Almost-perfect Secret Sharing

Tarik Kaced

Almost-perfect secret sharing

Tarik Kaced
Laboratoire d'Informatique Fondamentale de Marseille (LIF), Université de Provence
email: tarik.kaced@lif.univ-mrs.fr

***Abstract*—To split 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. 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).**

I. 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 [6] and [7]. 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 [12] and further developped in [8]) 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 $\varkappa$.

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).

[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.

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 [5], [11]). However, the problem becomes much more difficult if we limit the size of shares. It is known (see [8]) 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 [18]). 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 [5], [13]; 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 [4], [17]). 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 [9]). On the other hand, the known upper bounds for general access structures are exponential in the number of participants (and rather simple, see [5], [11]).

II. Nonperfect secret sharing

The relaxation of the perfectness property is natural when efficiency is involved (see [2], [14], [19]). Our attempt here is to encapsulate existing definitions of non-perfect schemes in the Shannon framework. We consider 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 are 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). If the information leak might not be huge for the uniform distribution, since 100 leaked bits are multiplied by 2^{-900} probability to have 900 trailing zeros; it can however become significant if the secret is not chosen uniformly, e.g. the user chooses a short password padded with trailing zeros.

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*, $H(\varkappa)$, the entropy of the secret divided by the maximal entropy of a single share;
- *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 this article we introduce several definitions of almost-perfect secret sharing schemes. Two versions in the framework of Shannon entropy for which we show that the stronger definition, where we require no missing information, gives the same notion; one version in the framework of Kolmogorov complexity. We prove that all these approaches are asymptotically equivalent (have equivalent asymptotical rates of schemes for each access structure). Hence, we can combine tools of Shannon's information theory and Kolmogorov complexity to investigate the properties of nonperfect secret sharing schemes.

Rather than providing constructions or stating trivial counterparts of known theorems, we emphasize our study on the behaviour of such schemes. Simple properties of perfect schemes provide new natural questions for nonperfect schemes which are in general not trivial. The main contribution of the paper is the proof of few of such natural properties, namely and Proposition 3.5 and Theorem 5.2 for scaling down a nonperfect scheme while keeping roughly the same information leak ratio.

We believe our modest contribution is a small step towards a promising path to discover new constructions and theorems in nonperfect secret sharing.

III. Approximately-perfect secret sharing schemes

We consider two versions of approximately-perfect secret sharing schemes, whether we allow missing information or not.

Definition 3.1: 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 $H(\varkappa|\sigma_A) \leq \varepsilon_1 H(\varkappa)$
- if $B \notin \Gamma$ then $I(\varkappa : \sigma_B) \leq \varepsilon_2 H(\varkappa)$

Definition 3.2: An ε-nonperfect secret sharing scheme is a $(0, \varepsilon)$-nonperfect scheme.

By ε-$\mathbf{NPS}(\Gamma, N, S)$, resp. $(\varepsilon_1, \varepsilon_2)$-$\mathbf{NPS}(\Gamma, N, S)$, 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 $\mathbf{PS}(\Gamma, N, S)$ 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 3.3: 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 3.1 such that parameters converge to $(\rho, \varepsilon_1, \varepsilon_2)$. i.e., if

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

Moreover, we say that Γ can be almost-perfectly implemented without missing information when the nonperfect schemes are in the sense of Definition 3.2.

Proposition 3.4: Let Γ be an access structure, 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.

The natural idea to prove this is to add the missing information to authorized groups. This plan is however not trivial to implement efficiently since the leak must remain small, hence we can not use a perfect scheme to share the missing information. The plan is to "materialize" the missing information and add it to each participant. This materialized missing information will only increase the information leak by a small amount. The following proposition shows we can indeed achieve a new leak comparable to the previous one.

Proposition 3.5: 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 $(\varepsilon_1, \varepsilon_2)$-$\mathbf{NPS}(\Gamma, N, S)$, let us transform it as follows. Take an authorized set $A \in \Gamma$, by definition it holds that $H(\varkappa|\sigma_A) \leq \varepsilon_1 N$. 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 3.6: 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 $H(\gamma) \leq 2H(\alpha|\beta) + O(1)$.

We apply lemma 3.6 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 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 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. ∎

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

Question 3.7: 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 [3] (using a result of Matúš [16]) 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 3.8: 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 $\mathcal{P} = \mathcal{Q} \backslash \{s\}$ 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 [16], 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. ∎

IV. 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 [15] and to [20].

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.

As opposed to Shannon entropy, Kolmogorov complexity provides a framework to talk about hardness of S conditional on X not only on average but for individual instances of the secret (see [1]). Kolmogorov complexity is not computable, but it is a reasonable limit value for all "practical" measures of algorithmic complexity and a very robust measure of randomness (it is not sensitive to small variations of S and X). We believe that the intuition from Kolmogorov's version of secret sharing may be quite adequate for practical applications.

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

Definition 4.1: 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 the problem 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 4.2: Let Γ be an access structure over n participants and $\rho, \varepsilon_1, \varepsilon_2$ be positive reals, 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, implicit in [10], between Shannon entropy and Kolmogorov complexity. It explain that the class of realizable complexity profiles and the class of entropy profiles are in some sense very similar.

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 $H(\cdot)$.

Theorem 4.3: 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 4.2 follows immediately from Theorem 4.3.

V. 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.

Proposition 5.1: Let Γ be an access structure:

(a) [scaling down] if there exists a $\mathbf{PS}(\Gamma, N, S)$ then for every positive integer $\ell \leq N$ there exists a $\mathbf{PS}(\Gamma, \ell, S)$.

(b) [scaling up] if there exists a $(\varepsilon_1, \varepsilon_2)$-$\mathbf{NPS}(\Gamma, N, S)$ then for every positive integer q there exists a $(q\varepsilon_1, q\varepsilon_2)$-$\mathbf{NPS}(\Gamma, qN, qS)$.

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 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. ∎

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. We formulate a slightly weaker statement (this is the main result of the paper):

Theorem 5.2: 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 an ε-$\mathbf{NPS}(\Gamma, N, S)$ where the secret is uniformly distributed, such that

$$N > N_0 \text{ and } nS < 2^{cN}$$

then there exists an ε'-$\mathbf{NPS}(\Gamma, 1, S)$ 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 an ε-$\mathbf{NPS}(\Gamma, N, S)$ 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 an ε'-$\mathbf{NPS}(\Gamma, 1, S)$ 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 can show that there exists such a splitting with small leak.

Notice that the secret must be uniformly distributed. The dependency on the probability distribution of the secret is not trivial in the nonperfect case. The assumption $nS = O(2^N)$ means that the result holds for various kind of access structures defined by the trade-off between the parameters n, S and N. 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 $O(\varepsilon)$?

VI. Conclusion

We introduced a notion of non-perfect secret sharing and its asymptotic version. The new natural questions in this setting are sometimes non-trivial and require a careful and technical analysis. For now, the question of separating perfect and almost-perfect secret sharing remains open.

Acknowledgment

The author would like to thank Andrei Romashchenko and Sasha Shen for stimulating discussions, and anonymous reviewers who helped substantially improve the manuscript. This work is partially supported by EMC ANR-09-BLAN-0164-01 and NAFIT ANR-08-EMER-008-01 grants.

References

[1] L. Antunes, S. Laplante, A. Pinto, and L. Salvador. Cryptographic security of individual instances. In *Information Theoretic Security*, volume 4883 of *LNCS*, pages 195–210. 2009.

[2] Amos Beimel and Matthew K. Franklin. Weakly-private secret sharing schemes. In *Theory of Cryptography*, pages 253–272, 2007.

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

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

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

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

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

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

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

[10] 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.

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

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

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

[14] Kaoru Kurosawa, Koji Okada, Keiichi Sakano, Wakaha Ogata, and Shigeo Tsujii. Nonperfect secret sharing schemes and matroids. In *Advances in cryptology*, EUROCRYPT '93, pages 126–141, 1994.

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

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

[17] Jessica Ruth Metcalf-Burton. Improved upper bounds for the information rates of the secret sharing schemes induced by the vamos matroid. *Discrete Mathematics*, 311(8-9):651 – 662, 2011.

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

[19] K. Srinathan, N. Tharani Rajan, and C. Pandu Rangan. Non-perfect secret sharing over general access structures. In *Proc. Progress in Cryptology*, INDOCRYPT '02, pages 409–421, 2002.

[20] 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.