


# Probabilistic Secret Sharing


## Paolo D'Arco

Dipartimento di Informatica, Università of Salerno, Italy  
pdarco@unisa.it

 <https://orcid.org/0000-0002-9271-4240>


## Roberto De Prisco

Dipartimento di Informatica, Università of Salerno, Italy  
robdep@unisa.it

 <https://orcid.org/0000-0003-0559-6897>


## Alfredo De Santis

Dipartimento di Informatica, Università of Salerno, Italy  
ads@unisa.it

 <https://orcid.org/0000-0001-8962-1919>


## Angel Pérez del Pozo

Departamento de Matemática Aplicada, Ciencia e Ingeniería de los Materiales y Tecnología Electrónica, Universidad Rey Juan Carlos, Madrid, Spain  
angel.perez@urjc.es

 <https://orcid.org/0000-0002-8135-9642>

## Ugo Vaccaro

Dipartimento di Informatica, Università of Salerno, Italy  
uvaccaro@unisa.it

 <https://orcid.org/0000-0003-4085-7300>

---

### Abstract

In classical secret sharing schemes a dealer shares a secret among a set of participants in such a way that qualified subsets can reconstruct the secret, while forbidden ones do not get any kind of information about it. The basic parameter to optimize is the size of the shares, that is, the amount of secret information that the dealer has to give to participants. In this paper we formalize a notion of *probabilistic* secret sharing schemes, in which qualified subsets can reconstruct the secret but only with a certain controlled probability. We show that, by allowing a bounded error in the reconstruction of the secret, it is possible to *drastically reduce the size* of the shares the participants get (with respect to classical secret sharing schemes). We provide efficient constructions both for threshold access structures on a finite set of participants and for evolving threshold access structures, where the set of participants is potentially infinite. Some of our constructions yield shares of *constant* size (i.e., not depending on the number of participants) and an error probability of successfully reconstructing the secret which can be made as *close to 1* as desired.

**2012 ACM Subject Classification** Security and privacy → Mathematical foundations of cryptography

**Keywords and phrases** Secret sharing, probabilistic secret sharing, evolving secret sharing

**Digital Object Identifier** 10.4230/LIPIcs.MFCS.2018.64

**Acknowledgements** The first and fourth authors are partially supported by research project MTM2016-77213-R funded by the Spanish MINECO.



© Paolo D'Arco, Roberto De Prisco, Alfredo De Santis, Angel Pérez del Pozo, and Ugo Vaccaro; licensed under Creative Commons License CC-BY

43rd International Symposium on Mathematical Foundations of Computer Science (MFCS 2018).

Editors: Igor Potapov, Paul Spirakis, and James Worrell; Article No. 64; pp. 64:1–64:16

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

## 1 Introduction

**Secret sharing.** A secret sharing scheme is a method through which a *dealer* shares a piece of information (*a secret*) among a set of participants, according to a specific privacy policy. Specifically, each participant, during the sharing phase, receives and securely stores a piece of information, called *share*. Then, in the reconstruction phase, prescribed subsets, called *qualified subsets*, by pooling together their shares or by sending them to a trusted combiner, can recover the secret through the computation of an appropriate reconstruction function. All the other remaining subsets of participants, called *forbidden subsets*, analyzing the shares they have, and applying *any* computation on them, do not get any information whatsoever about the secret. The collection of qualified subsets forms the *access structure* to the secret.

The notion of secret sharing and the first constructions were introduced in 1979, independently by Shamir [34] and Blakley [6]. Both of them considered *threshold* access structures, usually referred to as  $(k, n)$ -threshold schemes, where the set of participants has size  $n$ , *any* subset of size greater than or equal to  $k$  is qualified, and *any* subset of size less than  $k$  is forbidden. General access structures were later considered in [22, 23, 23, 4, 35, 25].

Secret sharing schemes have been widely used in cryptographic protocol design and have been extended in many ways in order to exhibit additional properties. For a detailed overview of the field and of the open problems the reader is referred to [2] and to [14].

**Visual cryptography (visual secret sharing).** Visual cryptography, introduced independently and in different forms in [31, 24], is a sharing technique in which the secret is an image, the shares are images printed on transparencies and the reconstruction is performed by the human visual system by looking at the superposed shares. Notice that, while the image can be seen as a sequence of black and white pixels and thus can encode arbitrary sequences of bits, the reconstruction function is fixed to be the **or** of the shares. Hence, any visual cryptography scheme can be used as a regular secret sharing scheme, i.e., as a scheme that uses the **or** function to reconstruct the secret; on the other hand, the converse is not true, unless the scheme uses the **or** function on the corresponding bits of the shares to reconstruct the secret. In the context of visual cryptography, the notion of probabilistic reconstruction has been widely studied, e.g., [36, 13, 19], since the erroneous reconstruction of a limited number of pixels does not significantly affect the recognizability of the reconstructed secret image.

**Evolving access structures.** An interesting new variant of secret sharing schemes has been introduced recently in [26, 27]. The authors have considered a setting in which the set of participants is *infinite* and the access structure is defined through a *collection* of access structures, not known at the beginning. More precisely, at any time  $t$ , a new participant arrives and new qualified subsets – if any – are added to the existing access structure  $\mathcal{A}_{t-1}$ , obtaining the new one  $\mathcal{A}_t$ . The authors of [26, 27] design secret sharing schemes in such a new scenario for threshold access structures, denoted as  $(k, \infty)$ -threshold schemes, and for general access structures. The authors of [26, 27] have also shown a nice equivalence between  $(2, \infty)$ -threshold schemes and prefix-free codes for the integers. Further results have been provided in [32, 28].

**Motivations of the present work.** Since their introduction, secret sharing schemes have represented a relevant research area in Cryptography. Secret sharing schemes are an important tool by themselves, as well as a building block both in the general solutions for multi-party

computation and in the design of ad-hoc protocols. A central issue in the area has been to provide constructive results and non-existential results towards the possibility of obtaining secret sharing schemes that provide to the users shares *short in size*. For threshold access structures and ramp schemes tight bounds have been provided in [11] and in [9].

Unfortunately, for general access structures what can be done is still an open problem: for many access structures the known constructions deliver to the users shares of exponential size in the number  $n$  of participants [5] (see also [30] for recent important improvements). The best lower bound on the size of the shares is instead sublinear as it was proved in [8, 15] using the information theoretic approach introduced in [10]. For the subclass of *linear* general secret sharing schemes recent results of [33] provide exponential lower bounds.

Several papers have considered secret sharing schemes in which the privacy condition has been relaxed, both in a *statistical* sense, i.e., the privacy is not information-theoretic but there is a probability of information leakage, and in a *computational* sense, i.e., the privacy is only guaranteed with respect to computationally bounded adversaries, e.g., [29]. In [16, 20] secret sharing schemes are seen as joint probability distributions of the shares and the secret. This particular view is introduced to study the case of infinite participants and to deal with infinite domains for the shares. The approach leads to a probabilistic notion of security allowing information leakage. So, it is quite different from the approach pursued in this paper. To our knowledge, although the relaxation of the property that qualified subsets can correctly recover the secret has been mentioned in a few papers, no study has focused on the analysis and the design of secret sharing schemes in which the secret can be reconstructed only with a prescribed high probability. Exceptions consist for the specific case of visual cryptography [17] and, notably, the secret sharing scheme of [21]. We remark that the model used in [21], that allows public information, is different from the one considered in this paper.

Hence, it seems natural to ask the following question:

*Can we reduce the size of the shares held by the participants if we allow a small probability of error in the reconstruction phase?*

In this paper we show that it is possible to give an answer to the above question by providing, among other results, a quantitative trade-off between the probability of a correct reconstruction and the size of the shares.

**Our contribution.** We proceed as follows: in Section 2, we introduce a formal definition of probabilistic secret sharing schemes that intends to capture the intuition given above. We consider both access structures on a finite set of participants and evolving access structures defined over an infinite set of participants. Then, in Section 3, we discuss probabilistic constructions for the finite case and, in Section 4, we propose a probabilistic construction for a  $(2, \infty)$ -threshold secret sharing scheme. In Section 5, we describe and analyze some methods to build more general schemes from simpler ones. Our techniques are of general interest since they apply to both deterministic and probabilistic secret sharing schemes. Then, in Section 6, we describe and analyze a direct construction for probabilistic secret sharing schemes, which gives to participants shares of constant size, with respect to the number of participants, and enables the dealer to set the probability of reconstruction as high as he needs. Finally, in Section 7, we provide conclusions and briefly discuss some open problems.

**Overview of results and techniques.** We define and provide constructions for  $\alpha$ -probabilistic secret sharing schemes for threshold access structures, where  $\alpha$  denotes *the probability of a correct reconstruction*, both for the finite and the infinite cases, by using a variety of

techniques. Throughout the paper, unless otherwise stated, we assume that the secret is a single bit.

- Focusing on the finite case, where the set of participants is fixed and has size  $n$ , we leverage on a nice connection in *visual* secret sharing schemes between deterministic and probabilistic schemes. We show how a probabilistic visual secret sharing scheme can be turned easily into an  $\alpha$ -probabilistic secret sharing scheme for the same access structure.
- To deal with evolving access structures, we design a  $(2, \infty)$ -threshold  $\frac{1+p}{2}$ -probabilistic secret sharing scheme, where  $(p, 1 - p)$  is the probability distribution of the secret bit. Our construction is inspired by the  $(2, \infty)$ -threshold visual cryptography scheme provided in [12], which seems to be the first paper that has considered the problem of constructing a visual secret sharing scheme for an infinite set of participants. It is simple and allows to share a 1-bit secret with shares of 1-bit.
- Successively, in order to construct more general schemes from simpler ones, using a recursive approach, we present two algorithms: the first builds a  $(k + 1, \infty)$ -threshold  $\alpha$ -probabilistic secret sharing scheme from a  $(k, \infty)$ -threshold  $\beta$ -probabilistic secret sharing scheme. The second builds a  $(k + 1, \infty)$ -threshold  $\alpha$ -probabilistic secret sharing scheme from  $k$  schemes, i.e., by using, for  $j = 2, \dots, k$ , a  $(j, \infty)$ -threshold  $\alpha_j$ -probabilistic secret sharing scheme. We point out that the algorithms can be used to construct *both* probabilistic schemes and deterministic schemes for evolving access structures. In particular, for both of our methods, if we use the most efficient deterministic  $(2, \infty)$ -threshold secret sharing scheme provided in [26, 27] and apply to the scheme resulting from the algorithms, the same domain reduction technique which is used in [26, 27], we get deterministic schemes for evolving access structures which achieve the same asymptotic share size of the ones obtained in [26, 27]. Hence, the new schemes can be seen as an *alternative way* for constructing deterministic schemes. On the other hand, for both of our algorithms, starting from our  $(2, \infty)$ -threshold  $\frac{1+p}{2}$ -probabilistic secret sharing scheme, we obtain  $(k, \infty)$ -threshold  $\alpha$ -probabilistic secret sharing schemes which achieve asymptotically the same share size of the deterministic schemes.
- Finally, through a direct construction, which uses the shares of Shamir's scheme, we provide a  $(k, \infty)$ -threshold  $\alpha$ -probabilistic secret sharing scheme which enables to share a 1-bit secret with shares of *constant size*. Moreover, the scheme exhibits a nice trade-off between the probability  $\alpha$  of successfully reconstructing the secret and the size of the underlying field: indeed,  $\alpha$  can approach 1 as much as desired by properly choosing the size of  $\mathbb{F}_q$ . For the case in which  $k$  is equal to 2, we explain the differences between this construction and the  $(2, \infty)$ -threshold  $\frac{1+p}{2}$ -probabilistic secret sharing scheme presented in Section 4. Finally, we emphasize that our construction also applies to the case of a finite number of participants, and we describe advantages and disadvantages associated with it.

Hence, the probabilistic approach we suggest enables to *beat the lower bounds* on the size of the shares the deterministic threshold schemes are subject to, both for the case of a finite set of participants and for the infinite one.

**Related work.** Other models for secret sharing schemes have been introduced in the past years in order to reduce the size of the shares held by the participants. More precisely, secret sharing schemes in which the correctness property holds with *no error*, and the privacy property holds with *identical* probability distributions on the shares held by the participants of a forbidden subset, are called *perfect*. *Non-perfect* secret sharing schemes are less restrictive. For example, in a  $(d, t, n)$ -ramp scheme [7], the first and most relevant case of non-perfect

secret sharing schemes, forbidden subsets of size less than  $d$  do not get any information about the secret, qualified subsets of size greater than or equal to  $t$  reconstruct the secret, while subsets whose sizes are “*in between*” get *some* information about the secret. Note that ramp schemes are a *close but different* class of non-perfect schemes, compared to the probabilistic ones we introduce here. Similarly, *computational* secret sharing schemes [29] are another class of non-perfect secret sharing schemes; in such schemes the privacy property requires computationally indistinguishable probability distributions on the shares held by the participants of a forbidden subset. In both cases, it is possible to design schemes with shorter share size compared to the size of the shares in perfect secret sharing schemes.

## 2 The Models

In this section we introduce the models we work with. We essentially follow and extend the treatment of [2, 26, 27].

Let  $\mathcal{P}_n = \{p_1, \dots, p_n\}$  be a finite set of  $n$  participants, and let  $2^{\mathcal{P}_n}$  be the set of all the subsets of  $\mathcal{P}_n$ . A collection of subsets  $\mathcal{A} \subseteq 2^{\mathcal{P}_n}$  is *monotone* if, for each subsets  $B, C \in \mathcal{P}_n$  such that  $B \subseteq C$ , the condition  $B \in \mathcal{A}$  implies  $C \in \mathcal{A}$ .

An access structure is defined as follows:

► **Definition 1.** An *access structure*  $\mathcal{A}$  on the set  $\mathcal{P}_n = \{p_1, \dots, p_n\}$  is a monotone collection of subsets of  $\mathcal{P}_n$ , i.e.,  $\mathcal{A} \subseteq 2^{\mathcal{P}_n}$ . Subsets in  $\mathcal{A}$  are called *qualified*. Subsets not in  $\mathcal{A}$  are called *forbidden*.

To avoid overburdening the notation, when it is clear from the context, we use the letter which denotes a subset of participants also to denote the subset of the indices of the participants. We define a probabilistic secret sharing scheme as follows.

► **Definition 2.** Let  $S$  be a set of secrets such that  $|S| \geq 2$ , and let  $\alpha$  be a positive real value such that  $0 < \alpha \leq 1$ . An  $\alpha$ -probabilistic secret sharing scheme  $\Pi$  for an access structure  $\mathcal{A}$  on the set of participants  $\mathcal{P}_n$  and set of secrets  $S$  consists of a pair of probabilistic polynomial time algorithms (**Share**, **Recon**) where

- **Share** gets as input a secret  $s \in S$  and outputs  $n$  shares  $sh_1, \dots, sh_n$
- **Recon** gets as input the shares of a subset  $A \subseteq \mathcal{P}_n$ , denoted by  $\{sh_i\}_{i \in A}$ , and outputs a string

such that the following two requirements are satisfied:

1.  **$\alpha$ -correctness:** for every  $s \in S$  and every qualified subset  $A \in \mathcal{A}$ , it holds that

$$\text{Prob}[\text{Recon}(\{sh_i\}_{i \in A}) = s] \geq \alpha.$$

2. **perfect privacy:** for every forbidden subset  $B \notin \mathcal{A}$  and for every two secrets  $s_1, s_2 \in S$ , it holds that the probability distributions  $\{sh_i^1\}_{i \in B}$  and  $\{sh_i^2\}_{i \in B}$ , associated to the corresponding secrets, are the same.

► **Remark.** Notice that, when the parameter  $\alpha$  is equal to 1, we get the traditional notion of perfect secret sharing scheme, in which the secret is *always* reconstructed by qualified subsets of participants.

► **Remark.** As pointed out in [2], the above definition can be easily relaxed to consider less stringent privacy notions, in which the probability distributions on the set of shares of forbidden subsets are not required to be identical but only statistically close or computationally indistinguishable.

The *share size* of the scheme is the maximum number of bits each participant holds in the worst case, over all participants and all secrets.

In order to introduce evolving schemes, we need to modify the setting and extend some of the previous notions. Basically, we define a sequence of access structures but require that the access structures be monotone: parties are *only added* and qualified subsets *remain qualified in the future*.

Let  $\mathcal{P} = \{p_1, p_2, \dots\}$  be an infinite set of participants.

► **Definition 3.** [26, 27] Let  $\mathcal{A}$  be an access structure on  $\mathcal{P}_n$  and let  $m$  be an integer such that  $0 < m < n$ . We denote by  $\mathcal{A}|_m$  the restriction of  $\mathcal{A}$  to  $\mathcal{P}_m$ , i.e., to the first  $m$  participants.

The following result holds:

► **Claim 4.** [26, 27] If  $\mathcal{A}$  is an access structure on  $\mathcal{P}_n$ , then  $\mathcal{A}|_m$  is an access structure on  $\mathcal{P}_m$ .

► **Definition 5.** [26, 27] Let  $\mathbb{N}$  be the set of the natural numbers. A (possibly infinite) sequence of access structures  $\{\mathcal{A}_t\}_{t \in \mathbb{N}}$  is called *evolving* if, for every  $t \in \mathbb{N}$ , the following conditions hold:

- $\mathcal{A}_t$  is an access structure over  $\mathcal{P}_t$
- $\mathcal{A}_t|_{t-1}$  is equal to  $\mathcal{A}_{t-1}$ .

At this point, we can extend the definition of a probabilistic secret sharing scheme to evolving access structures:

► **Definition 6.** Let  $S$  be a set of secrets such that  $|S| \geq 2$ , and let  $\alpha$  be a positive real value such that  $0 < \alpha \leq 1$ . An  $\alpha$ -probabilistic secret sharing scheme  $\Pi$  for an evolving access structure  $\{\mathcal{A}_t\}_{t \in \mathbb{N}}$  on the infinite set of participants  $\mathcal{P}$  and set of secrets  $S$  consists of a pair of probabilistic polynomial time algorithms (**Share**, **Recon**) where

- **Share** gets as input a secret  $s \in S$  and the shares  $sh_1, \dots, sh_{t-1}$ , generated for participants  $p_1, \dots, p_{t-1}$ , and outputs the share  $sh_t$  for the  $t$ -th participant
- **Recon** gets as input the shares of a subset  $A \subseteq \mathcal{P}$ , denoted by  $\{sh_i\}_{i \in A}$ , and outputs a string

such that the following two requirements are satisfied:

1.  **$\alpha$ -correctness:** for every  $s \in S$ , for every  $t \in \mathbb{N}$ , and for every qualified subset  $A \in \mathcal{A}_t$ , it holds that

$$\text{Prob}[\text{Recon}(\{sh_i\}_{i \in A}) = s] \geq \alpha.$$

2. **perfect privacy:** for every  $t \in \mathbb{N}$ , for every forbidden subset  $B \notin \mathcal{A}_t$  and for every two secrets  $s_1, s_2 \in S$ , it holds that the probability distributions  $\{sh_i^1\}_{i \in B}$  and  $\{sh_i^2\}_{i \in B}$ , associated to the corresponding secrets, are the same.

The *share size* of the scheme is the maximum number of bits the  $t$ -th participant holds in the worst case, over all secrets and previous share assignments.

► **Remark.** When the parameter  $\alpha$  is equal to 1, we get the notion of perfect evolving secret sharing scheme, in which the secret is *always* reconstructed by qualified subsets of participants, given in [26, 27]. Notice also that the above definition, when  $\mathcal{P}$  is finite and  $\mathcal{A}$  is fixed and known at the beginning, i.e.,  $\mathcal{P} = \mathcal{P}_n$  for a certain  $n$  and  $\{\mathcal{A}_t\}_{t \in \mathbb{N}} = \mathcal{A}$ , it formally *does not* coincide with Definition 2. Indeed, the former generates the shares in *one-shot*, while the latter generates the shares sequentially. However, it is easy to see they are equivalent. Moreover, the considerations we have done on relaxing the privacy notion apply also here.

Notice that in [3] a unified framework for secret sharing schemes has been introduced. It enables to model together perfect, statistically a computationally secure secret sharing schemes. It also models the notion of robustness, i.e., the possibility of reconstructing a secret even if some shares are missing or corrupted, assuming an honest dealer. We point out that the 36 notions the authors have provided do not consider any relaxation of the correctness condition. Moreover, we have preferred to follow [2, 26, 27] in modeling the notion instead of extending [3] because it is easy to work with [2, 26, 27] and, perhaps, results in an abstract easier to read.

### 3 Probabilistic schemes for the threshold finite case

Visual cryptography schemes are a special type of secret sharing schemes for which, roughly speaking, the Recon algorithm is the `or` function<sup>1</sup>. Several models of visual cryptography have been studied: Kafri and Keren [24] introduced the so-called random grid model, Naor and Shamir [31] coined the term “visual cryptography” providing a deterministic model, Yang [36] introduced the probabilistic model, which actually is equivalent to the model of Kafri and Keren, and Cimato et al. [13] generalized the probabilistic model. Finally, De Prisco and De Santis [19] proved that all these models are related to each other and, thus, they can be seen simply as different ways of looking at the same object. The interested reader is referred to [17] for a recent survey on models, issues, applications and new directions in visual cryptography and to the references therein quoted.

The particular “view” that is of interest in the context of this paper is the probabilistic one: in that model we already have the notion of a probabilistic reconstruction, where a secret pixel is correctly reconstructed only with a given probability. Nevertheless, notice that in the context of visual cryptography the error is less critical than in the context of general secret sharing: indeed, the whole secret which is visually reconstructed consists of many pixels, often thousands, and, even if some of them are incorrectly reconstructed, the only tangible effect is that the secret is reconstructed on a different, usually darker, background.

Anyway, being visual cryptography a special type of secret sharing, we can use visual cryptography schemes as secret sharing schemes. Since there is basically no research on probabilistic secret sharing, it is useful to start by taking probabilistic visual secret sharing scheme and “translating” them into probabilistic secret sharing schemes. We said “translating” instead of “using” because an obvious improvement that can be made is that of using a different Recon function, since in regular secret sharing we are not constrained to using the `or` performed by the human visual system in the reconstruction process.

In [19] it has been proved that any deterministic visual cryptography scheme can be transformed into a probabilistic visual cryptography scheme. By using this result we can transform any deterministic visual cryptography scheme into a probabilistic secret sharing scheme. We explain the technique using an example.

---

<sup>1</sup> In visual cryptography schemes, the bits of the shares are pixels printed on transparencies and the reconstruction consists in superposing the transparencies; the human visual system performs the `or` operation on the “bits” in the corresponding positions.



Consider a (3, 4)-threshold scheme. The following deterministic scheme has been presented in [1]. The scheme is described by two base matrices,  $B_0$  and  $B_1$ :

$$B_0 = \begin{bmatrix} 000111 \\ 001011 \\ 001101 \\ 001110 \end{bmatrix} \quad B_1 = \begin{bmatrix} 000111 \\ 100110 \\ 010110 \\ 001110 \end{bmatrix}$$

The two base matrices define the collections  $\mathcal{C}_0$  and  $\mathcal{C}_1$ , where  $\mathcal{C}_b$ ,  $b = 0, 1$ , contains all the matrices that can be obtained by permuting in all possible ways the columns of  $B_b$ . In order to share the secret the dealer (randomly) chooses a specific permutation and gives to each participant a row of the corresponding matrix of the collection  $\mathcal{C}_b$ , where  $b$  is the secret bit. More specifically, participant  $i$  gets the  $i^{\text{th}}$  row of the selected matrix (permutation).

For example, considering, for simplicity, the identity permutation, if the secret pixel is  $b = 0$ , that is a white pixel, then participant 1 gets a share where the first three subpixels are white and the last three are black, described with the binary string 000111, while participant 2 gets a share described by 001011, that is, the subpixels are white-white-black-white-black-black; etc. Superposing three shares for the reconstruction, it is guaranteed that, if the secret pixel is white, then the reconstructed version has 4 black subpixels out of 6; while, if the secret pixel is black, then the reconstructed version has 5 black subpixels out of 6. The fact that all permutations are considered ensures security.

A probabilistic visual cryptography scheme can be easily derived from the above deterministic scheme (see [19] for more details). In such a scheme, the secret pixel (bit) is shared by giving to each participant a white (0) or black (1) pixel (bit) according to the following sets<sup>2</sup>:

$$\mathcal{C}_0 = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right\},$$

$$\mathcal{C}_1 = \left\{ \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right\}.$$

More precisely, if the secret pixel is  $b$ , with  $b \in \{0, 1\}$ , the 4 participants are given shares according to one of the vectors in the set  $\mathcal{C}_b$ , where the specific vector is chosen *uniformly at random* in the set. The reconstruction function is the **or** of 4 bits. Looking at this scheme as a visual cryptography scheme, we have that a secret white (0) pixel is reconstructed correctly 1/3 of the times, while a secret black (1) pixel is reconstructed correctly 5/6 of the times. Assuming a uniform distribution of the secret pixel, the reconstruction is correct with probability 7/12.

On the other hand, using the **xor** function as Recon we have that in both cases the secret pixel is reconstructed correctly 5/6 of the times. This provides a 5/6-probabilistic scheme for sharing one bit, regardless of the distribution of the secret bit.

<sup>2</sup> Notice that these sets are easily constructed from the base matrices since each member of the set corresponds to a column of the base matrix.



The above “transform” of a visual cryptography scheme into a probabilistic secret sharing scheme can be applied to any visual cryptography scheme. In particular, it is possible to construct schemes for threshold and general access structures defined on a finite set of participants. Unfortunately, the constructions *do not extend* to the evolving case. So, we would like to find schemes that allow to manage an *evolving* set of participants.

As a side note, we point out an interesting fact: in the recent years, it has been shown that visual cryptography schemes can be used for secure computation in non standard settings, in which it is desirable to reduce the trust in digital devices [19, 18]. Here, we are going the other way around: we are using visual cryptography schemes for building probabilistic secret sharing schemes which can be used in standard digital computation.

#### 4 A probabilistic $(2, \infty)$ -threshold construction

In this section we present a construction of a probabilistic threshold scheme for the case of  $k = 2$ . The construction works both for a finite set of participants and for an infinite set of participants; the sharing phase is similar to the one described in Algorithm 2 of [12]. We present it as a  $(2, \infty)$ -threshold scheme, although the same construction works for a  $(2, n)$ -threshold scheme, when  $n$  is fixed in advance.

Let  $s$  be a secret bit. Let  $p_i$  be the  $i$ -th participant, with  $i$  potentially growing to  $\infty$  (or up to a fixed  $n$ ).

► **Construction 7.** *The construction works as follows.*

- *The Share algorithm takes as input the index  $i$  and produces a share for  $p_i$  as follows: for the first participant, that is for  $i = 1$ , the share is a random bit  $b_1$ ; for the other participants, that is, for  $i > 1$ , if the secret is  $s = 0$  then the share is  $b_1$ , the same bit given to  $p_1$ , whereas if the secret is  $s = 1$  the share is a new random bit  $b_i$ . In other words, if the secret is  $s = 0$ , then only one random bit is produced and all participants get that random bit as their share, while if the secret is 1 then each participant gets a new random bit.*
- *The Recon algorithm takes in input two shares, that is two bits  $b_i$  and  $b_j$  and outputs 0 if  $b_i = b_j$  (the two shares are equal), and 1 if  $b_i \neq b_j$  (the two shares are different).*

► **Theorem 8.** *Construction 7 builds a  $\frac{1+p}{2}$ -probabilistic  $(2, \infty)$ -threshold scheme, where  $(p, 1-p)$  is the distribution of the secret bit.*

**Proof.** We start by proving that the scheme is secure, that is any forbidden set does not have information about the secret bit. Indeed, let  $B = \{p_i\}$  be a forbidden set, a set with a single participant, and let  $s_1, s_2 \in S$  be two secret bits. The probability distribution of the share that  $p_i$  gets for  $s_1$  is the same as the one that  $p_i$  gets for  $s_2$ . Indeed the share is always a random bit, so in both cases the probability distribution is  $(0.5, 0.5)$  over the two possible values.

Next we prove that a qualified subset can reconstruct the secret with  $(1+p)/2$ -correctness. Let  $A$  be a qualified subset. In order to compute  $\text{Prob}[\text{Recon}(\{sh_i\}_{i \in A}) = s]$ , consider the two possible cases,  $s = 0$  and  $s = 1$ . The first one occurs with probability  $p$  and the second one with probability  $(1-p)$ . Thus, we have that:

$$\begin{aligned} \text{Prob}[\text{Recon}(\{sh_i\}_{i \in A}) = s] &= p \cdot \text{Prob}[\text{Recon}(\{sh_i\}_{i \in A}) = 0 | s = 0] + \\ &\quad (1-p) \cdot \text{Prob}[\text{Recon}(\{sh_i\}_{i \in A}) = 1 | s = 1]. \end{aligned}$$

When  $s = 0$ , all the shares are equal, thus Recon gives 0 as output and the reconstruction is always correct. Hence,  $\text{Prob}[\text{Recon}(\{sh_i\}_{i \in A}) = 0 | s = 0] = 1$ . On the other hand, when

## 64:10 Probabilistic Secret Sharing

$s = 1$ , all the shares are independent random bits, thus Recon gives in output 1 only half of the times, which means that  $\text{Prob}[\text{Recon}(\{sh_i\}_{i \in A}) = 1 | s = 1] = 1/2$ .

Therefore, we have that:

$$\text{Prob}[\text{Recon}(\{sh_i\}_{i \in A}) = s] = p \cdot 1 + (1 - p) \cdot \frac{1}{2} = \frac{1 + p}{2}. \quad \blacktriangleleft$$

For  $p = 0.5$ , we get a scheme with  $\frac{3}{4}$ -correctness. Notice also that, when  $p \neq 0.5$ , since we can easily swap 0 and 1, we can always change  $p$  to be  $1 - p$  to get a better correctness probability.

Finally, it is also easy to see that the above protocol can be strengthened, by using shares of 2 or more bits, constructed along the same line of the former, in order to make the probability of error as low as desired. Precisely, for sharing 0, the dealer chooses  $c$  bits uniformly at random and gives them to all participants. On the other hand, for sharing 1, to each new participant are provided  $c$  bits, chosen uniformly at random each time.

### 5 Transforms for general schemes from simpler ones

Once we have provided a probabilistic  $(2, \infty)$ -threshold construction it is a natural problem to extend it to the probabilistic  $(k, \infty)$ -threshold case. In this section we provide two different constructions for the general threshold case. The first one builds on an auxiliary probabilistic  $(k, \infty)$ -threshold construction which is used in a black-box way to build a probabilistic  $(k + 1, \infty)$ -threshold scheme. The probability  $\alpha$  of correct reconstruction is preserved. For the second construction we use a family of probabilistic  $(j, \infty)$ -threshold schemes, for  $j \leq k$ , to obtain a probabilistic  $(k + 1, \infty)$ -threshold scheme. The new scheme correctly reconstructs with probability at least the worse reconstruction probability of the schemes from the family.

The interesting aspect of the second construction lies in the fact that parties are grouped in generations of increasing size. The sizes of these generations are left as parameters of the construction and choosing them carefully leads to improvements in the share size with respect to the first construction.

Note that, if all auxiliary schemes provide 1-correctness, then the compiled constructions are also 1-correct; therefore, we are providing alternative constructions for the deterministic evolving  $(k, \infty)$ -threshold schemes presented in [26, 27]. In addition, if we apply to our constructions the same domain reduction technique which is used in [26, 27] to reduce the size of the shares, we get deterministic schemes for evolving access structures which achieve the same asymptotic share size of the ones obtained in [26, 27].

We denote by  $[n]$  the set  $\{1, \dots, n\}$  and, for consistency of some formulas,  $[0]$  denotes the empty set.

#### 5.1 From $(k, \infty)$ -threshold to $(k + 1, \infty)$ -threshold

Let  $s \in \{0, 1\}$  be the secret. The idea behind this construction is that at the arrival of party  $t$ , he receives the value  $s \oplus r$ , where  $r$  is a freshly and uniformly random generated bit. The bit  $r$  is then shared by using the  $(k, \infty)$  scheme with every party arriving after that moment.

More precisely, let  $\Pi$  denote the auxiliary  $(k, \infty)$ -threshold scheme and let  $\Lambda$  be the  $(k + 1, \infty)$ -threshold we are about to construct. At the time of arrival of party  $t$ , the share  $sh_t$  for the new scheme  $\Lambda$  is constructed in the following way:

1. A bit  $r_t \in \{0, 1\}$  is chosen uniformly at random.
2. For every  $j \in [t-1]$  a new share  $w_{t,j}$  of  $r_j$  is computed with  $\Pi$ .
3. The share of party  $t$  for the scheme  $\Lambda$  is the following (ordered) set of values:

$$sh_t = \{s \oplus r_t\} \cup \{w_{t,j}\}_{j \in [t-1]}$$

For the Recon algorithm of  $\Lambda$ , assume that  $k+1$  parties  $P_{t_0}, P_{t_1}, \dots, P_{t_k}$ , which are chronologically ordered, want to reconstruct. Then, the last  $k$  parties run the Recon algorithm of  $\Pi$  with inputs  $(w_{t_1, t_0}, w_{t_2, t_0}, \dots, w_{t_k, t_0})$  in order to recover the value  $r_{t_0}$ . Once  $r_{t_0}$  is recovered it is xored with the value  $s \oplus r_{t_0}$ , held by  $P_{t_0}$ , to recover  $s$ .

► **Theorem 9.** *If  $\Pi$  is an  $\alpha$ -probabilistic scheme for the  $(k, \infty)$ -threshold access structure then  $\Lambda$  is an  $\alpha$ -probabilistic scheme for the  $(k+1, \infty)$ -threshold access structure.*

**Proof.** First we prove the security of  $\Lambda$ . Let  $\mathcal{F} = \{P_{t_1}, \dots, P_{t_l}\}$  be a set of  $l \leq k$  parties which is chronologically ordered. The only value that party  $P_{t_j}$  holds which is related to the secret is  $s \oplus r_{t_j}$ . But then, as  $r_{t_j}$  has only been shared with players arriving later than  $P_{t_j}$  and there are at most  $k-1$  of them, the value  $r_{t_j}$  is a uniformly distributed random bit from the perspective of  $\mathcal{F}$  due to the perfect privacy of  $\Pi$ . Therefore, the value  $s \oplus r_{t_j}$  is also a uniformly distributed random bit for the set  $\mathcal{F}$ . Thus, we have shown perfect privacy for  $\Lambda$ .

Next, for  $\alpha$ -correctness, notice that the reconstruction algorithm of  $\Pi$  is used precisely once when reconstructing with  $\Lambda$ . If the value  $r_{t_0}$  is correctly reconstructed so it is the secret  $s$ . Therefore, if  $r_{t_0}$  is correctly reconstructed with probability at least  $\alpha$ , then the same holds for  $s$ . Our result for  $\alpha$ -correctness follows from this fact. ◀

► **Remark.** Note that for  $\alpha = 1$  we get a transform for regular (i.e. non probabilistic) evolving schemes.

**Share size.** Let  $size_{\Pi}(sh_t)$  denote the bitlength of the  $t$ -th share of the scheme  $\Pi$ . For the scheme  $\Lambda$  the size of the  $t$ -th share verifies

$$size_{\Lambda}(sh_t) = 1 + \sum_{j=1}^{t-1} size_{\Pi}(sh_j) \leq 1 + (t-1) \cdot size_{\Pi}(sh_{t-1})$$

where the last inequality holds if we assume that the shares are increasing in size, which is usually the case.

## 5.2 From $\{(j, \infty)\text{-threshold}\}_{j=2, \dots, k}$ to $(k+1, \infty)\text{-threshold}$

Let  $k \geq 2$  be an integer number. Assume that, for any  $j \in \{2, \dots, k\}$ ,  $\Pi_j$  is an auxiliary  $(j, \infty)$ -threshold scheme, and let  $\Lambda$  be the  $(k+1, \infty)$ -threshold scheme we are about to construct. For consistency of notation, assume that  $\Pi_1$  is a scheme that provides the secret to every participant. Let  $s \in \{0, 1\}$  be the secret. In this construction parties are grouped together in *generations*. For every integer  $i \geq 1$ , generation  $G_i$  is a set consisting of  $g_i$  consecutive participants.  $G_1$  starts with  $P_1$  while each subsequent generation starts with the participant following the last participant of the previous generation. For generation sizes we only require that they are an increasing sequence and all greater or equal than the target threshold, that is,  $k < g_1 \leq g_2 \leq g_3 \leq \dots$

When a generation  $G_m$  starts, the following values are computed:

1.  $k$  random bits  $r_1^{(m)}, \dots, r_k^{(m)}$  are chosen.
2. For every  $j \in [k]$ , the value  $s \oplus r_j^{(m)}$  is shared by using a regular  $(j, g_m)$ -threshold scheme, e.g., Shamir's scheme. Let  $u_{j,l}^{(m)}$  denote the  $l$ -th share.
3. The secret  $s$  is shared by using a  $(k+1, g_m)$ -threshold scheme. Let  $u_{k+1,l}^{(m)}$  denote the  $l$ -th share.

When the player  $P_t$ , which is the  $l$ -th player of generation  $G_m$ , arrives, the following values are computed:

4. For each  $i \in [m-1]$  and  $j \in [k]$  a new share for the random bit  $r_j^{(i)}$  is computed by using the  $(k+1-j, \infty)$ -threshold scheme  $\Pi_{k+1-j}$ . Note that it takes as inputs all the shares of  $r_j^{(i)}$  previously computed. Let  $v_{j,l}^{(i)}$  denote this share.
5. The share of party  $t$  is the following (ordered) set of values:

$$\Lambda_t^{(s)} = \{u_{j,l}^{(m)}\}_{j \in [k+1]} \cup \{v_{j,l}^{(i)}\}_{j \in [k], i \in [m-1]}$$

For the Recon algorithm of  $\Lambda$ , assume that a set  $\mathcal{F}$  consisting of  $k+1$  parties want to reconstruct. Moreover, assume that  $m$  is the first index such that a party from  $G_m$  is in  $\mathcal{F}$ . Let split  $\mathcal{F}$  in two parts,  $\mathcal{F}_0 = \mathcal{F} \cap G_m$  and  $\mathcal{F}_1 = \mathcal{F} \setminus \mathcal{F}_0$ , that is,  $\mathcal{F}_0$  consists of the parties from  $\mathcal{F}$  which are in generation  $G_m$  and  $\mathcal{F}_1$  consists of parties from subsequent generations. Let  $k_0 > 0$  be the cardinal of  $\mathcal{F}_0$  and  $k_1 \geq 0$  the cardinal of  $\mathcal{F}_1$ . Note that  $k_0 + k_1 = k+1$ . Now there are two different cases:

1. If  $k_1 = 0$ , that is, all players are in generation  $G_m$ , they use their  $\{u_{k+1,l}^{(m)}\}_l$  shares from the  $(k+1, g_m)$ -threshold scheme to recover  $s$ .
2. If  $k_1 > 0$ , then the players in  $\mathcal{F}_0$  use their  $\{u_{k_0,l}^{(m)}\}_l$  shares from the  $(k_0, g_m)$ -threshold scheme to recover  $s \oplus r_{k_0}^{(m)}$ . On the other hand, the players in  $\mathcal{F}_1$  use their  $\{v_{k_1,l}^{(m)}\}_l$  shares from the  $(k_1, \infty)$ -threshold scheme  $\Pi_{k_1}$  to recover  $r_{k_0}^{(m)}$ . Then, the two values  $s \oplus r_{k_0}^{(m)}$  and  $r_{k_0}^{(m)}$  are xored together and the secret is recovered.

► **Theorem 10.** *If, for every  $j \in \{2, \dots, k\}$ ,  $\Pi_j$  is an  $\alpha_j$ -probabilistic scheme for the  $(j, \infty)$ -threshold access structure, then  $\Lambda$  is an  $\alpha$ -probabilistic scheme for the  $(k+1, \infty)$ -threshold access structure, where  $\alpha = \min_{j=2, \dots, k} \{\alpha_j\}$ .*

**Proof.** The result follows from a similar analysis than the one for the proof of Theorem 9. For  $\alpha$ -correctness note that at most one of the schemes  $\Pi_j$  is used for reconstruction, while the other steps provide 1-correctness. ◀

**Share size.** The share of party  $t$ , which is the  $l$ -th participant from generation  $m$  includes  $k+1$  different shares  $\{u_{j,l}^{(m)}\}_{j \in [k+1]}$  for a  $(j, g_m)$ -threshold scheme. If instantiated with Shamir's scheme each of them is of size  $\lceil \log_2(g_m) \rceil$ . Therefore we have:

$$\text{size}_\Lambda(\text{sh}_t) = (k+1) \lceil \log_2(g_m) \rceil + \sum_{i=1}^{m-1} \sum_{j=1}^k \text{size}_{\Pi_j}(v_{j,l}^{(i)})$$

## 6 A probabilistic $(k, \infty)$ -threshold construction with constant share size

It is possible to construct probabilistic  $(k, \infty)$ -threshold schemes starting from our construction provided in Section 4. In order to do so, we need to first apply iteratively the transforms from Section 5, and then apply the same domain reduction technique of [26, 27]. However, the

probabilistic  $(k, \infty)$ -threshold constructions obtained in this way have the same asymptotic share size as the ones in [26, 27]. Thus, it might seem that there is no gain in moving from the deterministic to the probabilistic scenario. However, in the following, we show how to construct schemes with better share size.

More precisely, we propose a probabilistic  $(k, \infty)$ -threshold construction with constant size shares, which is known to be impossible in the deterministic scenario, due to the lower bound presented in [26, 27]. Moreover, by choosing the parameters appropriately, the scheme can be made  $\alpha$ -correct, with  $\alpha$  as close to 1 as desired, at the expenses of an increase in the size of the underlying field.

Let  $q > k$  be a prime power and let  $\mathbb{F}_q$  be a finite field with  $q$  elements. The idea behind this construction is giving each player an independently chosen at random Shamir share for a  $(k, q)$ -threshold scheme. In this case the secret  $s$  is an arbitrary element of  $\mathbb{F}_q$ , that is,  $s \in \mathbb{F}_q$ .

The scheme works as follows: at the beginning of the execution, a  $k-1$  degree polynomial  $p(x) \in \mathbb{F}_q$  is chosen as in Shamir's scheme, that is, such that  $p(0) = s$ . Upon arrival of participant  $t$ , a value  $r_t$  is chosen uniformly at random from  $\mathbb{F}_q \setminus \{0\}$ . The share of participant  $t$  is the pair  $(r_t, p(r_t))$ .

For reconstruction, a group of  $m$  participants checks if they hold at least  $k$  different values from  $\mathbb{F}_q$  as the first component of their shares. If this is the case they recover polynomial  $p(x)$  by interpolation and output  $p(0)$ . Otherwise, they output a random value in  $\mathbb{F}_q$ .

► **Theorem 11.** *The previous construction is an  $\alpha$ -probabilistic scheme for the  $(k, \infty)$ -threshold access structure, where*

$$\alpha = \frac{1}{(q-1)^k} \prod_{i=1}^k (q-i)$$

**Proof.** For security, take into account that  $m < k$  participants hold  $m$  shares for the Shamir's  $(k, q)$  threshold scheme and perfect privacy trivially follows.

For  $\alpha$ -correctness, the probability of  $k$  different participants getting  $k$  different shares and thus being able to correctly reconstruct the secret equals the probability of getting  $k$  different items when choosing  $k$  times, independently and uniformly at random, from  $q-1$  different items, which equals

$$\prod_{i=1}^k \frac{q-i}{q-1} = \frac{1}{(q-1)^k} \prod_{i=1}^k (q-i)$$

Note also that if  $m \geq k$  participants are present upon reconstruction, the probability of getting  $k$  different values only increases. The value of  $\alpha$  follows from these facts. ◀

**Share size.** A single share is a pair of two elements of  $\mathbb{F}_q$ , thus its size equals  $2(\lceil \log q \rceil + 1)$ .

► **Remark.** For a fixed value of  $k$ , the probability of correct reconstruction  $\alpha$  approaches to 1 when  $q \rightarrow \infty$ . Therefore, it is possible to get a scheme with  $\alpha$  as close to 1 as desired by appropriately choosing the value of  $q$ . Of course, increasing the value of  $q$  produces an increase in the share size.

► **Remark.** As pointed out in the proof, the participation of more than  $k$  parties in the reconstruction phase makes the probability of correctly reconstructing the secret to increase.

**Comparison with the scheme from Section 4.** Next we provide a brief comparative analysis between our constructions from Sections 4 and 6, when both are used to share secrets of the same size for the  $(2, \infty)$ -threshold access structure. Assume that  $s \in \{0, 1\}^l$  is a bitstring of

length  $l$ . When using the construction from Section 4 in a direct way,  $l$  independent instances are needed in order to share  $s$ . Thus, the share size equals  $l$  and the probability of perfect reconstruction, for example, assuming the uniform distribution on the secret space, equals  $(3/4)^l$ . On the other hand, when using the construction from this section with  $k = 2$ , we can choose  $q$  as the smaller prime power such that  $q > 2^l$ . Then, the share size equals  $\lfloor \log q \rfloor$  which will be equal or very close to  $l$ . And the probability of correct reconstruction equals

$$\frac{q-1}{q-1} \cdot \frac{q-2}{q-1} = \frac{q-2}{q-1}$$

Note that both constructions have almost the same share size, but the probability  $\alpha$  of correct reconstruction for the former scheme tends to 0, while for the latter scheme tends to 1 as  $l$  grows. We can conclude, looking at concrete numbers, that our construction from this section performs much better than the one from Section 4, even for small values of  $l$ .

## 7 Conclusions and open problems

We have introduced the notion of  $\alpha$ -probabilistic secret sharing schemes and provided two efficient constructions for threshold access structures and for evolving threshold access structures with shares of constant size, with respect to the number of participants, and probability of reconstruction as close to 1 as desired.

Many questions arise from the above study. We point out just two main challenging problems: the first one is how to design efficient probabilistic secret sharing schemes for *general access structures* for an infinite set of participants and which gain (if any) we can get, compared to perfect secret sharing schemes, in terms of share size. The second one is related to the *power* of probabilistic secret sharing schemes. Indeed, in [2] (Section 6), results, attributed to Rudich, show that it is unlikely to obtain efficient secret sharing schemes for certain access structures unless  $NP = \text{co-NP}$ . The proof uses the *perfect* correctness of the secret sharing schemes. The question is whether or not we can overcome the impossibility results by Rudich with probabilistic secret sharing schemes.

---

### References

- 1 G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson. Visual cryptography for general access structures. *Inf. Comput.*, 129(2):86–106, 1996. doi:10.1006/inco.1996.0076.
- 2 A. Beimel. Secret-sharing schemes: A survey. In *Proceedings of the Third International Conference on Coding and Cryptology*, LNCS 6639, pages 11–46, Berlin, Heidelberg, 2011. Springer-Verlag. URL: <http://dl.acm.org/citation.cfm?id=2017916>.2017918.
- 3 M. Bellare and P. Rogaway. Robust computational secret sharing and a unified account of classical secret-sharing goals. In *Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS '07*, pages 172–184, New York, NY, USA, 2007. ACM. doi:10.1145/1315245.1315268.
- 4 J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In *Proceedings on Advances in Cryptology*, LNCS 403, pages 27–35, Berlin, Heidelberg, 1990. Springer-Verlag. URL: <http://dl.acm.org/citation.cfm?id=88314>.88328.
- 5 J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In *Proceedings on Advances in Cryptology (CRYPTO '88)*, LNCS 403, pages 27–35, Berlin, Heidelberg, 1990. Springer-Verlag. URL: <http://dl.acm.org/citation.cfm?id=88314>.88328.
- 6 G. R. Blakley. Safeguarding cryptographic keys. In *Proceedings of the 1979 AFIPS National Computer Conference*, pages 313–317. AFIPS Press, 1979.



- 7 G. R. Blakley and C. Meadows. Security of ramp schemes. In *Proceedings of CRYPTO 84 on Advances in Cryptology*, pages 242–268, New York, NY, USA, 1985. Springer-Verlag New York, Inc. URL: <http://dl.acm.org/citation.cfm?id=19478.19498>.
- 8 C. Blundo, A. De Santis, R. De Simone, and U. Vaccaro. Tight bounds on the information rate of secret sharing schemes. *Designs, Codes and Cryptography*, 11(2):107–110, May 1997. doi:10.1023/A:1008216403325.
- 9 A. Bogdanov, S. Guo, and I. Komargodski. Threshold secret sharing requires a linear size alphabet. In *Proceedings, Part II, of the 14th International Conference on Theory of Cryptography*, LNCS 9986, pages 471–484, Berlin, Heidelberg, 2016. Springer-Verlag. doi:10.1007/978-3-662-53644-5\_18.
- 10 R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *J. Cryptol.*, 6(3):157–167, 1993. doi:10.1007/BF00198463.
- 11 I. Cascudo, R. Cramer, and C. Xing. Bounds on the threshold gap in secret sharing and its applications. *Information Theory, IEEE Transactions on*, 59:5600–5612, 09 2013.
- 12 S.-K. Chen and S.-J. Lin. Optimal  $(2, n)$  and  $(2, \infty)$  visual secret sharing by generalized random grids. *J. Vis. Commun. Image R.*, 23:677–684, 2012.
- 13 S. Cimato, R. De Prisco, and A. De Santis. Probabilistic visual cryptography schemes. *Comput. J.*, 49(1):97–107, 2006. doi:10.1093/comjnl/bxh152.
- 14 R. Cramer, I. Damgard, and J. B. Nielsen. *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press, New York, NY, USA, 1st edition, 2015.
- 15 L. Csirmaz. The size of a share must be large. *Journal of Cryptology*, 10(4):223–231, Sep 1997. doi:10.1007/s001459900029.
- 16 László Csirmaz. Probabilistic infinite secret sharing. *IACR Cryptology ePrint Archive*, 2012:412, 2012.
- 17 P. D'Arco and R. De Prisco. Visual cryptography - models, issues, applications and new directions. In *Innovative Security Solutions for Information Technology and Communications - 9th International Conference, SECITC 2016, Bucharest, Romania, June 9-10, 2016, Revised Selected Papers*, LNCS 10006, pages 20–39, 2016. doi:10.1007/978-3-319-47238-6\\_2.
- 18 P. D'Arco, R. De Prisco, and Y. Desmedt. Private visual share-homomorphic computation and randomness reduction in visual cryptography. In *Information Theoretic Security - 9th International Conference, ICITS 2016, Tacoma, WA, USA, August 9-12, 2016, Revised Selected Papers*, LNCS 10015, pages 95–113, 2016. doi:10.1007/978-3-319-49175-2\\_5.
- 19 R. De Prisco and A. De Santis. On the relation of random grid and deterministic visual cryptography. *IEEE Trans. Information Forensics and Security*, 9(4):653–665, 2014. doi:10.1109/TIFS.2014.2305574.
- 20 A. Dibert and L. Csirmaz. Infinite secret sharing - examples. *J. Mathematical Cryptology*, 8(2):141–168, 2014.
- 21 Y. Ishai, H. K. Maji, A. Sahai, and J. Wullschleger. Single-use ot combiners with near-optimal resilience. In *2014 IEEE International Symposium on Information Theory*, pages 1544–1548, June 2014. doi:10.1109/ISIT.2014.6875092.
- 22 M. Ito, A. Saio, and T. Nishizeki. Secret sharing schemes realizing general access structure. In *Proc. of the IEEE Global Telecommunication Conf., Globecom '87*, pages 99–102. IEEE, 1987.
- 23 M. Ito, A. Saio, and T. Nishizeki. Multiple assignment scheme for sharing secret. *J. Cryptology*, 6(1):15–20, 1993. doi:10.1007/BF02620229.
- 24 O. Kafri and E. Keren. Encryption of pictures and shapes by random grids. *Optics letters*, 12:377–379, 1987.
- 25 M. Karchmer and A. Wigderson. On span programs. In *Proc. of the 8th IEEE Structure in Complexity Theory*, pages 102–111, 1993. doi:10.1109/SCT.1993.336536.



- 26 I. Komargodski, M. Naor, and E. Yogev. How to share a secret, infinitely. In *Procc. of TCC 2016*, LNCS 9986, pages 485–514. Springer, 2016.
- 27 I. Komargodski, M. Naor, and E. Yogev. How to share a secret, infinitely. *IEEE Transactions on Information Theory*, 64(6):4179–4190, June 2018. doi:10.1109/TIT.2017.2779121.
- 28 I. Komargodski and A. Paskin-Cherniavsky. Evolving secret sharing: Dynamic thresholds and robustness. In *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part II*, LNCS 10678, pages 379–393, 2017. doi:10.1007/978-3-319-70503-3\_12.
- 29 H. Krawczyk. Secret sharing made short. In *Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '93)*, LNCS 773, pages 136–146, Berlin, Heidelberg, 1994. Springer-Verlag. URL: <http://dl.acm.org/citation.cfm?id=646758.705700>.
- 30 T. Liu and V. Vaikuntanathan. Breaking the circuit-size barrier in secret sharing. Cryptology ePrint Archive, Report 2018/333, 2018. URL: <https://eprint.iacr.org/2018/333>.
- 31 M. Naor and A. Shamir. Visual cryptography. In *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, LNCS 950, pages 1–12, 1994. doi:10.1007/BFb0053419.
- 32 A. Paskin-Cherniavsky. How to infinitely share a secret more efficiently. *IACR Cryptology ePrint Archive*, 2016:1088, 2016.
- 33 R. Robere, T. Pitassi, Rossman B., and S. A. Cook. Exponential lower bounds for monotone span programs. In *2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 406–415, Oct 2016. doi:10.1109/FOCS.2016.51.
- 34 A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.
- 35 J. G. Simmons, W. Jackson, and K. Martin. The geometry of shared secret schemes. *Bulletin of the Institute of Combinatorics and its Applications*, 1, 01 1991.
- 36 C.-N. Yang. New visual secret sharing schemes using probabilistic method. *Pattern Recogn. Lett.*, 25(4):481–494, mar 2004. doi:10.1016/j.patrec.2003.12.011.