k/2$ different elements from A and estimate the sum of the corresponding ρ'_x. Note that expectation of this sum is one half of the sum of ρ'_x for all $x \in A$, i.e, $(1 - p_\gamma)/2$. It remains to estimate the deviation of this sum from its expectation. We use the version of Hoeffding's bound for samplings without replacement, which can be used to estimate deviations for a sampling of $k/2$ points from a k-elements set, ([**?**][section 6]). The probability of the event that the sum exceeds expected value plus some τ can be bounded as follows:

$$\Pr[\sum_{x \in B} \rho'_x \geq (1 - p_\gamma)/2 + \tau] \leq e^{-\frac{2\tau^2}{|B|\gamma^2}} = e^{-\frac{4\tau^2}{k\gamma^2}}$$

Together with "large" values ρ_x we have

$$\Pr[\sum_{x \in B} \rho_x \geq (1 - p_\gamma)/2 + \tau + p_\gamma] \leq e^{-\frac{4\tau^2}{k\gamma^2}}$$

Now we fix the parameter τ to be equal to one half of the upper bound for p_γ, i.e., $\tau = \frac{1+\delta}{2\log(\gamma k)}$. It follows that,

$$\Pr[\sum_{x \in B} \rho_x \geq 1/2 + 2\tau] \leq e^{-\frac{4\tau^2}{k\gamma^2}}$$

From this bound, we can deduce the symmetric bound for the sum of ρ_x in $A \setminus B$:

$$\Pr[\sum_{x \in A \setminus B} \rho_x \leq 1/2 - 2\tau] \leq e^{-\frac{4\tau^2}{k\gamma^2}}$$

Since $A \setminus B$ and B share the same distribution (the uniform one), this bound also holds for B. Sum up the two bounds and we are done. $\qquad\square$

We are now ready to prove Theorem 4.3.

Proof. (of Theorem 4.3). Let $\mathcal{K}_0$ be a random subset of the set of all secrets $\mathcal{K}$ such that $|\mathcal{K}_0| = 2^{N-1}$. $\mathcal{K}_0$ is chosen uniformly over all possible such fair splittings of $\mathcal{K}$. If $\varkappa$ be the random variable for the N-bit secret in the initial scheme, let us define the new secret bit ξ as the bit defined by "$\varkappa \in \mathcal{K}_0$" ($\xi$ is indeed a bit since $H(\xi) = 1$). Our goal is to estimate $H(\xi|\sigma_B)$ for any $B \notin \Gamma$ be a forbidden group, and show it is large. Formally, we want to show that $H(\xi|\sigma_B) \geq 1 - \varepsilon'$ where $\varepsilon' = 8\varepsilon^{\frac{2}{3}}$.

First, we notice that for any bit ξ constructed as above, $I(\xi : \sigma_B) \leq \varepsilon$ holds for all $B \notin \Gamma$, so we can assume that $\varepsilon' \leq \varepsilon$, i.e,

$$\varepsilon' \geq \frac{8^3}{N^2} \tag{1}$$

We know that $H(\varkappa|\sigma_B)$ is rather large. More precisely,

$$H(\varkappa|\sigma_B) \geq N(1 - \varepsilon)$$

We introduce some positive parameter δ (to be fixed later) to separate all values of σ_B into two classes:

more typical values b such that $H(\varkappa|\sigma_B = b) \geq N(1 - \delta)$

and

less typical values b such that $H(\varkappa|\sigma_B = b) < N(1 - \delta)$

Since the entropy $H(\varkappa|\sigma_B)$ is large, the total measure of all "less typical" values b is rather small (more precisely, it is not greater than $\frac{\varepsilon}{\delta}$). We do not care about the conditional entropy of ξ when b is non-typical (the total weight of these b is so small that they do not contribute essentially to $H(\xi|\sigma_B)$). We focus on the contribution of $H(\xi|\sigma_B = b)$ for a typical value b. To estimate this quantity we apply lemma 4.4 to the distribution k conditional to $\sigma_B = b$, it follows that

$$H(\xi|\sigma_B = b) \geq h(1/2 + 2\tau) \geq 1 - 16\tau^2 \text{ with probability } 1 - 2e^{-\frac{4\tau^2}{\gamma^2}2^{-N}}$$

for some new parameter $\gamma > 0$ and $\tau = \frac{1+\delta N}{2(\log \gamma + N)}$.

This inequality true for all forbidden group B and any typical share b. Thus if we sum up the bad events, we obtain that the following estimation for $H(\xi|\sigma_B)$:

$$
\begin{aligned}
H(\xi|\sigma_B) &= \sum_{b \in \mathcal{S}_B} \Pr[\sigma_B = b]H(\xi|\sigma_B = b) \\
&\geq \sum_{\text{typical } b} \Pr[\sigma_B = b]H(\xi|\sigma_B = b) \\
&\geq (1 - \frac{\varepsilon}{\delta})(1 - 16\tau^2) \\
&\geq 1 - \frac{\varepsilon}{\delta} - 16\tau^2
\end{aligned}
$$

holds with probability at least

$$1 - |\overline{\Gamma}||\mathcal{S}_{\mathcal{P}}|2e^{-\frac{4\tau^2}{\gamma^2}2^{-N}} \tag{2}$$

where $\mathcal{S}_{\mathcal{P}}$ is the set of all possible shares given to the group of all participants.

Now, we choose our parameters γ and δ to deduce our result and show that our choice is valid. We take

$$16\tau^2 = \frac{\varepsilon}{\delta} = \frac{1}{2}\varepsilon' = 4\varepsilon^{\frac{2}{3}} \tag{3}$$

Under these conditions

$$\log \gamma = -N\left[1 - \frac{1}{8}\left(\frac{\varepsilon'}{\varepsilon N} + 2\right)\right] \tag{4}$$

and

$$H(\xi|\mathbf{B}) \geq 1 - 8\varepsilon^{\frac{2}{3}} = 1 - \varepsilon'$$

We want to find a simple sufficient condition that guarantees that the probability (2) is non-negative. To this end we do some (rather boring) calculations. We take the required inequality and reduce it step

12

by step to a weaker but more suitable form:

$$
\begin{array}{rcl}
|\overline{\Gamma}||S_{\mathcal{P}}|2e^{-\frac{4\tau^2}{\gamma^2}2^{-N}} & < & 1 \\[4pt]
|\overline{\Gamma}||S_{\mathcal{P}}| & < & 2e^{\frac{4\tau^2}{\gamma^2}2^{-N}} \\[4pt]
2^n 2^{nS} & < & 2e^{\frac{4\tau^2}{\gamma^2}2^{-N}} \\[4pt]
2^{n(S+1)} & < & 2^{\frac{4\tau^2}{\gamma^2}2^{-N}} \\[4pt]
n(S+1) & < & \frac{4\tau^2}{\gamma^2}2^{-N} \\[4pt]
2nS & < & \frac{4\tau^2}{\gamma^2}2^{-N} \\[4pt]
2nS & < & \frac{\varepsilon'}{8}2^{N(1-\frac{1}{4}(\frac{\varepsilon'}{\varepsilon N}+2))} \\[4pt]
nS & < & \varepsilon' 2^{\frac{1}{4}N-4} \\[4pt]
2^{cN} & < & \varepsilon' 2^{\frac{1}{4}N-4} \\[4pt]
1 & < & \varepsilon' 2^{(\frac{1}{4}-c)N-4} \\[4pt]
0 & < & (\tfrac{1}{4}-c)N + \log\varepsilon' - 4 \\[4pt]
0 & < & (\tfrac{1}{4}-c)N - 2\log N + 5
\end{array}
$$

	that is what we need, see (2)
	trivial upper bounds for $|\overline{\Gamma}|$ and $|S_{\mathcal{P}}|$
	since $e > 2$
	by applying log
	since $S \geq 1$
	from (3) and (4)
	since $\varepsilon' \leq \varepsilon N$
	by assumption
	from (1)

The last inequality (which is a sufficient condition for (2) to be non-negative) holds when $c < \frac{1}{4}$ and $N > N_0$ for some large enough N_0 depending on c. $\qquad\square$

Notice that in this case we consider schemes where the secret is uniformly distributed since the dependency on the probability distribution of the secret is not trivial in the nonperfect case. Sharing exactly one bit instead of N seems more difficult. We do not know whether this bound can be improved, in particular, can we achieve a leak of $O(\varepsilon)$? The assumption $nS = O(2^N)$ points out that the result holds for various kind of access structures defined by some trade-off between the number of participants n and the size of the shares S of a scheme for N-bit secrets.

5   Conclusion

In this article we introduced several definitions of almost-perfect secret sharing schemes (two versions in the framework of Shannon's entropy and another version in the framework of Kolmogorov complexity). We proved that all these approaches are asymptotically equivalent (have equivalent asymptotical rates of schemes for each access structure). This means that we can combine tools of Shannon's information theory and Kolmogorov complexity to investigate the properties of approximately-perfect secret sharing.

The major questions remain open. The most important one is to understand: can an almost perfect secret sharing scheme (for some access structure) achieve a better information rate than perfect (in classic sense) secret sharing schemes? The known proofs of lower bounds for the rate of perfect secret sharing schemes are based on combinations of information inequalities; so it is not hard to check that mostly the same argument would imply the same bounds for almost perfect schemes. Thus, the problem of separating the information rates for *almost-perfect* and exactly *perfect* schemes looks rather hard.

References

[1] L. Antunes, S. Laplante, A. Pinto, and L. Salvador. Cryptographic security of individual instances. In Yvo Desmedt, editor, *Information Theoretic Security*, volume 4883 of *Lecture Notes in Computer Science*, pages 195–210. Springer Berlin / Heidelberg, 2009.

[2] Amos Beimel, Noam Livne, and Carles Padró. Matroids can be far from ideal secret sharing. In *TCC*, pages 194–212, 2008.

[3] Amos Beimel and Ilan Orlov. Secret sharing and non-shannon information inequalities. In *TCC*, pages 539–557, 2009.

[4] Josh Cohen Benaloh and Jerry Leichter. Generalized secret sharing and monotone functions. In *CRYPTO*, pages 27–35, 1988.

[5] E. F. Brickell and D. R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes, 1992. 10.1007/BF02451112.

[6] Ernest F. Brickell and Daniel M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology*, 4(2):123–134, 1991.

[7] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *Journal of Cryptology*, 6:157–168, 1993.

[8] László Csirmaz. The size of a share must be large. *J. Cryptology*, 10(4):223–231, 1997.

[9] Daniel Hammer, Andrei Romashchenko, Alexander Shen, and Nikolai Vereshchagin. Inequalities for shannon entropy and kolmogorov complexity. *J. Comput. System Sci.*, 60(2):442–464, 2000.

[10] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. In *IEEE Globecom*, pages 99–102, 1987.

[11] Ehud D. Karnin, Jonathan W. Greene, and Martin E. Hellman. On secret sharing systems. *IEEE Transactions on Information Theory*, 29:35–41, 1983.

[12] Kaoru Kurosawa and Koji Okada. Combinatorial lower bounds for secret sharing schemes. *Inf. Process. Lett.*, 60(6):301–304, 1996.

[13] M. Li and P. Vitányi. *An Introduction to Kolmogorov complexity and its applications*. Springer-Verlag, second edition, 1997.

[14] František Matúš. Matroid representations by partitions. *Discrete Mathematics*, 203(1-3):169 – 194, 1999.

[15] Jessica Ruth Metcalf-Burton. Improved upper bounds for the information rates of the secret sharing schemes induced by the vamos matroid. *CoRR*, abs/0809.3010, 2008.

[16] Andrei Romashchenko. Pairs of words with nonmaterializable mutual information. *Problems of Information Transmission*, 36(1):1–18, 2000.

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

[18] A. K. Zvonkin and L. A. Levin. The complexity of finite objects and the development of the concepts of information and randomness by means of the theory of algorithms. *Russian Math. Surveys*, page 11, 1970.