Upslices, Downslices, and Secret-Sharing with Complexity of 1.5^n

Benny Applebaum
Tel-Aviv University
Tel-Aviv, Israel
benny.applebaum@gmail.com

Oded Nir
Tel-Aviv University
Tel-Aviv, Israel
odednir123@gmail.com

April 12, 2021

Abstract

A secret-sharing scheme allows to distribute a secret s among n parties such that only some predefined "authorized" sets of parties can reconstruct the secret, and all other "unauthorized" sets learn nothing about s. The collection of authorized/unauthorized sets can be captured by a monotone function $f : \{0,1\}^n \to \{0,1\}$. In this paper, we focus on monotone functions that all their min-terms are sets of size a, and on their duals – monotone functions whose max-terms are of size b. We refer to these classes as (a, n)-*upslices* and (b, n)-*downslices*, and note that these natural families correspond to monotone a-regular DNFs and monotone $(n - b)$-regular CNFs. We derive the following results.

1. (General downslices) Every downslice can be realized with total share size of $1.5^{n+o(n)} < 2^{0.585n}$. Since every monotone function can be cheaply decomposed into n downslices, we obtain a similar result for general access structures improving the previously known $2^{0.637n+o(n)}$ complexity of Applebaum, Beimel, Nir and Peter (STOC 2020). We also achieve a minor improvement in the exponent of linear secrets sharing schemes.
2. (Random mixture of upslices) Following Beimel and Farràs (TCC 2020) who studied the complexity of random DNFs with constant-size terms, we consider the following general distribution F over monotone DNFs: For each width value $a \in [n]$, uniformly sample k_a monotone terms of size a, where $\mathbf{k} = (k_1, \ldots, k_n)$ is an arbitrary vector of non-negative integers. We show that, except with exponentially small probability, F can be realized with share size of $2^{0.5n+o(n)}$ and can be linearly realized with an exponent strictly smaller than $2/3$. Our proof also provides a candidate distribution for "exponentially-hard" access structure.

We use our results to explore connections between several seemingly unrelated questions about the complexity of secret-sharing schemes such as worst-case vs. average-case, linear vs. non-linear and primal vs. dual access structures. We prove that, in at least one of these settings, there is a significant gap in secret-sharing complexity.

1 Introduction

Secret-sharing schemes, introduced by Shamir [34] and Blakley [13], are a central cryptographic tool with a wide range of applications including secure multiparty computation protocols [10, 15], threshold cryptography [19], access control [30], attribute-based encryption [24, 38], and oblivious transfer [35, 37]. In its general form [26], an n-party secret-sharing scheme for a family of authorized sets $F \subseteq 2^{[n]}$ (referred to as *access structure*) allows to distribute a secret s into n shares, $s_1, \ldots, s_n$, one for each party, such that: (1) every authorized set of parties, $A \in F$, can reconstruct s from its shares; and (2) every unauthorized set of parties, $A \notin F$, cannot reveal any partial information on the secret even if the parties are computationally unbounded. For example, in the canonical case of threshold secret sharing the family F contains all the sets whose cardinality exceeds some certain threshold. For this case, Shamir's scheme [34] provides a solution whose complexity, measured as the total share-size $\sum_i |s_i|$, is quasi-linear, $O(n \log n)$, in the number of parties n. Moreover, Shamir's scheme is *linear*, that is, each share can be written as a linear combination of the secret and the randomness that are taken from a finite field. This form of linearity turns to be useful for many applications. (See Appendix A.1 for a formal definition of secret sharing and linear secret sharing.)

The complexity of general secret-sharing schemes. Determining the complexity of general access structures is a basic, well-known, open problem in information-theoretic cryptography. Formally, given a (monotone) access structure[1] F we let $\mathsf{SSize}(F) := \min_{\mathcal{D} \text{ realizes } F} |\mathcal{D}|$, where $|\mathcal{D}|$ denotes the total share size of a secret-sharing scheme $\mathcal{D}$. For over 30 years, since the pioneering work of Ito et al. [26], all known upper-bounds on $\mathsf{SSize}(F)$ are tightly related to the computational complexity of the characteristic function F. Here we think of F as the monotone function that given a vector $x \in \{0,1\}^n$ outputs 1 if and only if the corresponding characteristic set $A = \{i : x_i = 1\}$ is an authorized set. Specifically, it is known that the complexity of an access structure is at most polynomial in the representation size of F as a monotone CNF or DNF [26], as a monotone formula [11], as a monotone span program [27], or as a multi-target monotone span program [12]. This leads to an exponential upper-bound of $2^{n(1-o(1))}$ for any n-party access structure F.

On the other hand, despite much efforts, the best known lower-bound on the complexity of an n-party access structure is $\Omega(n^2/\log n)$ due to [17]. Moreover, we have no better lower-bounds even for *non-explicit* functions! This leaves a huge exponential gap between the upper-bound and the lower-bound. For the case of linear schemes, a counting argument (see, e.g., [9]) shows that for most monotone functions $F : \{0,1\}^n \to \{0,1\}$, the complexity of the best linear secret-sharing (LSS) scheme, denoted by $\mathsf{LSSize}(F)$, is at least $2^{n/2-o(n)}$.[2] Furthermore, Pitassi and Robere [32] (building on results of [33, 31]) prove that for every n there exists an explicit n-input function F such that $\mathsf{LSSize}(F) = 2^{\Omega(n)}$. In his 1996 thesis [4], Beimel conjectured that an exponential lower-bound of $2^{\Omega(n)}$ also holds for the general case. Resolving this conjecture has remained one of the main open problems in the field of secret sharing [5]. Taking a broader view, similar exponential communication-complexity gaps exist for a large family of information-theoretic secure computation tasks [21, 25, 3, 23, 7]. Among these, secret-sharing is of special interest due to its elementary nature: Secret data is only *stored and revealed* without being processed or manipulated.

[1] Monotonicity here means that for any $A \subset B$ it holds that $A \in F \Rightarrow B \in F$. It is not hard to see that a non-monotone access structure does not admit a secret-sharing scheme, and therefore this requirement is necessary.

[2] The bound holds for any finite field. From now on when the field is unspecified we take it, by default, to be the binary field. This only makes our positive results stronger.

Recent advances: slices, multislices and general access structures. In the past three years, the seemingly tight correspondence between computational complexity and secret-sharing complexity was challenged by several works. In a breakthrough result, Liu, Vaikuntanathan and Wee [29, 28] showed that *any general access structure* can be realized with complexity of $2^{0.994n}$, thus breaking the formula-size (or even circuit-size) barrier of $2^{n-o(n)}$. The exponent was further reduced to 0.64 in follow-up works of Applebaum, Beimel, Farràs, Nir and Peter [1, 2]. From a technical point of view, all these works reduced the problem of realizing a general monotone function F to the problem of realizing the simpler case of *slice functions* and *multislice functions* (originally referred to as "fat slices" by [28]). Formally, $(a : b, n)$-*multislices* are monotone functions that are unconstrained on inputs x of weight $\mathrm{wt}(x) \in [a, b]$, but must take the value 0 on lighter inputs, and the value 1 on heavier inputs. An $(a : a, n)$-multislice is referred to as an (a, n)-*slice*. Roughly, the results of [28] were obtained by a sequence of 3 reductions: (1) Secret sharing for slice functions with sub-exponential share size of $2^{\tilde{O}(\sqrt{n})}$ based on constructions of Conditional Disclosure of Secrets (CDS) [29]; (2) Secret sharing for $((0.5-\epsilon)n, (0.5+\epsilon)n, n)$-multislices (aka ϵ-midslice) with non-trivial cost of 2^{cn} for some $c < 1$ based on slice functions; and (3) Secret sharing for general access structures with 2^{cn} complexity based on midslice secret sharing. The work of [1] showed how to improve Step 3 based on combinatorial covers, and the work of [2] improved the second step by presenting and constructing *robust-CDS* schemes. A combination of these results allows us to realize any n-party access structure by a secret sharing scheme of complexity $2^{0.64n+o(n)}$ and by a linear secret sharing scheme of complexity $2^{0.762n+o(n)}$.

Intriguing questions. This state of affairs leaves open several intriguing questions. Firstly, what is the best-achievable *exponent* of secret-sharing schemes? Secondly, which access structures are the hardest to realize? While the above results do not seem to yield sub-exponential share size, they also do not give rise to a candidate "hard" access structure. That is, to the best of our knowledge, we do not have an explicit candidate distribution over access structures whose cost is $2^{\Omega(n)}$ even if one restricts the attention to the current schemes. Indeed, it was recently observed by Beimel and Farràs [8] that a randomly chosen monotone function is likely to be a $(n/2-1, n/2+2, n)$-multislice, and therefore it can be realized with sub-exponential complexity.

2 Our Contribution

We make progress towards answering the above questions by shifting the focus from slices and multislices to *downslices* and *upslices*. Before stating our results, let us introduce these new access structures.

2.1 Upslice and Downslices

A monotone function $f : \{0,1\}^n \to \{0,1\}$ is an (a, n)-upslice if all its min-terms are of size exactly a. Similarly to (a, n)-slice functions, an (a, n)-upslice is unconstrained for inputs of weight a and takes the value 0 on lighter inputs, however, in contrast to slice functions, an input y of weight larger than a takes the value 1 only if there exists a *smaller* input $x \leq y$ of weight a on which the function takes the value 1.[3] This means that f is the pointwise *smallest* function among all the monotone functions that agree with f on inputs of weight a. Downslices are defined in a dual way. That is, a monotone function f is a (b, n)-downslice if all its *max-terms* are of size exactly b. This means that f is unconstrained over b-weight inputs, takes the value 1 on heavier inputs, and (unlike slice functions) evaluates to 0 on an input y of weight smaller than b

[3] We use the standard partial order over strings that is induced by inclusion over the corresponding characteristic sets. That is, $x \leq y$ if for every index i it holds that $x_i \leq y_i$.

only if there exists a *larger* input $x \geq y$ of weight b on which the function evaluates to 0. Accordingly, f is the pointwise *largest* function among all the monotone functions that agree with f on inputs of weight b. (An example of upslices and downslices is depicted in Figure 1.)

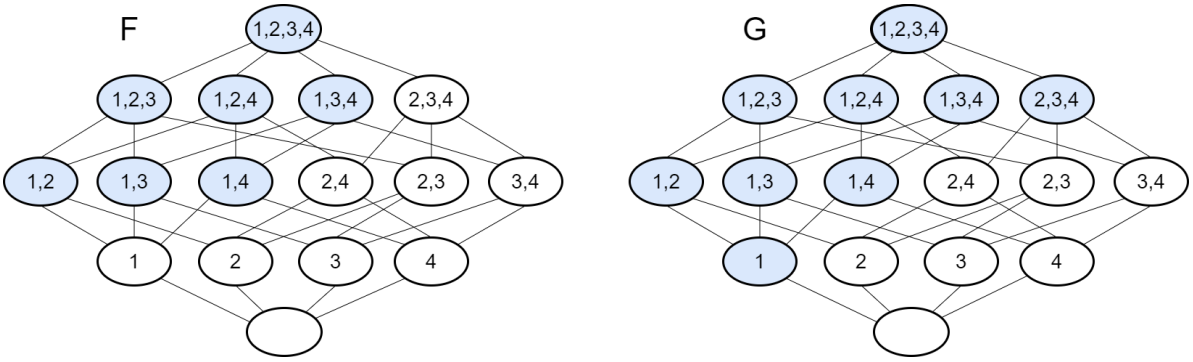


Figure 1: An example of a 2-upslice access structure F and a 2-downslice access structure G. Both access structures are defined over 4 parties and colored nodes correspond to authorized sets. Note that in this example F and G agree on sets of size 2.

Why Upslices and Downslices? Upslices and downslices are natural classes of monotone functions. Indeed, (a, n)-upslices (resp., (b, n)-downslices) are exactly the functions that can be represented by logical formulas in a Disjunctive Normal Form (resp., Conjunctive Normal Form) in which each term (resp., clause) consists of exactly a variables (resp., $n - b$ variables). Therefore, these function families capture the basic computational models of regular monotone-DNFs and regular monotone-CNFs. Additionally, every monotone function can be decomposed into a disjunction of its upslices, i.e., $f = \bigvee_{a \in [n]} f_a$ where f_a is the (a, n)-slice function that agrees with f on its a-weight inputs (hereafter referred to as the *a-upslice of f*). Similarly, f can be written as a conjunction of its downslices. Using standard closure properties of secret sharing, we conclude that the secret-sharing complexity of worst-case monotone functions is at most n times larger than the secret-sharing complexity of downslices/upslices. This should be contrasted with the status of "simple" slice functions whose complexity seems significantly smaller (i.e., sub-exponential) than the complexity of general monotone functions. Indeed, one can show that the complexity of an a-slice function f is the smallest among all monotone functions that agree with f on inputs of weight a (ignoring low-order terms).[4] For general values of a and b, the best known secret sharing schemes of (a, n)-upslices and (b, n)-downslices are based on their DNF and CNF representations and therefore have total share size of $\binom{n}{a}$ and $\binom{n}{b}$, respectively. Up to logarithmic improvements, these worst-case bounds have remained unchanged even for the special case of $(2, n)$-upslices that correspond to *graph* access structures [14] (not to be confused with *forbidden graph* access structures [36] that correspond to $(2, n)$-slices). See [8] for additional references.

2.2 Worst-Case Downslices

In Section 4 we show that every (b, n)-downslice admits a secret sharing scheme with complexity of $(3/2)^{n+o(n)}$. Using the completeness of downslices this allows us to improve the complexity of general

[4] To see this, observe that if f is the a-slice of a monotone function g, we can write f as $f = (g \wedge T_{a-1}) \vee T_{a+1}$ where T_k is the k threshold function over n-bit inputs. By using standard closure properties of secret sharing, one can therefore transform a secret sharing for g into a secret sharing for f with an additive cost of $O(\log n)$.

access structures. Formally, following [2], we define the *secret-sharing exponent* of a monotone function $f : \{0,1\}^n \to \{0,1\}$, denoted by $\mathbf{S}(f) := n^{-1} \cdot \log_2 \mathsf{SSize}(f)$ and define the (worst-case) *secret-sharing exponent* $\mathbf{S}$ to be $\mathbf{S} = \limsup_{n\to\infty} \max_{f\in\mathcal{M}(n)} \mathbf{S}(f)$, where $\mathcal{M}(n)$ is the family of all monotone functions over $\{0,1\}^n$ (equivalently, all n-party access structures). We prove the following theorem.

Theorem 2.1 (Main theorem)**.** *Every access structure over n parties can be realized by a secret-sharing scheme with a total share-size of $1.5^{n+o(n)}$. That is, $\mathbf{S} \leq \log \frac{3}{2} < 0.585$.*

Recall that the previous best exponent, due to [2], was 0.637. The proof of the theorem is based on two schemes for $(\beta n, n)$-downslices. The first scheme is tailored to low downslices with $\beta \leq 1/2$ and achieves an exponent of β, and the second scheme is tailored to high downslices with $\beta \geq 1/2$ and achieves an exponent of $\mathrm{H}_2(\beta) - (1-\beta)$ where H_2 is the binary entropy function. The most expensive downslice corresponds to the case where $\beta = 2/3$ and has an exponent of $\log(\frac{3}{2})$. (See Figure 2 in Section 4.) The two schemes are based on adaptation of previous tools, such as robust-CDS and combinatorial covers, to the current setting. See Section 4 for details.

Linear schemes. We also obtain a minor improvement for the exponent of linear secret-sharing schemes. Let $\mathbf{S}_\ell$ denote the *linear exponent*, that is defined analogously to $\mathbf{S}$, except that $\mathsf{SSize}(F)$ is replaced with $\mathsf{LSSize}(F)$, the minimal complexity of a linear scheme that realizes F.

Theorem 2.2 (Worst-case linear exponent)**.** *Every access structure over n parties can be realized by a linear secret sharing scheme with a total share-size of $2^{0.7576n+o(n)}$. That is, the linear exponent $\mathbf{S}_\ell$ is at most 0.7576.*

Recall that the previous best linear exponent, due to [2], was 0.762. Again the theorem is based on LSS for $(\beta n, n)$-downslices for an arbitrary density β. Unfortunately, a naive approach that mimics the proof of Theorem 2.2 yields an exponent of $\frac{1}{2} + \frac{\beta}{2}$ or, for $\beta > 0.5$, an exponent of $\mathrm{H}_2(\beta) - \frac{1}{2}(1-\beta)$. For densities larger than $1/2$, the exponent can be as large as 0.772 which is strictly larger than the exponent 0.762 that is achieved by [2]. To overcome this difficulty, we introduce several additional tools that are tailored to the linear setting. Most notably, we present a bootstrapping technique that starts with an LSS for a target downslice with a given density γ, transforms it into an LSS for upslices of various densities and then exploits the new schemes, to obtain a better LSS for the target $(\gamma n, n)$-downslice. We apply this procedure iteratively to several key values of γ, and use these pivots to propagate the improvement to all other values of β. See Section 5 for details.

2.3 Random Upslices and Mixed DNFs

Following [8], we study the complexity of randomly-chosen upslices. For this we define a family of distributions over monotone-DNFs that is parameterized by an arbitrary vector $\mathbf{k} = (k_1, \ldots, k_n)$ of non-negative integers. We sample a DNF from the $\mathbf{k}$-DNF distribution as follows: For each width parameter a, select k_a random clauses uniformly at random from the set of all possible $\binom{n}{a}$ monotone a-clauses. We prove the following theorem.

Theorem 2.3 (Average case exponents)**.** *For every non-negative vector $\mathbf{k}$, a randomly chosen $\mathbf{k}$-DNF f can be realized with complexity of $2^{0.5n+o(n)}$ except with exponentially small probability of $2^{-\Omega(n)}$. For linear schemes, we get an exponent which is strictly smaller than $2/3$.*

Observe that there is a polynomial gap between the average-case complexity and the best-known worst-case complexity. It is instructive to compare this gap with the results of Beimel and Farràs [8] who considered (1) The uniform distribution over all access structures, and (2) the uniform distribution over $(a = O(1), n)$-upslices with exactly k_a min-terms for an arbitrary value of k_a. For these distributions, [8] have established *super-polynomial* gaps between the average case complexity and the best-known worst-case complexity. Our results may indicate that such dramatic gaps are an artifact of the chosen distribution. Technically, the proof of Theorem 2.3 extends the ideas of [8] to handle arbitrary large values of $a \in [n]$. (We note that the proof of [8] suffers from an a^a dependency and so it cannot be applied to $(a = \Omega(n), n)$-upslices.)

Candidate hard distribution. We believe that random upslices form a good candidates for *exponentially-hard* distributions. Concretely, the proof of Theorem 2.3 suggests that the hardest case (for existing schemes) corresponds to the uniform distribution over $(n/2, n)$-upslices with $\sqrt{\binom{n}{n/2}} = 2^{n/2+o(n)}$ min-terms. (Equivalently, random DNF that contains $\sqrt{\binom{n}{n/2}}$ random monotone terms of width $n/2$). We believe that identifying such a candidate hard distribution is a valuable first step towards achieving further progress either at the upper-bound front or at the lower-bound front.

Is the worst-case/average-case gap real? Recall that in the average-case, we derive an exponent of 0.5 for general schemes and an exponent slightly better than $2/3$ for linear schemes, whereas the worst-case exponents are $\log(3/2)$ and slightly over $3/4$ respectively. Admittedly, we do not know whether this gap is "real", and as far as we can see, there may be a way to reduce the worst-case exponents to the average-case ones. (We do not have good candidates for separation either.) While we cannot prove the existence of such a gap, we can relate it to other central questions in the complexity of secret sharing like the power of *non-linearity* and closure under *duality*. Define the *dual* access structure of an n-party access structure f to be the n-party access structure that accepts of all sets x whose complements $\bar{x}$ are unauthorized under f, i.e., $\textsc{Dual}(f)(x) = 1 - f(\bar{x})$. We prove the following gap theorem.

Theorem 2.4 (Gap theorem)**.** *At least one of the following gaps hold:*

1. *(Duality gap) There exists an n-party monotone access structure[5] f whose secret-sharing exponent is strictly smaller than the secret-sharing exponent of its dual.*
2. *(Non-linearity gap) The (general) secret sharing exponent $\mathbf{S}$ is strictly smaller than the linear secret sharing exponent $\mathbf{S}_\ell$.*
3. *(Average-case gap) Every $\mathbf{k}$-DNF distribution can be realized, except with exponentially small probability, with an exponent $\bar{\mathbf{S}}$ that is strictly smaller than the worst-case secret sharing exponent $\mathbf{S}$.*

Let us elaborate on the first two possibilities. The first item asserts that $\mathsf{SSize}(f) < \mathsf{SSize}(\textsc{Dual}(f)) \cdot 2^{\Omega(n)}$. The *absence* of a duality gap, hereafter referred to as the *duality hypothesis*, asserts that $\mathsf{SSize}(f) = \mathsf{SSize}(\textsc{Dual}(f)) \cdot 2^{o(n)}$. That is, the primal and dual access structure have similar secret-sharing complexity up to sub-exponential difference. This hypothesis is known to hold for LSS, and, to the best of our knowledge, its status for general secret-sharing schemes is wide open. In fact, a recent paper of Csirmaz [18] refers to a stronger version of this hypothesis (e.g., $\mathsf{SSize}(f) = \mathsf{SSize}(\textsc{Dual}(f))$ as a long-standing open

[5]Formally, for asymptotic purposes one should think of f as a sequence of access structures $\{f_n : \{0,1\}^n \to \{0,1\}\}_{n \in \mathbb{N}}$.

problem. Item 1 asserts that the complexity-gap between primal and dual structures may be exponentially large.

The second item asserts that there is an exponential gap between linear-schemes and non-linear schemes even in the worst-case! While we can prove such a result for concrete cases (e.g., random slice functions), we do not know whether non-linearity significantly helps for worst-case functions, and one may guess that eventually the two exponents $\mathbf{S}_\ell$ and $\mathbf{S}$ will collapse to, say $1/2$. Item 2 asserts that this is not the case.

Proving Theorem 2.4. To prove the theorem, we show that, under the duality hypothesis, one can improve Theorem 2.3 so that a random DNF, that is sampled from an arbitrary $\mathbf{k}$-DNF distribution, can be realized with an exponent that is strictly smaller than 0.5, except with exponentially small probability. If, in addition, there is no Average-case gap, we get that the worst-case exponent $\mathbf{S}$ is smaller than 0.5. Since it is known that the linear exponent $\mathbf{S}_\ell$ cannot be smaller that 0.5 (e.g., by counting), we conclude that the linear exponent must be strictly larger than the general exponent. (See Section 6.)

3 Preliminaries

General. By default, all logarithms are taken to base 2. For positive integers $k \leq n$, we let $\binom{n}{\geq a} := \sum_{a \leq i \leq n} \binom{n}{i}$. We use the following standard estimate for the binomial coefficients

$$\binom{n}{k} = \Theta(k^{-1/2} 2^{\mathrm{H}_2(k/n)n}) \tag{1}$$

where $\mathrm{H}_2(\cdot)$, denotes the *binary entropy function*, that maps a real number $\alpha \in (0,1)$ to $\mathrm{H}_2(\alpha) = -\alpha \log \alpha - (1-\alpha)\log(1-\alpha)$ and is set to zero for $\alpha \in \{0,1\}$.

Secret sharing. Standard background on secret-sharing schemes and on slices, multislices, downslices, and upslices, are deferred to Appendix A. Let us just mention the following complexity conventions. Given a (monotone) access structure $f : \{0,1\}^n \to \{0,1\}$ we let $\mathsf{SSize}(f) := \min_{\mathcal{D} \text{ realizes } f} |\mathcal{D}|$, where $|\mathcal{D}|$ denotes the total share size of a secret-sharing scheme $\mathcal{D}$. The *exponent* of F, denoted by $\mathbf{S}(F)$ is $n^{-1} \cdot \log_2 \mathsf{SSize}(F)$. If $\mathcal{F}$ is a collection of n-party access structures then

$$\mathsf{SSize}(\mathcal{F}) := \max_{f \in \mathcal{F}} \mathsf{SSize}(f), \qquad \text{and} \qquad \mathbf{S}(\mathcal{F}) := \max_{f \in \mathcal{F}} \mathbf{S}(f).$$

When $\mathcal{F} = \{\mathcal{F}_n\}$ is a sequence of collections $\mathcal{F}_n$ of n-party access structures we think of $\mathsf{SSize}(\mathcal{F})$ as a function of n, and define the *secret-sharing exponent* $\mathbf{S}(\mathcal{F})$ to be $\mathbf{S}(\mathcal{F}) := \limsup_{n \to \infty} \mathbf{S}(\mathcal{F}_n)$. All these definitions naturally extend to the linear setting as well.

We denote by $\mathbf{D}(b,n)$ (resp., $\mathbf{D}_\ell(b,n)$) the secret-sharing exponent (resp., the LSS exponent) of (b,n)-downslices and by $\mathbf{D}(\beta)$ (resp., $\mathbf{D}_\ell(\beta)$) the secret-sharing exponent (resp., the LSS exponent) of $(\beta n, n)$-downslices. The notation $\mathbf{U}(a,n), \mathbf{U}_\ell(a,n), \mathbf{U}(\alpha)$ and $\mathbf{U}_\ell(\alpha)$ is defined analogously for the secret-sharing exponents and LSS exponents of (a,n)-upslices and $(\alpha n, n)$-upslices. The secret-sharing exponents and LSS exponents of $(a : b, n)$-multislices and $(\alpha n : \beta n, n)$-multislices are denoted by $\mathbf{M}(a : b, n), \mathbf{M}_\ell(a : b, n), \mathbf{M}(\alpha : \beta)$ and $\mathbf{M}_\ell(\alpha : \beta)$.

3.1 Covers

We will make use of the following combinatorial concept of "covers".

Definition 3.1 (Covering a slice)**.** *We say that a collection of subsets $\mathcal{G} = \{G_i\}$ over a ground set $[n]$* upcovers a slice *t if for every set A of size t, exists a set $G_i \in \mathcal{G}$ such that $A \subseteq G_i$. Analogously, we say that $\mathcal{G}$* downcovers a slice *t, if for every set A of size t, exists a set $G_i \in \mathcal{G}$ such that $G_i \subseteq A$.*

We start by introducing a fact about *combinatorial covering designs* by Erdős and Spenser:

Fact 3.2 ([20])**.** *For every positive integers $a \leq b \leq n$, there exists a family $\mathcal{G} = \{G_i\}_{i=1}^{L}$ of b-subsets of $[n]$ that upcovers the slice a where $\mathcal{G}$ is of size $L = L(n,a,b) \leq \left[\binom{n}{a}/\binom{b}{a}\right]\left[1+\log\binom{b}{a}\right]$.*

We will make use of the following dual fact.

Fact 3.3. *For every positive integers $a \leq b \leq n$, there exists a family $\mathcal{G} = \{G_i\}_{i=1}^{L}$ of a-subsets of $[n]$ that downcovers the slice b where $\mathcal{G}$ is of size $L = L(n,a,b) \leq \left[\binom{n}{n-b}/\binom{n-a}{n-b}\right]\left[1+\log\binom{n-a}{n-b}\right]$.*

Moreover, for some constant $C > 1$, a random family $\mathcal{G}$ of a-subsets of n of size at least $\bar{L}(n,a,b) = \left[\binom{n}{a}/\binom{b}{a}\right] \cdot n$ downcovers the slice b except with probability C^{-n}.

The reader should note that $\left[\binom{n}{a}/\binom{b}{a}\right] = \left[\binom{n}{n-b}/\binom{n-a}{n-b}\right]$.

Proof. Whenever a collection $\{G_i\}_{i=1}^{L}$ upcovers the slice a, the collection of complement sets $\left\{\bar{G}_i\right\}_{i=1}^{L}$ *downcovers* the slice $n-a$. Fact 3.2 therefore implies the first part.

For the "Moreover" part. Sample $\mathcal{G}$ by sampling each G_i uniformly at random among all a-subsets of $[n]$. Fix some b-subset $B \subseteq [n]$. For every $i \in [L]$, the probability that $G_i \subseteq B$ is $p = \binom{b}{a}/\binom{n}{a}$, and therefore

$$\Pr[\forall i, G_i \nsubseteq B] \leq (1-p)^L = (1-p)^{n/p} < e^{-n},$$

where the equality follows by noting that $\bar{L}(n,a,b) \cdot p = n$. Therefore, by a union bound over all sets of size b, the probability that there is some b-set that does not contain any G_i is at most $\binom{n}{b} \cdot e^{-n} < 2^n \cdot e^{-n} = 1/C^n$ for $C = e/2$. □

4 General secret-sharing for downslices

Recall that $\mathbf{D}(\beta)$ and $\mathbf{D}_\ell(\beta)$ denote the secret-sharing exponent and LSS exponent of $(\beta n, n)$-downslices. The classical CNF-based scheme [26] that enumerates over all of the max-terms of size βn, yields an LSS exponent of $\mathrm{H}_2(\beta)$. One can also get an exponent of 0.637 via the general-purpose secret-sharing scheme of [2]. In this section, we improve these results and show that $\mathbf{D}(\beta) \leq \log(3/2)$ for any β.

Theorem 4.1. *Every n-party downslice access structure can be realized with complexity of $2^{\log(3/2)n+o(n)}$. Additionally, for LSS, $\mathbf{D}_\ell(\beta) \leq \frac{1}{2} + \frac{\beta}{2}$ and, for $\beta > 0.5$, it holds that $\mathbf{D}_\ell(\beta) \leq \mathrm{H}_2(\beta) - \frac{1}{2}(1-\beta)$.*

The linear exponent will be improved in the next section. Before proving Theorem 2.1, we will need the following simple observation whose proof is deferred to Appendix C.1.

Observation 4.2. *Let f be an access structures over n parties, and assume that F_i, the i-downslice of f, can be realized (resp., linearly realized) with total share size of S_i for every $i \in [0,n]$. Then, f can be realized (resp., linearly realized) with share size of $\sum_{i=0}^{n} S_i \leq n \max_i S_i$.*

We can now prove Theorem 2.1.

Proof of Theorem 2.1. Fix some access structure f over n parties and let F_b denote the (b,n)-downslice of f. By Theorem 4.1 the access structure F_b can be realized with total share size S_b of at most $2^{\log\left(\frac{3}{2}\right)n+o(n)}$, and so by Observation 4.2, f can be realized with complexity of $\max_b(S_b)\cdot n \leq 2^{\log\left(\frac{3}{2}\right)n+o(n)}$. □

The proof of Theorem 4.1 is based on the following two lemmas.

Lemma 4.3 (low-density downslices)**.** *Secret sharing for (b,n)-downslices can be realized (resp., linearly realized) with share size of $2^{b+o(n)}$ (resp., $2^{b/2+n/2+o(n)}$). Consequently, for any constant $\beta \in [0,1]$, it holds that*

$$\mathbf{D}(\beta) \leq \beta \qquad \textit{and} \qquad \mathbf{D}_\ell(\beta) \leq \frac{1}{2}+\frac{\beta}{2}.$$

The proof of Lemma 4.3 appears in Section 4.1 and it is based on a scheme for multislices that will be employed also in the next sections. Lemma 4.3 presents an improvement over previously known schemes for (b,n)-downslices in the regime $b \in [0, 0.637n]$, i.e., as long as the level b is smaller than the exponent of [2]. Higher levels, for which Lemma 4.3 provides no improvement, are treated by the following lemma.

Lemma 4.4 (high-density downslices)**.** *For every integers n and $b \in (0.5n, n]$, every (b,n)-downslice can be realized with share size of*

$$\left[\binom{n}{n-b}/\binom{2n-2b}{n-b}\right]\cdot 2^{n-b+o(n)},$$

and can be realized by a linear scheme with share size

$$\left[\binom{n}{n-b}/\binom{2n-2b}{n-b}\right]\cdot 2^{(3n-3b)/2+o(n)}.$$

Consequently, for every constant $\beta \in (0.5, 1]$, it holds that

$$\mathbf{D}(\beta) \leq \mathrm{H}_2(\beta)-(1-\beta) \qquad \textit{and} \qquad \mathbf{D}_\ell(\beta) \leq \mathrm{H}_2(\beta)-\frac{1}{2}(1-\beta).$$

We note that the maximal value of $\mathbf{D}(\beta)$ is $\log\left(\frac{3}{2}\right)$ and it is obtained when $\beta = 2/3$. Therefore, a combination of Lemma 4.3 and Lemma 4.4 yield Theorem 4.1. The proof Lemma 4.4 is deferred to Section 4.2 and is based on a general cover-reduction that will be also useful for the next sections.

The exponents of the above lemmas together with the CNF-based exponent and the exponent of [2] are depicted in Figure 2.

4.1 Low-density downslices via multislices

Secret sharing schemes for $(a : b, n)$ multislice access structures were considered in [28, 1, 2], for the special cases of "mid-slices" where $a = \left(\frac{1}{2}-\delta\right)n$, $b = \left(\frac{1}{2}+\delta\right)n$ for some constant $\delta \in [0, 0.5]$. It is possible to generalize the scheme of [2] that was originally designed to handle mid-slices to handle any pair $a < b \in [n]$ as follows. Recall that, for every constants $0 \leq \alpha < \beta \leq 1$, we let $\mathbf{M}(\alpha : \beta)$ (resp., $\mathbf{M}_\ell(\alpha : \beta)$) denote the exponent (resp., LSS exponent) of $(\alpha n : \beta n, n)$-multislice access structures.

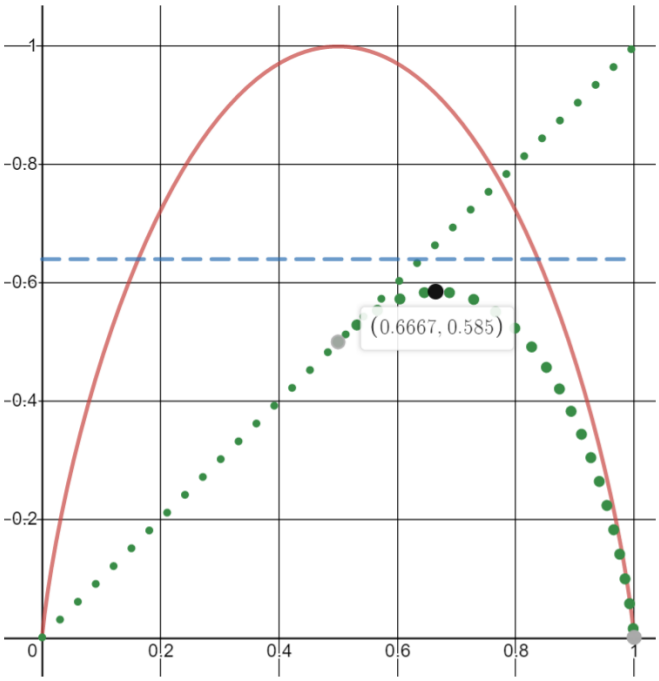


Figure 2: A description of the exponents of four general schemes for $(\beta n, n)$-downslices. The horizontal axis represents the density β of the slice, and the vertical axis represents the resulting exponents. The solid red curve corresponds to the exponent of the CNF-based scheme. The constant exponent of the general access structures scheme of [2] appears as the dashed blue line. The dotted green straight line represents the exponent that is achieved by the scheme of Lemma 4.3, and the dotted green curve which starts at $x = 0.5$ represents the scheme for downslices of Lemma 4.4.

Lemma 4.5 (multislice lemma)**.** *For every $a < b \in [n]$, every $(a : b, n)$-multislice access structure can be realized by a secret-sharing scheme with share size $\binom{b}{\geq a} \cdot 2^{o(n)}$ and by a linear scheme with share size $\sqrt{\binom{b}{\geq a}} \cdot 2^{n/2+o(n)}$. Consequently, for every constants $0 \leq \alpha < \beta \leq 1$, the exponent $\mathbf{M}(\alpha : \beta)$ of $(\alpha n : \beta n, n)$-multislice access structures satisfies*

$$\mathbf{M}(\alpha : \beta) \leq \begin{cases} \beta \, \mathrm{H}_2\left(\frac{\alpha}{\beta}\right) & \text{if } \alpha > \beta/2 \\ \beta & \text{if } \alpha \leq \beta/2 \end{cases},$$

and, for the linear case, the exponent $\mathbf{M}_\ell(\alpha : \beta)$ satisfies

$$\mathbf{M}_\ell(\alpha : \beta) \leq \begin{cases} \frac{1}{2} + \frac{\beta}{2} \cdot \mathrm{H}_2\left(\frac{\alpha}{\beta}\right) & \text{if } \alpha > \beta/2 \\ \frac{1}{2} + \frac{\beta}{2} & \text{if } \alpha \leq \beta/2 \end{cases}.$$

The proof follows the exact steps of the proof of Lemma 5.10 from [2] except that we use a more general setting of parameters. See Appendix B for details. By using multislices to implement downslices, we derive Lemma 4.3.

Proof of Lemma 4.3. Let F be a (b, n)-downslice and let F' be the $(0 : b, n)$-multislice of F. Observe that F equals F', and so by Lemma 4.5 it can be implemented with the desired share sizes since $\binom{b}{\geq 0} = 2^b$. □

4.2 Reducing high-density downslices to low downslices

In order to prove Lemma 4.4 we reduce the problem of realizing (b, n)-downslices for $b > 0.5n$ to the problem of realizing (b', n')-downslices over a smaller set of parties $n' < n$ and for density $b' = n'/2$. This is, in fact, a special case of the following more general reduction that will be also applied in its full power later in Section 5.

Lemma 4.6 (cover reduction lemma)**.** *Let $v < b \leq n$ be positive integers. If $(b - v, n - v)$-downslices can be realized (resp., linearly realized) with share size $z(b - v, n - v)$ then (b, n)-downslices can be realized (resp., linearly realized) with share size of*

$$\left[\binom{n}{n-b}/\binom{n-v}{n-b}\right]\left[1+\log\binom{n-v}{n-b}\right]\cdot z(b-v,n-v) \tag{2}$$

Consequently, for every constants $0 < \alpha \leq \beta < 1$, if $(\alpha m, m)$-downslices can be realized (resp., linearly realized) with exponent of $z'(\alpha)$ then $(\beta n, n)$-downslices can be realized with an exponent of

$$\mathrm{H}_2(\beta) - (1-\beta)\left(\frac{\mathrm{H}_2(\alpha) - z'(\alpha)}{1-\alpha}\right). \tag{3}$$

The proof of Lemma 4.6 is deferred to Section 4.3.

Remark 4.7 (Generalizations of Lemma 4.6 and completeness of downslices)**.** *The proof of Lemma 4.6 relies on downcovers. One can use upcovers to prove a similar lemma that reduces low-density downslices to high-density downslices. Moreover, both, Lemma 4.6 and its low-to-high variant, can be also proved for the dual setting of upslices. So overall, Lemma 4.6 represents four possible transformations. (The other three will not be used in this work.) By combining these reductions with the completeness of downslices/upslices (Observation 4.2), we conclude that it is possible to reduce a general access structures to downslices or upslices of specific density.*

We are now ready to realize high-density downslices.

Proof of Lemma 4.4. Let f be a (b, n)-downslice with $b \in (0.5n, n]$. Let $v = 2b - n$, and observe that $v \in (0, b]$ since $b \in (0.5n, n]$. We use the *cover reduction lemma* (Lemma 4.6) to realize f based on secret-sharing scheme for downslices with parameters $(b-v, n-v) = (n-b, 2n-2b)$.[6] The latter can be realized (non-linearly) with share size of $2^{n-b+o(n)}$ by Lemma 4.3. Overall, Lemma 4.6 yields a (non-linear) scheme for f with total share size of

$$\left[\binom{n}{n-b}/\binom{2n-2b}{n-b}\right]\left[1+\log\binom{2n-2b}{n-b}\right]\cdot 2^{n-b+o(n)}$$

which equals $\left[\binom{n}{n-b}/\binom{2n-2b}{n-b}\right]\cdot 2^{n-b+o(n)}$. In the linear case, we realize $(n-b, 2(n-b))$-downslices using the linear secret-sharing scheme promised by Lemma 4.3. This results in the desired share size:

$$\left[\binom{n}{n-b}/\binom{2n-2b}{n-b}\right]\left[1+\log\binom{2n-2b}{n-b}\right]\cdot 2^{(3n-3b)/2+o(n)}$$

which equals $\left[\binom{n}{n-b}/\binom{2n-2b}{n-b}\right]\cdot 2^{(3n-3b)/2+o(n)}$. If we plug in $b = \beta n$ for a constant $\beta \in (0.5, 1]$ and make use of (1), the general and linear share sizes translate to $2^{(\mathrm{H}_2(\beta)-2(1-\beta)+(1-\beta))n+o(n)}$ and $2^{(\mathrm{H}_2(\beta)-2(1-\beta)+\frac{3}{2}(1-\beta))n+o(n)}$, leading to the desired exponents. □

[6] This choice of v can be shown to be optimal for both for the general and linear case.

4.3 Proof of the cover reduction

The proof of Lemma 4.6 is based on the following construction.

Construction 4.8. *Let F be a (b, n)-downslice. We share the secret s according to F as follows:*

1. *Pick a family $\mathcal{G} = \{G_i\}_{i=1}^{L}$ of sets of size v that downcovers the slice b.*
2. *For every $G_i \in \mathcal{G}$ define the access structure F_i over the participant's set $[n] \setminus G_i$ as follows:*
$$F_i(x') = F(x' \cup G_i)$$
where x' is viewed as a subset of $[n] \setminus G_i$.
3. *Split the secret s with an (L-out-of-L) LSS scheme to random shares $s_1, \ldots, s_L \in \{0,1\}$ such that $s_1 \oplus \cdots \oplus s_L = s$. For every $1 \leq i \leq L$ share s_i according to the access structure F_i.*

Claim 4.9. *Construction 4.8 realizes the access structure F.*

Proof. It suffices to show that $F = \bigwedge_i F_i$. Assume that x is authorized under F, we will show that it is also authorized by F_i for every i. Fix i and let $x' = x \cap \bar{G}_i$, we claim that x' is authorized under F_i. Indeed, by definition, $F_i(x') = F(x' \cup G_i)$ which is 1 since $x' \cup G_i$ contains x and is therefore authorized under F.

Next, assume that x is unauthorized under F. Since F is a (b, n)-downslice, x must be a subset of some unauthorized set B of size b, and by the down-covering property there exists an index $i \in [L]$ such that G_i is a subset of the same set B. Again letting $x' = x \cap \bar{G}_i$, we then get that $x' \cup G_i \subseteq B$, and therefore $F_i(x') = F(x' \cup G_i) = 0$. The claim follows. □

Claim 4.10. *For every $1 \leq i \leq L$, F_i is a $(b - v, n - v)$-downslice access structure.*

Proof. Fix a maximal unauthorized set $x' \subset [n] \setminus G_i$ of F_i. We show that x' contains exactly $b - v$ parties. For this, it suffices to show that $x = x' \cup G_i$ is a maximal unauthorized set of F. By definition, $x' \cup G_i$ is unauthorized under F. Moreover, every strict super-set y of $x' \cup G_i$ must be F-authorized. Otherwise, if y is F-unauthorized then the set $y' = y \cap \bar{G}_i$ must be also F_i-unauthorized and since y' is a strict-super set of x', this contradicts the fact that x' is max-unauthorized under F_i. Finally, since any max-term of F is of size b, the max-terms of F_i is of size $b - v$. □

Share size analysis: Due to Fact 3.3 we can pick a family $\mathcal{G}$ for step 1 of the scheme of size

$$L = \left[\binom{n}{n-b} / \binom{n-v}{n-b} \right] \left[1 + \log \binom{n-v}{n-b} \right],$$

and for every set in $\mathcal{G}$ we use a secret sharing scheme with share size $z(b - v, n - v)$, which results in the desired share size. This completes the proof of the first part of Lemma 4.6.

The "Consequently" part follows immediately by plugging-in $b = \lceil \beta n \rceil$, $v = \lceil \frac{\beta - \alpha}{1 - \alpha} n \rceil$, and noting that $\alpha_n = \frac{b-v}{n-v}$ converges to α when n goes to infinity. Observe that the exponent of $(\alpha_n(n - v), (n - v))$-downslices is the same as the exponent, $z'(\alpha)$, of α-downslice.[7] Now, by applying (1) and noting that $\beta_n = b/n = \lceil \beta n \rceil / n$ converges to β when n grows, we derive an exponent of

$$\mathrm{H}_2(\beta) - \frac{1 - \beta}{1 - \alpha} \mathrm{H}_2(1 - \alpha) + z'(\alpha) \cdot \frac{1 - \beta}{1 - \alpha},$$

which equals the expression in (3), as required.

[7] More generally, whenever $|g(n) - g'(n)| = o(n)$, the exponent of $(g(n), n)$-downslices is equal to the exponent of $(g'(n), n)$-downslices. To see this, observe that $(g(n), n)$-downslices can be written as a sub-exponential formula over $(g'(n), n)$-downslices.

5 Linear secret sharing for downslices

In this section we present a LSS for general access structures with an exponent of 0.7576 (Theorem 2.2). As in Section 4, this is done by showing that downslices can be linearly realized with this exponent.

Theorem 5.1. *Every n-party downslice access structure can be linearly realized with complexity of $2^{0.7576n+o(n)}$.*

The proof of Theorem 5.1 is based on a bootstrapping procedure which strongly exploits the *duality* properties of LSS.

Section Organization In Section 5.1 we describe a property of linear schemes for *dual access structures*. In Section 5.2 we reduce downslices to upslices and vice versa. In Section 5.3 we iteratively employ these reductions together with tools from the previous section, to obtain a LSS for downslices with lower exponents than before. Lastly in Section 5.4 we prove Theorem 2.2. Some additional optimizations for low downslices (that do not affect Theorem 5.1) appear in Appendix C.3.

5.1 Exploiting duality

Definition 5.2 (Dual Access structures)**.** *The* dual *access structure of an n-party access structure f is an n-party access structure, denoted by $\text{DUAL}(f)$, that consists of all sets x whose complements $\bar{x}$ are unauthorized under f. Viewing f as a function, this means that for every input x*

$$\text{DUAL}(f)(x) = 1 - f(\bar{x}).$$

Consequently, the complement of every min-term of f is a max-term of the dual $\text{DUAL}(f)$, and the complement of every max-term of f is a min-term of $\text{DUAL}(f)$.

We make the following observation.

Fact 5.3 (Duals of slice access structures)**.** *Let f be an access structure. Then:*

1. *If f is an (a, n)-slice then its dual is an $((n-a), n)$-slice.*
2. *If f is an (a, n)-upslice then its dual is a $((n-a), n)$-downslice, and vice versa.*
3. *If f is an $(a : b, n)$-multislice then its dual is an $(n-b : n-a, n)$-multislice.*

It is known that for linear schemes the total share size of an access structure is equal to the total share size of its dual.

Fact 5.4 ([22])**.** *A linear secret sharing scheme for an access structure f can be converted into a linear scheme for the dual access structure $\text{DUAL}(f)$ with the same total share size.*

By Fact 5.4, Fact 5.3, Lemma 4.3, and Lemma 4.4, we get the following corollary.

Corollary 5.5 (Duality reduction)**.** *For every integers $a \leq n$, the LSS complexity of the family of (a, n)-downslices equals to the LSS complexity of the family $(n-a, n)$-upslices.*

By Lemma 4.4 and Lemma 4.3, for any constant $0 < \alpha < 1$, the family of $(\alpha n, n)$-upslices can be linearly realized with an exponent of

$$\mathbf{U}_\ell(\alpha) \leq \begin{cases} \mathrm{H}_2(\alpha) - \frac{1}{2}(\alpha) & \text{if } \alpha < \frac{1}{2} \\ \frac{1}{2} + \frac{1-\alpha}{2} & \text{if } \alpha \geq \frac{1}{2} \end{cases}.$$

5.2 High-density downslices from low-density upslices and mid-range multislices

In the following lemma we improve the exponent of a (c,n)-downslice f by decomposing it into two access structures: one that has the same min-terms as f up to a specific size u (which will be realized using low-density upslices), and one that is simply the $(u:c,n)$ multislice of f.

Lemma 5.6 (Reducing downslices to upslices)**.** *Let $u \leq c < n$ be integers. Given a LSS that realizes (a,n)-upslices with an exponent of $\mathbf{U}'_\ell(a,n)$ and a LSS that realizes the $(u:c,n)$-multislices with an exponent of $\mathbf{M}'_\ell(u:c,n)$, there exists a LSS that realizes (a,n)-downslices with an exponent of*

$$\mathbf{D}_\ell(c,n) \leq \min_u \left[\max \left(\max_{i \leq u} \left\{ \mathbf{U}'_\ell(i,n) \right\}, \mathbf{M}'_\ell(u:c,n) \right) \right] + o(1),$$

where $o(1)$ stands for a quantity that tends to zero as n increases, regardless of the values of u and c.

Proof. It suffices to show that for every $u \leq c$ any downward-induced (c,n) access structure f can be realized with an exponent of

$$\max \left(\max_{i \leq u} \left\{ \mathbf{U}'_\ell(i,n) \right\}, \mathbf{M}'_\ell(u:c,n) \right) + o(1). \tag{4}$$

Fix some $u \in [0,c]$. Define $f_{u,c}$ to be the $(u:c,n)$-multislice of f, and $f^{\mathrm{up}}_{0,u}$ as the disjunction of the first u upslices of f. More formally, $f^{\mathrm{up}}_{0,u} := \bigvee_{i=0}^{u} f_i$ where f_i is the i-upslice of f. Clearly, $f^{\mathrm{up}}_{0,u}$ can be linearly realized with an exponent of $\max_{i \leq u} \{\mathbf{U}'_\ell(i,n)\} + O(n^{-1} \log n)$ (just duplicate the secret u times and deal the i-th copy via the access structure f_i). Consequently, the access structure $f^{\mathrm{up}}_{0,u} \vee f_{u,c}$ can be linearly realized with an exponent of (4). We complete the proof by showing that $f = f^{\mathrm{up}}_{0,u} \vee f_{u,c}$.

For inputs x such that $|x| \leq u$, $f(x) = f^{\mathrm{up}}_{0,u}(x)$ and $f_{u,c}(x) = 0$. For inputs x such that $u < |x| \leq c$, it holds that (1) $f(x) = f_{u,c}(x)$, and (2) $f^{\mathrm{up}}_{0,u} \leq f$ since the min-terms of $f^{\mathrm{up}}_{0,u}$ are a subset of those of f. We therefore conclude that for such inputs $f(x) = f^{\mathrm{up}}_{0,u}(x) \vee f_{u,c}(x)$. Finally, for inputs x with $|x| > c$, both $f(x)$ and $f_{u,c}(x)$ take the value 1, and so equality holds in this case as well. □

5.3 Bootstrapping (c,n)-downslices

In this section we construct an LSS for (c,n)-downslices via an iterative process. In each iteration, we will start with an LSS for (c,n)-downslices and end-up with a new LSS for (c,n)-downslices whose exponent is at least as good as the one achieved in the previous iteration. Each iteration i is composed of three steps: (1) We generate LSS for all downslices of density larger than c; (2) We generate LSS for all upslices of density smaller than $n-c$; (3) We use the current schemes for (u,n)-upslices for $u < u_i$ for some parameter u_i to obtain a new LSS for (c,n)-downslices. Note that the target slice c is kept fixed across iterations. The structure of a single iteration that consists of the three reductions is depicted below. The process is formally defined in Construction 5.7.

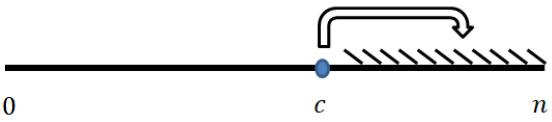
Construction 5.7 (Bootstrapping downslices)**.** *Given integer n, a target slice $c < n$, and time-bound $t \in \mathbb{N}$, initialize an LSS for (c,n)-downslice based on Theorem 4.1 and set $\mathbf{D}_\ell(c,n)[0]$ to be its exponent, and repeat the following steps for $i \in [t]$ iterations:*

1. *For every $d \in (c,n]$, apply the cover reduction (Lemma 4.6) and transform the current LSS for (c,n)-downslices to an LSS for (d,n)-downslices with exponent*

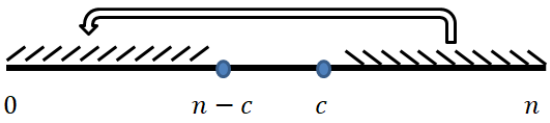
$$\mathbf{D}_\ell(d,n)[i+1] = \mathrm{H}_2(d/n) - (1-d/n)\left(\frac{\mathrm{H}_2(c/n) - \mathbf{D}_\ell(c,n)[i]}{1-c/n} \right) + o(1). \tag{5}$$

Three reductions of Construction 5.7

1. The cover reduction (Lemma 4.6): Transform a scheme for (c,n)-downslices with to a scheme for downslices with higher density.



2. Duality reduction: Transform high downslices to low upslices (Corollary 5.5): Transform a scheme for downslices of high density in $(c,n]$ to a scheme for upslices with low density in $[0,n-c)$.



3. Reducing high downslices to low upslices (Lemma 5.6): For an integer $u \leq c$, transform a scheme for upslices in the range $[0,u]$ and a scheme for the $(u:c,n)$-multislice to a scheme for the c-downslice.

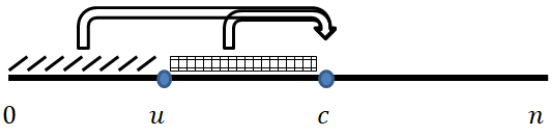


Figure 3: We place all slices on an horizontal axis with an arrow which represents the direction of the transformation.

2. *For every $d \in (c,n]$, apply the duality reduction (Corollary 5.5) and transform the LSS for (d,n)-downslices to an LSS for $(n-d,n)$-upslices with an exponent of*

$$\mathbf{U}_\ell(n-d,n)[i+1] = \mathbf{D}_\ell(d,n)[i+1]. \tag{6}$$

3. *Construct an LSS for (c,n)-downslices by applying Lemma 5.6 where (j,n)-upslices for every $j < n-c$ are instantiated with the LSS that were derived in the previous step. Accordingly, the new LSS for (c,n)-downslices has an exponent of*

$$\mathbf{D}_\ell(c,n)[i+1] = \min_{u \leq c}\left[\max\left(\max_{j \leq u}\mathbf{U}_\ell(j,n)[i+1], \mathbf{M}^0_\ell(u:c,n)\right)\right] + o(1). \tag{7}$$

where $\mathbf{M}^0_\ell(a:b,n)$ denotes the linear exponent of $(a:b,n)$-multislice access structures that is achieved in Lemma 4.5.

Now by Lemma 4.6, Corollary 5.5 and Lemma 5.6, for any parameter t, Construction 5.7 yields an LSS for (c,n)-downslices. For a given $\gamma \in [0,1]$ and constant t, we can define a function $\Phi_t(\gamma)$ that captures the asymptotic exponent that is achieved for $(\gamma n,n)$-downslices after running Construction 5.7 for t iterations. Formally,

$$\Phi_0(\gamma) := \begin{cases} \frac{1}{2} + \frac{1}{2}\gamma & \text{if } \gamma \leq \frac{1}{2} \\ \mathrm{H}_2(\gamma) - \frac{1}{2}(1-\gamma) & \text{if } \gamma > \frac{1}{2} \end{cases}$$

is set to be the exponent derived from Theorem 4.1. Then by (5), (6) and (7)

$$\Phi_{i+1}(\gamma) := \min_{\upsilon \in [0,\gamma]}\left[\max\left(\max_{\chi \in [0,\upsilon]}(\mathbf{U}'_\ell(\chi,\gamma), \mathbf{M}'_\ell(\upsilon,\gamma)\right)\right],$$

where

$$\mathbf{U}'_\ell(\chi,\gamma) := \mathrm{H}_2(\chi) - \chi\left(\frac{\mathrm{H}_2(\gamma)-\Phi_i(\gamma)}{1-\gamma}\right),$$

and

$$\mathbf{M}'_\ell(\upsilon,\gamma) := \begin{cases} \frac{1}{2}+\frac{1}{2}\gamma\,\mathrm{H}_2(\upsilon/\gamma) & \text{if } \gamma/2<\upsilon<\gamma \\ \frac{1}{2}+\frac{1}{2}\gamma & \text{if } \upsilon<\gamma/2 \end{cases}.$$

We therefore conclude that

Lemma 5.8. *For every constant $t \in \mathbb{N}$ and constant $\gamma \in [0,1]$, and for all n's, the LSS constructed by invoking Construction 5.7 for t steps on $(\gamma n, n)$, has an exponent of $\Phi_t(\gamma)+\epsilon(n)$ where $\epsilon(n)$ tends to zero when n grows.*

Lemma 5.8 suffices for proving Theorem 5.1 (see Section 5.4).

Remark 5.9. *Assuming the* duality hypothesis*, the same bootstraping idea can be employed for general (non-linear) schemes. However, it does not yield better general exponents than the ones shown in the previous section for any downwslice .*

5.4 Proof of Theorem 5.1

A natural approach for proving Theorem 5.1 would be to run the bootstrapping scheme for each possible target $c \in [n]$, and then glue together all the (c,n)-downslices. This approach fails since the exponents of some slices will still be too high. Instead we will apply Construction 5.7 for only two concrete values of c and use the cover reduction to handle downslices of higher densities. Downslices with low density will be treated by Lemma 4.5. Details follow.

By applying Construction 5.7 with $\gamma_1 = 0.5$ and $\gamma_2 = 0.535$ for $t = 7$ times, we derive the following claim from Lemma 5.8.

Claim 5.10. *Set $\gamma_1 = 0.5$ and $\gamma_2 = 0.535$. The family of $(\gamma_1 n, n)$-downslices and the family of $(\gamma_2 n, n)$-downslices can be linearly realized with exponents of $z_1 = 0.736$ and $z_2 = 0.748$.*

Let f be a (d,n)-downslice. We distinguish between the following cases.

1. For $d \in [0, 0.5n]$ linearly realize f by Lemma 4.3 with a maximal exponent of 0.75.
2. For $d \in [0.5n, 0.535n]$ linearly realize f by applying the cover reduction (Lemma 4.6) instantiated with the LSS for $(0.5n, n)$-downslices of Claim 5.10. This yields an exponent of
$$\mathrm{H}_2(d/n) - (1-d/n)\frac{\mathrm{H}_2(\gamma_1)-z_1}{1-\gamma_1} < \mathrm{H}_2(d/n) - 0.528(1-d/n) \tag{8}$$
which is upper-bounded by 0.751 for $d \in [0.5n, 0.535n]$.
3. For $d \in [0.535n, n]$ linearly realize f by applying the cover reduction (Lemma 4.6) instantiated with the LSS for $(0.535n, n)$-downslices of Claim 5.10. This yields an exponent of
$$\mathrm{H}_2(d/n) - (1-d/n)\frac{\mathrm{H}_2(\gamma_2)-z_2}{1-\gamma_2} < \mathrm{H}_2(d/n) - 0.534(1-d/n) + o(1) \tag{9}$$
which is upper-bounded by 0.7576 for $d \in [0.535n, n]$.

The proof of Theorem 5.1 follows.

Remark 5.11. *A more careful analysis allows to obtain a better exponent for values of $d \le 0.535n$. We sketch this result in Appendix C.3.*

6 Random upslices

Recall that, for a vector of non-negative integers $\mathbf{k} = (k_1, \ldots, k_n)$, the $\mathbf{k}$-DNF distribution is defined by selecting, for each parameter a, k_a clauses uniformly at random from the set of all possible $\binom{n}{a}$ monotone a-clauses. (We allow repetitions though this choice does not change the results.) When $\mathbf{k} = (0^{a-1}k_a0^{n-a})$ is supported on a single level a, we refer to this distribution as a random (a, k_a, n)-upslice. Observe that this special case is *complete* in the following sense.

Observation 6.1. *For every $\mathbf{k} = (k_1, \ldots, k_n)$ the following holds. If, for every $a \in [n]$, a random (a, k_a, n)-upslice can be realized (resp., linearly realized) with total share size of at most S_a except with probability ϵ, then, a random $\mathbf{k} = (k_1, \ldots, k_n)$ can be realized (resp., linearly realized) with an complexity of at most $\sum S_a$ except with probability $n\epsilon$.*

Proof. A random $\mathbf{k}$-DNF f can be written as $f = \bigvee_a f_a$ where each f_a is a random (a, k_a, n)-upslice. Hence, we can share f by duplicating the secret n times and sharing the ath copy according to f_a. The claim follows by applying union-bound. □

We can therefore reduce Theorem 2.3 to the following refined statements (Theorem 6.2 and Theorem 6.3) about random (a, k_a, n)-upslices. Specifically, we prove the following theorem in Section 6.1.

Theorem 6.2 (random upslices)**.** *Let $a \in [n]$, $k \leq \binom{n}{a}$ and let f be a randomly chosen (a, k_a, n)-upslice. Then, with probability $1 - 2^{-\Omega(n)}$,*

$$\mathsf{SSize}(f) \leq \begin{cases} \sqrt{\binom{n}{\alpha^* n}} \cdot 2^{o(n)} & \text{if } a \in [0, \alpha^* n] \\ \sqrt{\binom{n}{a}} \cdot 2^{o(n)} & \text{if } a \in [\alpha^* n, n] \end{cases},$$

where $\alpha^* \sim 0.157$ is the root of $0.25\,\mathrm{H}_2(\alpha) - \alpha$. Moreover, under the duality hypothesis*, with probability $1 - 2^{-\Omega(n)}$, the function f can be realized with an exponent of at most $\frac{1}{2}\,\mathrm{H}_2(\lambda) \sim 0.491$, where λ is the root of $\frac{1}{2}\,\mathrm{H}_2(\lambda) - (1-\lambda)\,\mathrm{H}_2(\frac{\lambda}{1-\lambda})$.*

The first part of the theorem (without the duality hypothesis), shows that, for every density $\alpha \in [0, 1]$, a random $(\alpha n, n)$-upslice can be realized, whp, with an exponent of 0.5. Thus, by Observation 6.1, the non-linear part of Theorem 2.3 follows. We further mention that we did not attempt to optimize the exponent for $a \leq \alpha^* n$, and indeed a better exponent can be achieved in this case.

Moving on to the second ("Moreover") part of the theorem, recall that the duality hypothesis asserts that for every $f = \{f_n\}$, it holds that $\mathsf{SSize}(f) \leq \mathsf{SSize}(\textsc{Dual}(f)) \cdot 2^{o(n)}$[8] and note that this part implies the gap Theorem (Theorem 2.4), based on Observation 6.1 and the outline given in Section 2.

We move on to handle the linear case.

Theorem 6.3 (LSS for random upslices)**.** *Let $a \in [n]$, $k \leq \binom{n}{a}$ and let f be a randomly chosen (a, k_a, n)-upslice. Then, with probability $1 - 2^{-\Omega(n)}$, it holds that*

$$\mathsf{LSSize}(f) \leq \binom{n}{a}^{1/3} \cdot 2^{\frac{n}{3}+o(n)}.$$

Moreover, with probability $1 - 2^{-\Omega(n)}$, f can be realized with an exponent of at most $0.6651 < 2/3$, where $0.6651 = \mathrm{H}_2(\lambda) - (1-\lambda)\,\mathrm{H}_2(\frac{\lambda}{1-\lambda})$ for the λ which is the root of $\mathrm{H}_2(\lambda) - \frac{3}{2}(1-\lambda)\,\mathrm{H}_2(\frac{\lambda}{1-\lambda}) - \frac{1}{2}$.

Together with Observation 6.1, Theorem 6.3 implies the non-linear part of Theorem 2.3. The proof of Theorem 6.3 appears in Section 6.2.

[8] In fact, a weaker hypothesis suffices that applies duality only to the family of $(a : b, n)$-multislices; See Lemma 6.4.

6.1 Proof of Theorem 6.2

Given a random (a, k_a, n)-upslice f we realize f via one of the following two schemes depending on k_a. Let t be some threshold parameter that will be chosen later.

1. If $k_a \leq t$ realize f via a DNF scheme with complexity of k_a.
2. If $k_a > t$, set b to be the smallest integer solution of the inequality

$$t \geq \left[\binom{n}{a} / \binom{b}{a} \right] \cdot n. \tag{10}$$

   If the min-terms of f downcover the slice b (that is, $f(x) = 1$ for every x of weight at least b) realize f via the $(a : b, n)$-multislice of f with the general scheme for multislices promised by Lemma 4.5. Otherwise, realize f via DNF and call this event "failure".

We analyze the complexity of the construction. We set t to $\sqrt{\binom{n}{a}}$. For $k_a \leq t$ we rely on the first scheme and get complexity of at most $t = \sqrt{\binom{n}{a}}$, as required. We move on to the case where $k_a \geq t$. By Fact 3.3, the probability of "failure" is $2^{-\Omega(n)}$ and so by Lemma 4.5, the complexity in this case is $\binom{b}{\geq a} \cdot 2^{o(n)}$. We will show that

$$\binom{b}{\geq a} \leq \begin{cases} \sqrt{\binom{n}{\alpha^* n}} \cdot 2^{o(n)} & \text{if } a \in [0, \alpha^* n] \\ \sqrt{\binom{n}{a}} \cdot 2^{o(n)} & \text{if } a \in [\alpha^* n, n] \end{cases}, \tag{11}$$

Let us start with the case of $a \geq \alpha^* n$. We claim that

$$\binom{b}{\geq a} \leq \binom{b}{a} \cdot 2^{o(n)} \underset{\star}{\leq} \sqrt{\binom{n}{a}} \cdot 2^{o(n)}. \tag{12}$$

Indeed, by plugging $t = \sqrt{\binom{n}{a}}$ into (10) and rearranging the terms, we get that b is the smallest integer that satisfies $\binom{b}{a} \geq n \cdot \sqrt{\binom{n}{a}}$. Therefore, $(\star)$ holds. To establish the first inequality, it suffices to show that $a + o(n) \geq b/2$, or, equivalently, that $\binom{2a}{a} \cdot 2^{o(n)} \geq \binom{b}{a}$. By $(\star)$ it suffices to show that $\binom{2a}{a} \cdot 2^{o(n)} \geq \sqrt{\binom{n}{a}}$. Taking logarithms from both sides, the inequality holds whenever $2a + o(n) > 0.5\, \mathrm{H}_2(a/n)n$ which is indeed the case for any $a > \alpha^* n$.

Next we deal with the case where $a < \alpha^* n$. By (10), in this regime, b grows monotonically with a and so in this case it holds that $b < 2\alpha^*$. Therefore

$$\binom{b}{\geq a} \leq \binom{2\alpha^* n}{\geq a} \leq \binom{2\alpha^* n}{\alpha^* n} \cdot 2^{o(n)} \leq \sqrt{\binom{n}{\alpha^* n}} \cdot 2^{o(n)},$$

where the last inequality follows from the previous case. This completes the proof of the first part of Theorem 6.2 (without the "Moreover" part.)

Proving the "Moreover" part under the duality hypothesis. Now we assume the duality hypothesis and derive the last part of the proof. We will need the following lemma that is implied by the duality conjecture and the multislice lemma (Lemma 4.5).

Lemma 6.4. *Assuming the duality hypothesis, if $(a : b, n)$-multislices can be realized with share size of S, then the dual $(n - b : n - a, n)$-multislices can be realized with share size of $S \cdot 2^{o(n)}$. Specifically, $(a : b, n)$-multislice can be realized with share size of $\binom{n-a}{\geq n-b} \cdot 2^{o(n)}$.*

It can be verified that the above lemma outperforms the original $(a : b, n)$-multislice construction (Lemma 4.5) whenever $b > n - a$.

Getting back to the proof of Theorem 6.2, we will now realize random (a, n)-upslices with the same scheme but with different parameters and ingredients. We will analyze this scheme for $a \in [0, \alpha^{**}n]$, where $\alpha^{**} \sim 0.686$ is the solution of the equation

$$\mathrm{H}_2(\alpha) + (1 - \alpha^*)\,\mathrm{H}_2\left(\frac{\alpha}{1-\alpha^*}\right) - \frac{1}{2}\,\mathrm{H}_2(\alpha^*) = 0$$

and $\alpha^* \sim 0.157$ is defined as before to be the root of $0.25\,\mathrm{H}_2(\alpha) - \alpha$. For a random (a, n)-upslice f, we will run the previous scheme with the following changes. In step (2) we will set b to be the smallest integer solution of the inequality

$$\sqrt{\binom{n}{n-b}} \geq \left[\binom{n}{a}/\binom{b}{a}\right] \cdot n = \left[\binom{n}{n-b}/\binom{n-a}{n-b}\right] \cdot n. \tag{13}$$

If in step (2) the min-terms of f downcover the slice b, we realize the $(a : b, n)$-multislice of f by the new construction (Lemma 6.4) with share size $\binom{n-a}{\geq n-b} \cdot 2^{o(n)}$. If the min-terms do not downcover the slice b, the process fails (and we use DNF-based secret sharing). In addition, we set the threshold t to $\sqrt{\binom{n}{b}}$.

Claim 6.5. *Under the duality hypothesis, for any $a \in [0, \alpha^{**}n]$ and any k, the above scheme realizes a randomly chosen (a, k, n)-upslice with total share size of $\sqrt{\binom{n}{n-b}} \cdot 2^{o(n)}$ except with probability $2^{-\Omega(n)}$.*

Proof. First observe that, by Fact 3.3, the scheme fail with probability at most $2^{-\Omega(n)}$. Conditioned on not failing, the share size is $\max(\binom{n-a}{\geq n-b}, t)$ and since $t = \sqrt{\binom{n}{b}} = \sqrt{\binom{n}{n-b}}$ it suffices to prove the following inequalities

$$\binom{n-a}{\geq n-b} \leq \binom{n-a}{n-b} \cdot 2^{o(n)} \underset{\star\star}{\leq} \sqrt{\binom{n}{n-b}} \cdot 2^{o(n)}.$$

Indeed, since b is the minimal integer that satisfies (13), we conclude that $(\star\star)$ holds. The first inequality can be established by showing that $n - b + o(n) \geq (n - a)/2$, or, equivalently, that $\binom{2(n-b)}{n-b} \cdot 2^{o(n)} \geq \binom{n-a}{n-b}$. By $(\star\star)$ it suffices to show that $\binom{2(n-b)}{n-b} \cdot 2^{o(n)} \geq \sqrt{\binom{n}{n-b}}$. Taking logarithms from both sides and dividing by n, we get that the inequality holds whenever $2(1 - b/n) + o(1) \geq 0.5\,\mathrm{H}_2(b/n)$ which holds whenever $b/n \leq 1 - \alpha^* + o(1)$. We conclude the argument by showing that $b/n \leq 1 - \alpha^* + o(1)$. Since b is monotonically increasing with a (by (13)) and since $a \leq \alpha^{**}n$, we may focus on the case where $a = \alpha^{**}n$. Let $\beta = b/n$. Taking logarithms from both sides of (13) and dividing by n, we can write $\frac{1}{2}\,\mathrm{H}_2(\beta) = \mathrm{H}_2(\alpha^{**}) - \beta\,\mathrm{H}_2(\alpha^{**}/\beta) + o(1)$, which, by the definition of α^{**}, guarantees that $\beta \leq 1 - \alpha^* + o(1)$, as required. This completes the proof of Claim 6.5. □

Combining the two schemes together. Overall we now can realize random (a, n) upslices where $a \in [\alpha^* n, \alpha^{**} n]$ with share size

$$\min\left(\sqrt{\binom{n}{a}} \cdot 2^{o(n)}, \sqrt{\binom{n}{n-b}} \cdot 2^{o(n)}\right) \tag{14}$$

where $b = b(a, n)$ is the minimal integer that satisfies (13). Denote by a_0 the value for which the two expressions in (14) are equal, i.e., $b(a_0, n) = n - a_0$. We will later calculate a_0 and show that it is about $0.421n$. For now let us record the fact that $a_0 < n/2$ and that, consequently, for any $a > a_0$ it holds that $b(a, n) > b(a_0, n) = n - a_0 > n/2$ (since $b(a, n)$ monotonically increases with a). Next, observe that, the bound (14) on the complexity for an (a, n) upslice simplifies to $\sqrt{\binom{n}{a}} \cdot 2^{o(n)}$ when $a \leq a_0$ and to $\sqrt{\binom{n}{n-b}} \cdot 2^{o(n)}$ when $a > a_0$. Furthermore, the first expression monotonically increases with a for $a < a_0 < n/2$, and the second expression monotonically decreases with a for $a > a_0$ (since $b(a, n) > n/2$ and since $b(a, n)$ increases with a). Hence, the upslice with the maximal share size in the given range will be the (a_0, n)-upslice. We move on to calculate a_0. Let $a = \alpha n$ and $b = \beta n$, by plugging (13) into the equation $b(a, n) = n - a$, we conclude that $\alpha_0 = a_0/n$ is the solution to the equation

$$\frac{1}{2}\,\mathrm{H}_2(1-\alpha) = \mathrm{H}_2(1-\alpha) - (1-\alpha)\,\mathrm{H}_2\left(\frac{\alpha}{1-\alpha}\right),$$

and therefore $\alpha_0 \sim 0.421$. Therefore (14) is upper-bounded by $\sqrt{\binom{n}{a_0}} \cdot 2^{o(n)} \leq 2^{0.5\,\mathrm{H}_2(\alpha_0)n + o(n)}$. We conclude that random (a, n)-upslices can be realized with an exponent of $0.5\,\mathrm{H}_2(\alpha_0) \leq 0.491$ whenever $a \in [\alpha^* n, \alpha^{**} n]$. We complete the proof by noting that all random upslices below $\alpha^* n$ and above $\alpha^{**} n$ can also be realized with exponents below 0.491 due to the first scheme. □

6.2 Proof of Theorem 6.3

We begin by proving the first part of Theorem 6.3 (without the moreover part). The construction is identical to the first construction presented in Section 6.1, except that the threshold t is selected differently to be $\binom{n}{a}^{1/3} \cdot 2^{n/3}$. Again for $k_a \leq t$ we rely on the first scheme and get complexity of at most $t = \binom{n}{a}^{1/3} \cdot 2^{n/3}$, as required. For $k_a \geq t$, by Fact 3.3 failure happens with $2^{-\Omega(n)}$ probability, and, by Lemma 4.5, conditioned on not failing, the share complexity is at most $2^{n/2+o(n)} \cdot \sqrt{\binom{b}{\geq a}}$. To complete the first part of the proof, it suffices to show that the latter quantity is at most $\binom{n}{a}^{1/3} \cdot 2^{\frac{n}{3}+o(n)}$. This follows from the following claim

$$\binom{b}{\geq a} \leq \binom{b}{a} \cdot 2^{o(n)} \underset{\star}{\leq} \binom{n}{a}^{2/3} \cdot 2^{-n/3+o(n)}.$$

Indeed, by plugging $t = \binom{n}{a}^{1/3} \cdot 2^{n/3}$ into (10) and rearranging the terms, we get that b is the smallest integer that satisfies $\binom{b}{a} \geq n \cdot \binom{n}{a}^{2/3} \cdot 2^{-n/3}$. Therefore, $(\star)$ holds. To establish the first inequality, it suffices to show that $a + o(n) \geq b/2$, or, equivalently, that $\binom{2a}{a} \cdot 2^{o(n)} \geq \binom{b}{a}$. By $(\star)$ it suffices to show that $\binom{2a}{a} \cdot 2^{o(n)} \geq \binom{n}{a}^{2/3} \cdot 2^{-n/3}$. Taking logarithms from both sides, the inequality holds whenever $2a + o(n) > (\frac{2}{3}\,\mathrm{H}_2(a/n) - 1/3)n$ which is indeed the case for every $a \in [n]$. This completes the proof of the first part of the theorem (without the moreover part).

To prove the "Moreover" part, we make use of the following lemma which is implied by the multislice construction (Lemma 4.5) and the duality closure of linear schemes (Fact 5.4):

Lemma 6.6 (LSS for multislices)**.** *Let $a, b \in [0, n]$ be integers, then the family of $(a : b, n)$-multislices can be linearly realized with share size $\sqrt{\binom{n-a}{\geq n-b}} \cdot 2^{n/2+o(n)}$.*

It can be verified that the above lemma outperforms the original linear $(a : b, n)$-multislice construction (Lemma 4.5) whenever $b > n - a$.

This time for a random (a, n)-upslice f, we will run the previous linear scheme with the following changes. In step (2), we will set b to be the smallest integer solution of the inequality

$$\binom{n}{b}^{1/3} \cdot 2^{n/3} \geq \left[\binom{n}{a} / \binom{b}{a}\right] \cdot n = \left[\binom{n}{n-b} / \binom{n-a}{n-b}\right] \cdot n. \tag{15}$$

In addition, we set the threshold t to $\binom{n}{b}^{1/3} \cdot 2^{n/3}$.

Claim 6.7. *For any $a \in [n]$ and any k, the above scheme realizes a randomly chosen (a, k, n)-upslice with total share size of $\binom{n}{n-b}^{1/3} \cdot 2^{n/3}$.*

Proof. First observe that by Fact 3.3 we fail with probability at most $2^{-\Omega(n)}$. Conditioned on not failing, the share size is $\max(\sqrt{\binom{n-a}{\geq n-b}} \cdot 2^{n/2+o(n)}, t)$ and since $t = \binom{n}{b}^{1/3} \cdot 2^{n/3} = \binom{n}{n-b}^{1/3} \cdot 2^{n/3}$ it suffices to show that

$$\sqrt{\binom{n-a}{\geq n-b}} \cdot 2^{n/2+o(n)} \leq \binom{n}{n-b}^{1/3} \cdot 2^{n/3} \cdot 2^{o(n)}. \tag{16}$$

We prove (16) by establishing the following inequalities

$$\binom{n-a}{\geq n-b} \leq \binom{n-a}{n-b} \cdot 2^{o(n)} \underset{\star\star}{\leq} \binom{n}{n-b}^{2/3} \cdot 2^{-n/3+o(n)}.$$

Indeed, since b is the minimal integer that satisfies (15), we conclude that $(\star\star)$ holds. The first inequality can be established by showing that $n - b + o(n) \geq (n - a)/2$, or, equivalently, that $\binom{2(n-b)}{n-b} \cdot 2^{o(n)} \geq \binom{n-a}{n-b}$. By $(\star\star)$ it suffices to show that $\binom{2(n-b)}{n-b} \cdot 2^{o(n)} \geq \binom{n}{n-b}^{2/3} \cdot 2^{-n/3}$. Taking logarithms from both sides and dividing by n, we get that the inequality holds whenever $2(1 - b/n) + o(1) \geq (\frac{2}{3} \operatorname{H}_2(b/n) - 1/3)$ which is indeed the case for every $b \in [n]$. This completes the proof of Claim 6.7. □

Combining the two schemes together. Overall we now can linearly realize random (a, n) upslices with share size of

$$\min\left(\binom{n}{a}^{1/3} \cdot 2^{n/3+o(n)}, \binom{n}{n-b}^{1/3} \cdot 2^{n/3+o(n)}\right) \tag{17}$$

where $b = b(a, n)$ is the smallest integer that satisfies (15). Similarly to the analysis in the proof for the general (non-linear) case, denote by a_0 the value for which the two expressions in (17) are equal, i.e., $b(a_0, n) = n - a_0$. We will later calculate a_0 and show that it is about $0.4595n$. For now let us record the fact that $a_0 < n/2$ and that, consequently, for any $a > a_0$ it holds that $b(a, n) > b(a_0, n) = n - a_0 > n/2$ (since $b(a, n)$ monotonically increases with a). Getting back to (17) observe that the complexity for an (a, n) upslice is $\binom{n}{a}^{1/3} \cdot 2^{n/3+o(n)}$ when $a \leq a_0$ and $\binom{n}{n-b}^{1/3} \cdot 2^{n/3+o(n)}$ when $a > a_0$. Furthermore, the first expression monotonically increases with a for $a < a_0 < n/2$, and the second expression monotonically decreases with a for $a > a_0$ (since $b(a, n) > n/2$ and since $b(a, n)$ increases with a). Hence, the upslice

with the maximal share size in the given range will be the (a_0, n)-upslice. We move on to calculate a_0. Let $a = \alpha n$ and $b = \beta n$, by plugging (15) into the equation $b(a, n) = n - a$, we conclude that $\alpha_0 = a_0/n$ is the solution to the equation

$$\frac{1}{3} + \frac{1}{3}\,\mathrm{H}_2(1-\alpha) = \mathrm{H}_2(1-\alpha) - (1-\alpha)\,\mathrm{H}_2\left(\frac{\alpha}{1-\alpha}\right),$$

and therefore $\alpha_0 \sim 0.4595$. It follows that (17) is upper-bounded by $\binom{n}{a_0}^{1/3} \cdot 2^{n/3+o(n)} \leq 2^{n\frac{\mathrm{H}_2(\alpha_0)+1}{3}+o(n)}$. We conclude that a random (a, n)-upslice can be linearly realized with an exponent of $\frac{\mathrm{H}_2(\alpha_0)+1}{3} \leq 0.6651$ for any a, and the "Moreover" part of Theorem 6.3 follows. □

Acknowledgement

We thank Amos Beimel and Naty Peter for valuable discussions.

References

[1] Benny Applebaum, Amos Beimel, Oriol Farràs, Oded Nir, and Naty Peter. Secret-sharing schemes for general and uniform access structures. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, volume 11478 of *Lecture Notes in Computer Science*, pages 441–471. Springer, 2019.

[2] Benny Applebaum, Amos Beimel, Oded Nir, and Naty Peter. Better secret sharing via robust conditional disclosure of secrets. In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *Proccedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, STOC 2020, Chicago, IL, USA, June 22-26, 2020*, pages 280–293. ACM, 2020.

[3] D. Beaver, J. Feigenbaum, J. Kilian, and P. Rogaway. Security with low communication overhead. In A. J. Menezes and S. A. Vanstone, editors, *CRYPTO '90*, volume 537 of *LNCS*, pages 62–76. Springer-Verlag, 1990.

[4] A. Beimel. *Secure Schemes for Secret Sharing and Key Distribution*. PhD thesis, Technion, 1996.

[5] A. Beimel. Secret-sharing schemes: A survey. In Y. Meng Chee, Z. Guo, S. Ling, F. Shao, Y. Tang, H. Wang, and C. Xing, editors, *Coding and Cryptology – Third International Workshop, IWCC 2011*, volume 6639 of *LNCS*, pages 11–46. Springer-Verlag, 2011.

[6] A. Beimel and B. Chor. Universally ideal secret-sharing schemes. *IEEE Trans. on Information Theory*, 40(3):786–794, 1994.

[7] A. Beimel, A. Gabizon, Y. Ishai, and E. Kushilevitz. Distribution design. In *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science*, pages 81–92. ACM, 2016.

[8] Amos Beimel and Oriol Farràs. The share size of secret-sharing schemes for almost all access structures and graphs. In Rafael Pass and Krzysztof Pietrzak, editors, *Theory of Cryptography - 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, Proceedings, Part III*, volume 12552 of *Lecture Notes in Computer Science*, pages 499–529. Springer, 2020.

[9] Amos Beimel, Oriol Farràs, Yuval Mintz, and Naty Peter. Linear secret-sharing schemes for forbidden graph access structures. In Yael Kalai and Leonid Reyzin, editors, *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part II*, volume 10678 of *Lecture Notes in Computer Science*, pages 394–423. Springer, 2017.

[10] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for noncryptographic fault-tolerant distributed computations. In *20th STOC*, pages 1–10. ACM, 1988.

[11] J. C. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In S. Goldwasser, editor, *CRYPTO '88*, volume 403 of *LNCS*, pages 27–35. Springer-Verlag, 1988.

[12] M. Bertilsson and I. Ingemarsson. A construction of practical secret sharing schemes using linear block codes. In J. Seberry and Y. Zheng, editors, *AUSCRYPT '92*, volume 718 of *LNCS*, pages 67–79. Springer-Verlag, 1992.

[13] G. R. Blakley. Safeguarding cryptographic keys. In *Proc. of the 1979 AFIPS National Computer Conference*, volume 48 of *AFIPS Conference proceedings*, pages 313–317. AFIPS Press, 1979.

[14] Carlo Blundo, Alfredo De Santis, Luisa Gargano, and Ugo Vaccaro. On the information rate of secret sharing schemes (extended abstract). In *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*, pages 148–167, 1992.

[15] D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols. In *20th STOC*, pages 11–19. ACM, 1988.

[16] B. Chor and E. Kushilevitz. Secret sharing over infinite domains. *J. of Cryptology*, 6(2):87–96, 1993.

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

[18] László Csirmaz. Secret sharing and duality. *J. Math. Cryptol.*, 15(1):157–173, 2020.

[19] Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In J. Feigenbaum, editor, *CRYPTO '91*, volume 576 of *LNCS*, pages 457–469. Springer-Verlag, 1991.

[20] Paul Erdos and John Spencer. *Probabilistic Methods in Combinatorics*. Academic Press, 1974.

[21] U. Feige, J. Kilian, and M. Naor. A minimal model for secure computation. In *26th STOC*, pages 554–563. ACM, 1994.

[22] Anna Gal. *Combinatorial methods in Boolean function complexity*. PhD thesis, University of Chicago, 1996.

[23] M. Göös, T. Pitassi, and T. Watson. Zero-information protocols and unambiguity in arthur-merlin communication. *Algorithmica*, 76(3):684–719, 2016.

[24] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *13th CCS*, pages 89–98. ACM, 2006.

[25] Y. Ishai and E. Kushilevitz. On the hardness of information-theoretic multiparty computation. In C. Cachin and J. Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 439 – 455. Springer-Verlag, 2004.

[26] M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structure. In *Globecom 87*, pages 99–102. IEEE, 1987. Journal version: Multiple assignment scheme for sharing secret. J. of Cryptology 6(1), 15-20, (1993).

[27] M. Karchmer and A. Wigderson. On span programs. In *8th Structure in Complexity Theory*, pages 102–111. IEEE Computer Society, 1993.

[28] Tianren Liu and Vinod Vaikuntanathan. Breaking the circuit-size barrier in secret sharing. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 699–708. ACM, 2018.

[29] Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Towards breaking the exponential barrier for general secret sharing. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*, volume 10820 of *Lecture Notes in Computer Science*, pages 567–596. Springer, 2018.

[30] M. Naor and A. Wool. Access control and signatures via quorum secret sharing. In *3rd CCS*, pages 157–167. ACM, 1996.

[31] T. Pitassi and R. Robere. Strongly exponential lower bounds for monotone computation. In *49th STOC*, pages 1246–1255. ACM, 2017.

[32] T. Pitassi and R. Robere. Lifting nullstellensatz to monotone span programs over any field. In *50th STOC*, pages 1207–1219. ACM, 2018.

[33] R. Robere, T. Pitassi, B. Rossman, and S. A. Cook. Exponential lower bounds for monotone span programs. In *57th FOCS*, pages 406–415. IEEE Computer Society, 2016.

[34] A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.

[35] B. Shankar, K. Srinathan, and C. Pandu Rangan. Alternative protocols for generalized oblivious transfer. In S. Rao, M. Chatterjee, P. Jayanti, C. S. Ram Murthy, and S. K. Saha, editors, *9th ICDCN*, volume 4904 of *LNCS*, pages 304–309. Springer-Verlag, 2008.

[36] Hung-Min Sun and Shiuh-Pyng Shieh. Secret sharing in graph-based prohibited structures. In *Proceedings IEEE INFOCOM '97, The Conference on Computer Communications, Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies, Driving the Information Revolution, Kobe, Japan, April 7-12, 1997*, pages 718–724, 1997.

[37] T. Tassa. Generalized oblivious transfer by secret sharing. *Designs, Codes and Cryptography*, 58(1):11–21, 2011.

[38] B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, editors, *PKC 2011*, volume 6571 of *LNCS*, pages 53–70. Springer-Verlag, 2011.

A Omitted Preliminaries

A.1 Secret Sharing

We present the definition of secret-sharing schemes, similar to [6, 16]. For the privacy of these schemes, we use the following notation: For two random variables X and Y, we say that $X \equiv Y$ if they are identically distributed.

Definition A.1 (Partial access structures)**.** *Let $P = \{P_1, \ldots, P_n\}$ be a set of parties. A* partial access structure *is a pair of collections $\Gamma = (\Gamma_{\text{no}}, \Gamma_{\text{yes}})$, where $\Gamma_{\text{no}}, \Gamma_{\text{yes}} \subseteq 2^P$ are non-empty collections of sets such that $B \not\subseteq A$ for every $A \in \Gamma_{\text{no}}, B \in \Gamma_{\text{yes}}$.*[9] *Sets in Γ_{yes} are called* authorized*, and sets in Γ_{no} are called* unauthorized*. If $\Gamma_{\text{no}} \cup \Gamma_{\text{yes}} = 2^P$ then Γ is called an access structure and will be denoted by the collection of authorized sets Γ_{yes}. We represent a subset of parties $A \subseteq P$ by its characteristic string $x_A = (x_1, \ldots, x_k) \in \{0,1\}^n$, where for every $j \in [n]$ it holds that $x_j = 1$ if and only if $P_j \in A$. Accordingly, an access structure $\Gamma = (\Gamma_{\text{no}}, \Gamma_{\text{yes}})$ will also be described by the monotone function $F : \{0,1\}^n \to \{0,1\}$, where $F(x_A) = 1$ for every subset of parties $A \in \Gamma_{\text{yes}}$ and $F(x_A) = 0$ for every set $A \in \Gamma_{\text{no}}$. Similarly, a partial access structure will be associated with a partial function from $\{0,1\}^n$ to $\{0,1\}$.*

Definition A.2 (Secret-sharing schemes)**.** *A* secret-sharing scheme*, with domain of secrets S, domain of random strings R, and finite domains of shares $S_1, \ldots, S_n$, is a deterministic function $\mathcal{D} : S \times R \to S_1 \times \cdots \times S_n$. A dealer distributes a secret $s \in S$ according to $\mathcal{D}$ by first sampling a random string $r \in R$ with uniform distribution, computing a vector of* shares *$\mathcal{D}(s,r) = (s_1, \ldots, s_n)$, and privately communicating each share s_i to party P_i. For a set $A \subseteq P$, we denote $\mathcal{D}_A(s,r)$ as the restriction of $\mathcal{D}(s,r)$ to its A-entries (i.e., the shares of the parties in A).*

A secret-sharing scheme $\mathcal{D}$ realizes a partial access structure $\Gamma = (\Gamma_{\text{no}}, \Gamma_{\text{yes}})$ if the following two requirements hold:

Perfect Correctness. *The secret s can be reconstructed by any authorized set of parties. That is, for any set $B = \left\{P_{i_1}, \ldots, P_{i_{|B|}}\right\} \in \Gamma_{\text{yes}}$ there exists a* reconstruction function *$\text{Recon}_B : S_{i_1} \times \cdots \times S_{i_{|B|}} \to S$ such that for every secret $s \in S$ and every random string $r \in R$, it holds that $\text{Recon}_B\left(\mathcal{D}_B(s,r)\right) = s$.*

Perfect privacy. *Any unauthorized set cannot learn anything about the secret from its shares. Formally, for any set $T = \left\{P_{i_1}, \ldots, P_{i_{|T|}}\right\} \in \Gamma_{\text{no}}$, every pair of secrets $s, s' \in S$, it holds that $\mathcal{D}_T(s,r) \equiv \mathcal{D}_T(s',r)$, where r is sampled with uniform distribution from R.*

The secret size *in a secret-sharing scheme $\mathcal{D}$ is defined as $\log|S|$ and the* share size *of the scheme $\mathcal{D}$ is defined as the largest share size, i.e., $\max_{1 \le i \le n}\{\log|S_i|\}$.*[10] *The scheme $\mathcal{D}$ is a* linear secret-sharing scheme over a finite field $\mathbb{F}$ *if $S = \mathbb{F}$, $R = \mathbb{F}^\ell$ for some integer $\ell \ge 1$, the sets $S_1, \ldots, S_n$ are vector spaces over $\mathbb{F}$, and the function $\mathcal{D} : \mathbb{F}^{\ell+1} \to S_1 \times \cdots \times S_n$ is a linear mapping over $\mathbb{F}$. By default, linearity is defined over the binary field $\mathbb{F}_2$.*

The definition of secret-sharing scheme can be naturally extended to collections of n-party access structures $\mathcal{F}$. In this case, $\mathcal{D}$ receives (a description of) an access structure $f \in \mathcal{F}$ as an auxiliary input, and $\mathcal{D}_f$ should realize f for every $f \in \mathcal{F}$.

Next, we define threshold secret-sharing schemes, and provide some known result for such schemes.

[9] We do not require that $2^P \setminus \Gamma_{\text{no}}$ and Γ_{yes} are equal or that they are monotone (this simplifies our presentation).

[10] The share size is sometimes defined to be the total share size, i.e., $\sum_{1 \le i \le n} \log|S_i|$. However, since the two differ by at most a linear factor of n, the difference is not important in our context.

Definition A.3 (Threshold secret-sharing schemes)**.** *We say that an n-party secret-sharing scheme is a k-out-of-n* secret-sharing scheme *if it realizes the access structure $\Gamma_{k,n} = \{A \subseteq P : |A| \geq k\}$.*

Theorem A.4 ([34])**.** *For every integers $1 \leq k \leq n$, there is a linear k-out-of-n secret-sharing scheme realizing $\Gamma_{k,n}$ for secrets of size m in which the share size is $\max\{m, O(\log n)\}$.*

A.2 Slices, multislices, downslices and upslices

We formally define four different types of "slice access structures" that will be used as key components in our general constructions. Throughout this section, we fix some complete access structure f over n parties. The following definitions were extensively used by [28]. For string $x, x' \in \{0,1\}^n$, we write $x \leq x'$ if for every $i \in [n]$, $x_i \leq x'_i$. We let $\mathrm{wt}(x)$ denote the Hamming weight of x.

Definition A.5 (Slices and Multislices)**.** *For $a \leq b \in [n]$, we define the* $(a : b)$-multislice *of f to be the access structure $F : \{0,1\}^n \to \{0,1\}$ for which*

$$F(x) = \begin{cases} 0 & \text{if } \mathrm{wt}(x) < a \\ f(x) & \text{if } \mathrm{wt}(x) \in [a,b] \\ 1 & \text{if } \mathrm{wt}(x) > b \end{cases}.$$

We say that F is $(a : b, n)$-multislice access-structure *(or just $(a : b, n)$-slice) if F is an $(a : b)$-multislice of some n-party access structure f. An $(a : a)$-multislice is refereed to as an* a-slice*.*

As already mentioned, our constructions strongly exploit the following fine-grained variants of slice access structures.

Definition A.6 (Upslices)**.** *For $a \in [n]$, we define the* a-upslice *of f to be the access structure $F : \{0,1\}^n \to \{0,1\}$ for which*

$$F(x) = \begin{cases} 0 & \text{if } \mathrm{wt}(x) < a \\ f(x) & \text{if } \mathrm{wt}(x) = a \\ 1 \iff \exists x' : \mathrm{wt}(x') = a, x' \leq x, f(x') = 1 & \text{if } \mathrm{wt}(x) > a \end{cases}.$$

We say that F is an (a, n)-upslice access structure *(or just (a, n)-upslice) if F is an (a, n)-upslice of some n-party access structure f.*

Observe that F is (a, n)-upslice if and only if all its min-terms are at level a.

Definition A.7 (Downslices)**.** *For $b \in [n]$, we define the* b-downslice *of f to be the access structure $F : \{0,1\}^n \to \{0,1\}$ for which*

$$F(x) = \begin{cases} 0 \iff \exists x' : \mathrm{wt}(x') = b, x \leq x', f(x') = 0 & \text{if } \mathrm{wt}(x) < b \\ f(x) & \text{if } \mathrm{wt}(x) = b \\ 1 & \text{if } \mathrm{wt}(x) > b \end{cases}.$$

We say that F is a (b, n)-downslice access structure *(or just (b, n)-downslice) if F is a b-slice of some n-party access structure f.*

Observe that F is a (b, n)-downslice if and only if all its max-terms are at level b.

B Proof of Lemma 4.5: Secret sharing for multislice access structures

To prove Lemma 4.5 we generalize the proof of [2, Lemma 5.10]. There are only slight deviations from the original proof, and we provide the full proof here for the completeness of the paper. Our starting point is the definition of [2] of a family of access structures we call *somewhat-regular access structures*. The best secret sharing scheme known for this family is based on *Robust Conditional Disclosure of Secrets Protocols*, which are defined and studied in [2].

Definition B.1 ((k, c, d)-somewhat-regular access structure)**.** *Let Π be a partition of the set of n parties P to k equal-sized sets $(I_1, \ldots, I_k)$, and integers $0 \leq c < d \leq n/k$. A (partial) access structure $\Gamma = (\Gamma_{\rm no}, \Gamma_{\rm yes})$ over n parties is (Π, c, d)-somewhat-regular if for every $A \in \Gamma_{\rm no} \cup \Gamma_{\rm yes}$ and every $i \in [k]$,*

$$c \leq |A \cap I_i| \leq d. \tag{18}$$

In other words, Γ puts no restriction on sets $A \subset [n]$ that violate (18) *for some i. We sometimes omit Π and refer to Γ as being* (k, c, d)-somewhat-regular.

Remark B.2. *We can take a fully defined access structure F and "puncture it" according to a given partition Π and parameters (c, d) and derive a (Π, c, d)-somewhat-regular version of F, denoted by $F_{\Pi,c,d}$, where $F_{\Pi,c,d}$ is undefined on inputs x for which some x_i has weight greater than d or smaller than c.*

The combination of Lemma 5.5 and Theorem 4.5 from [2] lead to the following lemma:

Lemma B.3. *For every (k, c, d)-somewhat-regular access structure F over n parties there exists a secret sharing scheme with share sizes of $m \cdot \sum_{j=c}^{d} \binom{n/k}{j}$ for each party, where m equals:*

$$m \quad = \quad 2^{o(n)} \cdot \left[\sum_{j=0}^{d-c} \binom{d}{c+j}\right]^{k-1} \cdot \left[(n/k) \log \binom{n/k}{d}\right]^{k},$$

Respectively m_ℓ for linear schemes is given by

$$m_\ell \quad \leq \quad O(2^{n/2}) \cdot \left[\sum_{j=0}^{d-c} \binom{d}{c+j} \log \binom{n/k}{d}\right]^{\frac{k-1}{2}}.$$

We now prove a probabilistic lemma, which will allow us to compose $O(n)$ somewhat-regular access structure to one multislice access structure. Fix a proximity parameter ϵ to be $n^{0.3}$, and $a < b \in [n^{0.85}, n - n^{0.85}]$ (We will deal with general a and b in the end of the section with an addition of $2^{o(n)}$ to the share size). Let $\Pi = (I_1, \ldots, I_k)$ be a partition of $[n]$ to $k = \sqrt{n}$ subsets of size $n/k = \sqrt{n}$ each. In the following, we say that an input $x \in \{0,1\}^n$ is *good* for the i-th block of Π, if the sub-string $x_i \in \{0,1\}^{\sqrt{n}}$ is of Hamming weight at least $a/\sqrt{n} - \epsilon$ and at most $b/\sqrt{n} + \epsilon$. We say that x is good for the partition Π if x is *good* for all the blocks $i \in [k]$ of Π. If x is not good then it is called bad. We will use the following lemma.

Lemma B.4. *There exists a collection of $\lambda = O(n)$ partitions $\Pi_1, \ldots, \Pi_\lambda$ of $[n]$ to $\sqrt{n}$ subsets of size $\sqrt{n}$ each, such that every n-bit string x of Hamming weight $n^{0.85} < a \leq \mathrm{wt}(x) \leq b < n - n^{0.85}$ is good for at least 0.7λ of the partitions.*

The hidden constant in the big-O notation depends on a and b.

Proof. We use the probabilistic method to choose at random such a collection of size $\lambda = O(n)$, and see that with positive probability all inputs are good for at least 0.7λ of the partitions.

Fix an input x of weight $a \leq \mathrm{wt}(x) \leq b$. We start the analysis by sampling a partition Π with uniform distribution. We first focus on a single block i, and denote by $Y_{j,i}$ the indicator random variable that is equal to 1 if and only if the j-th bit of the i-th block is 1. For every $i \in [\sqrt{n}]$, the $\sqrt{n}$ variables $\{Y_{j,i}\}_{j\in[\sqrt{n}]}$ are negatively associated (see [2, Lemma A.7]). We now denote $Y_i = \sum_j Y_{j,i}$ to be the random variable representing the number of ones of x that are placed in the i-th block of Π. Due to the linearity of expectation, and to x being of weight between a and b, the expectation μ of Y_i satisfies $a/\sqrt{n} \leq \mu \leq b/\sqrt{n}$. The probability that x is bad for the i-th block is a sum of two probabilities, that x puts too many ones or too few in the block. These two probabilities behave the same asymptotically, so we will analyze only the former probability. By the negative associativity, we can use the Chernoff bound and get that

$$\Pr\left[Y_i \geq \frac{b}{\sqrt{n}} + \epsilon\right] = \Pr\left[Y_i \geq \frac{b}{\sqrt{n}}(1 + \epsilon\frac{\sqrt{n}}{b})\right] \leq e^{-\frac{\epsilon^2\sqrt{n}}{3b}} = e^{-\Omega(n^{0.1})},$$

where the last equation follows from our choice of $\epsilon = n^{0.3}$. Dealing only with $b > n^{0.85}$ allows to apply the Chernoff bound as $0 < \epsilon\frac{\sqrt{n}}{b} < n^{-0.05} < 1$

Now by union bound over all blocks, the probability that x is bad for the partition Π is at most

$$p = \sqrt{n}e^{-\Omega(n^{0.1})} = o(1).$$

Finally, if we independently sample λ partitions, the probability that x is bad for at least 0.3λ of the partitions is, by a Chernoff bound, at most $2^{-\Omega(\lambda)}$. By taking $\lambda = Cn$ for sufficiently large constant C, the latter probability is smaller than 2^{-n}, so the lemma follows by applying a union bound over all possible inputs. □

We can now realize a scheme for $(a : b, n)$ multislice access structures.

Lemma B.5. *Let F be an $(a : b, n)$ multislice access structure with $n^{0.85} < a < b < n - n^{0.85}$. Then, F can be realized by a secret-sharing scheme with share size of $m' \cdot O(n \log n)$, assuming that any (k, c, d)-somewhat-regular access structure can be realized by a secret-sharing scheme with share size of m', where*

$$k = \sqrt{n},\ c = a/\sqrt{n} - n^{0.3},\ \textit{and}\ d = b/\sqrt{n} + n^{0.3}.$$

Proof. We start by considering an $(a : b, n)$ partial multislice access structure. Recall that such access structure is defined only over the inputs whose Hamming weight is in the interval $[a, b]$.

Construction B.6. *We realize such an access structure F as follows:*

1. *Let $L = (\Pi_1, \ldots, \Pi_\lambda)$ be the list of partitions of length $\lambda = O(n)$ promised by Lemma B.4.*
2. *Share s into λ shares $(\sigma_1, \ldots, \sigma_\lambda)$ via a $\lambda/2$-out-of-λ threshold secret-sharing scheme (using fresh randomness).*
3. *For every $i \in [\lambda]$ share each σ_i with a different random string r_i by a secret-sharing scheme realizing the (k, c, d)-somewhat-regular access structure $F_{\Pi_i,c,d}$ (as defined in Remark B.2).*

We analyze the construction. Fix some input x of Hamming weight $a \leq \mathrm{wt}(x) \leq b$. Let $I \subset [\lambda]$ denote the set $\{i : x \text{ is good for } \Pi_i\}$, and recall that, by Lemma B.4, the set I is of size at least 0.7λ. Observe that $F(x) = F_{\Pi_i,c,d}(x)$ for every $i \in I$. If $F(x) = 1$ then at least 0.7λ shares σ_i, where $i \in I$, can be reconstructed by the parties in x and s can be recovered. If $F(x) = 0$ then at least 0.7λ shares σ_i, where

$i \in I$, are kept perfectly hidden (due to the privacy of $F_{\Pi_i,c,d}$) and so s remains perfectly hidden (i.e., we can perfectly simulate the view of the parties that participate in x).[11]

We use Shamir's secret-sharing scheme [34] to implement the threshold part and so each σ_i is of length $O(\log \lambda)$ (see Theorem A.4). Hence, the share size per party is $O(m'\lambda \log \lambda) = O(m'n \log n)$ where m' is the size of shares of the underlying somewhat-regular scheme.

We move on to handle the case where F is defined over all inputs. This part of the construction is quite straightforward. Recall that such an access structure takes the value 0 over light inputs, the value 1 over heavy inputs, and may take arbitrary values in between. Letting F' denote the partial $(a : b, n)$ multislice access structure that agrees with[12] F over the inputs with Hamming weight between a and b, we realize F as follows:

1. Share s via a $(b+1)$-out-of-n secret-sharing scheme and give the i-th share, denoted by u_i, to the i-th party.
2. Share s via 2-out-of-2 secret-sharing into s_0 and s_1.
3. Share s_0 via a a-out-of-n secret-sharing scheme and give the i-th share, denoted by v_i, to the i-th party.
4. Share s_1 to all parties according to F' (using Construction B.6) and give the i-the share, denoted by w_i, to the i-th party.

Correctness: Any input x of weight at least $b+1$ can reconstruct s via the u shares, and any input x with Hamming weight between a and b which is authorized (i.e., $F(x) = 1$) can recover s_0 and s_1 (via the v and w shares) and can therefore recover s.

Privacy: A coalition that corresponds to light inputs learns nothing from the u shares and the v shares (due to the privacy of the threshold schemes) and therefore learns nothing about s. A medium-slice coalition that is unauthorized (i.e., $F(x) = 0$) learns nothing from the u shares (due to the privacy of the threshold scheme) and learns nothing from the w shares (due to the privacy of the F' scheme) and so it learns nothing on s.

Since each w_i is of length $O(m'n \log n)$ and the bit-length of u_i and v_i is $O(\log n)$, the share size per party is $O(m'n \log n) + O(\log n) = O(m'n \log n)$. □

We now conclude the proof of Lemma 4.5, by putting together Lemma B.5 and Lemma B.3, which results in a secret sharing scheme for $(a : b, n)$ multislice access structures with a total share size of:

$$m \;=\; 2^{o(n)} \cdot \left[\sum_{j=0}^{\frac{b-a}{\sqrt{n}}+2n^{0.3}} \binom{b/\sqrt{n}+n^{0.3}}{a/\sqrt{n}-n^{0.3}+j} \right]^{\sqrt{n}-1} \cdot \left[(\sqrt{n}) \log \binom{\sqrt{n}}{b/\sqrt{n}} \right]^{\sqrt{n}} \cdot O(n \log n),$$

which equals

$$\binom{b/\sqrt{n}}{\geq a/\sqrt{n}}^{\sqrt{n}} \cdot 2^{o(n)}.$$

[11] Note that when $i \notin I$ there are no guarantees on the share σ_i, e.g., it is possible that $F(x) = 0$ and the parties in x can recover σ_i or that $F(x) = 1$ and the parties in x would have no information on σ_i. However, since we use a threshold scheme to share s, this does not affect the correctness and privacy of the construction.

[12] We say that a pair of partial functions f and g agree with each other if they take the same value on every input x for which both functions are defined.

For the linear case we get that

$$m_\ell \;\leq\; O(2^{n/2}) \cdot \left[\sum_{j=0}^{\frac{b-a}{\sqrt{n}}+2n^{0.3}} \binom{b/\sqrt{n}+n^{0.3}}{a/\sqrt{n}-n^{0.3}+j} \log \binom{\sqrt{n}}{b/\sqrt{n}} \right]^{\frac{\sqrt{n}-1}{2}} \cdot O(n \log n),$$

which equals

$$m_\ell = \sqrt{\binom{b/\sqrt{n}}{\geq a/\sqrt{n}}^{\sqrt{n}}} \cdot 2^{n/2+o(n)}.$$

Recall that so far we handled multislices where $n^{0.85} < a < b < n - n^{0.85}$. Generalizing our scheme to any $(a : b, n)$ multislice f is relatively simple. We first realize the $(n^{0.85} : n - n^{0.85}, n)$ multislice of f, and then add the missing min-terms of f of size $< n^{0.85}$ with a DNF scheme and the missing max-terms of size $> n - n^{0.85}$ with a CNF scheme. The total additive cost to the share size is then $O\left(n\binom{n}{n^{0.85}}\right) = 2^{o(n)}$. Lastly we see that by Fact C.2 $\sqrt{\binom{b/\sqrt{n}}{\geq a/\sqrt{n}}^{\sqrt{n}}} \leq \binom{b}{\geq a} \cdot 2^{o(n)}$, which concludes the proof and will allow us to work with latter simpler expression from now on.

□

C Proofs and Facts

C.1 Proof of Observation 4.2

We claim that

$$f = \bigwedge_{i=0}^{n} F_i.$$

Fix an input x and let a denote its Hamming weight. We show that the RHS evaluates to $f(x)$. If $f(x) = 0$ then $F_a(x) = 0$ and so the RHS also evaluates to zero. The case of $f(x) = 1$ follows by observing that: (1) By definition, $F_i(x) = 1$ for all $i \leq a$; and (2) Since f is monotone, $f(y) = 1$ for every $y \supset x$, and therefore $F_i(x) = 1$ for all $i \geq a$.

Based on the above equality, we can distribute a secret s according to f as follows: Distribute $s \in \{0, 1\}$ into n single-bit shares via $(n+1)$-out-of-$(n+1)$ secret-sharing and share the i-th share via F_i. The overall complexity is $\sum_{i=0}^{n} S_i \leq n \max_i S_i$.

C.2 Simple inequalities

Fact C.1. *Let $a \leq b, k$ be integers such that $k|a$ and $k|b$. Then it holds that $\binom{b/k}{a/k}^k \leq \binom{b}{a}$*

Proof. Fix a and k, we prove by induction over b. For the base case where $b = a$ it holds that $\binom{a/k}{a/k}^k = 1^k = 1 = \binom{a}{a}$ as desired. Next we assume that $\binom{b/k}{a/k}^k \leq \binom{b}{a}$ and show that $\binom{(b+k)/k}{a/k}^k \leq \binom{b+k}{a}$. First we see that

$$\binom{b+k}{a} = \binom{b}{a} \cdot \prod_{i=1}^{k}(b+i) \cdot \prod_{i=1}^{k}(b-a+i)^{-1} \geq \binom{b/k}{a/k}^k \cdot \prod_{i=1}^{k}(b+i) \cdot \prod_{i=1}^{k}(b-a+i)^{-1}.$$

and that

$$\binom{b/k}{a/k}^k = \binom{(b+k)/k}{a/k}^k \cdot \left(\frac{b+k}{k}\right)^{-k} \cdot \left(\frac{b-a+k}{k}\right)^k.$$

If we combine the two parts it remains to show that $\frac{\prod_{i=1}^{k}(b+i)\cdot(b-a+k)^k}{\prod_{i=1}^{k}(b-a+i)\cdot(b+k)^k} \geq 1$, which is true since for every positive integers a, b, i, k such that $b > a$ and $1 \leq i \leq k$ it holds that $\frac{b-a+k}{b-a+i} \geq \frac{b+k}{b+i}$. □

Fact C.2. *Let $a \leq b \leq n$ be integers such that $\sqrt{n}|a$ and $\sqrt{n}|b$. Then it holds that $\binom{b/\sqrt{n}}{\geq a/\sqrt{n}}^{\sqrt{n}} \leq \binom{b}{\geq a} \cdot 2^{o(n)}$*

Proof. We denote $M = b/2$ when $a < b/2$, and $M = a$ otherwise. Then

$$\binom{b/\sqrt{n}}{\geq a/\sqrt{n}}^{\sqrt{n}} \leq \left(\frac{b-a+1}{\sqrt{n}} \cdot \binom{b/\sqrt{n}}{M/\sqrt{n}}\right)^{\sqrt{n}} \leq \left(\frac{b-a+1}{\sqrt{n}}\right)^{\sqrt{n}} \binom{b}{M} \leq \binom{b}{\geq a} \cdot 2^{o(n)},$$

where the middle inequality is a result of Fact C.1 with $k = \sqrt{n}$. □

C.3 LSS for downslices with constant density below 0.5

In Section 5.4 we did not try to optimize the exponent of LSS for every specific downslice. In this section we prove a refined bound for the exponent of LSS of a given downslice.

Theorem C.3. *LSS for (b, n)-downslices can be realized with the following exponents:*

$$\mathbf{D}_\ell(b,n) \leq \begin{cases} \mathrm{H}_2(b/n) - 0.534(1-b/n) + o(1) & \text{if } 0.535n < b < n \\ \mathrm{H}_2(u_b^*/n) - 0.534u_b^*/n & \text{if } 0.135n \leq b \leq 0.535n \\ \mathrm{H}_2(b/n) - 0.534(b/n) + o(1) & \text{if } 0 < b < 0.135n \end{cases},$$

where $u_b^* \in [b]$ is the value of u that solves the equation $\mathrm{H}_2(u/n) - 0.534u/n - \frac{1}{2} - \frac{b}{2n} \cdot \mathrm{H}_2(u/b) = 0$.

For every β-downslice, Theorem C.3 yields an exponent E_β that is better than the exponent, $\mathrm{H}_2(\beta)$, of the CNF-based scheme, and is worse than than $\frac{1}{2}\mathrm{H}_2(\beta)$ that can be shown to lower-bound the linear exponent of β-downslices. (The lower bound follows from counting arguments for span programs similarly to the lower bound for slice access structures given in [9]

Proof. The proof is given by showing three different (though closely related) schemes. The scheme for the first case of $0.535n < b < n$ is that described in Section 5.4 summarized by (9), and the other two use it as a building block. Both schemes for the latter cases are applicable for a wide range of slices, but one is better for the range $[0, 0.135n]$ and the other for $[0.135n, 0.535n]$. We start by showing the scheme for the slices in the low range:

Claim C.4. *For $b < \beta_0 n$ where $\beta_0 \sim 0.408$ is the maximizer of the expression $\mathrm{H}_2(\beta) - 0.534(\beta)$, it holds that $\mathbf{D}_\ell(b,n) \leq \mathrm{H}_2(b/n) - 0.534(b/n) + o(1)$.*

Proof of Claim C.4. The proof relies on the following variant of Lemma 5.6.

Fact C.5. *Let $b < n$ be integers, then*

$$\mathbf{D}_\ell(b,n) \leq \max_{i \leq b+1}\{\mathbf{U}_\ell(i,n)\} + o(1) = \max_{j \geq n-(b+1)}\{\mathbf{D}_\ell(j,n)\} + o(1).$$

Proof of Fact C.5. It suffices to prove the inequality since the equality follows from the duality of LSS (Corollary 5.5). For a (b,n)-downslice f, let f_i be the i-upslice of f. Since the min-terms of f cannot be bigger than $b+1$, it holds that $f = \bigvee_{i=0}^{b+1} f_i$ and we can linearly realize f with an exponent of $\max_{i\le b+1}\{\mathbf{U}_\ell(i,n)\} + o(1)$. □

We now combine Fact C.5 with the upper-bound obtained in (9) (the first case of Theorem C.3), and bound the exponent of (b,n) downslices by the exponent of low upslices:

$$\mathbf{D}_\ell(b,n) \le \max_{j\le b+1}\{\mathrm{H}_2(j/n) - 0.534j/n\} + o(1) \qquad \forall b \in [n-0.535n, n].$$

Then since $\mathrm{H}_2(j/n) - 0.534(j/n)$ is monotonically increasing with j until $j = \lfloor \beta_0 n \rfloor$, the expression can be simplified to the desired one for every $b < \beta_0 n$. □

Next we describe the scheme for slices in the range $[0.135n, 0.535n]$.

Claim C.6. *For every $b \in [0.135n, 0.58n]$, every (b,n)-downslice can be linearly realized with an exponent of*

$$\mathbf{D}_\ell(b,n) \le \min_{u\in[b]}\left[\max\left(\mathrm{H}_2(u/n) - 0.534u/n, \frac{1}{2} + \frac{b}{2n}\cdot \mathrm{H}_2(u/b)\right)\right] + o(1).$$

Proof of Claim C.6. We start from (9), with an exponent of $\mathbf{D}_\ell(d/n) \le \mathrm{H}_2(d/n) - 0.534(1-d/n)$ for every $d \in [0.535n, n]$. Then, by duality (Corollary 5.5), we have linear schemes for upslices in the range $[0, 0.465n]$ with the same share size as their duals. Next, we apply Lemma 5.6 on the downslice b with our new schemes for upslices and get the following exponents:

$$\mathbf{D}_\ell(b,n) \le \min_{u\in[b], u<0.465n}\left[\max\left(\max_{j\le u}\left(\mathrm{H}_2(j/n) - 0.534j/n\right), \mathbf{M}_\ell(u:b,n)\right)\right] + o(1).$$

We then realize the $(u:b,n)$ multislice with the following exponent promised by Lemma 4.5:

$$\mathbf{M}_\ell(u:b,n) \le \begin{cases} \frac{1}{2} + \frac{b}{2n}\cdot \mathrm{H}_2\left(\frac{u}{b}\right) & \text{if } u > b/2 \\ \frac{1}{2} + \frac{b}{2n} & \text{if } u \le b/2 \end{cases}. \tag{19}$$

The RHS of (19) is monotonically non-increasing in u, and $\max_{j\le u}(\mathrm{H}_2(j/n) - 0.534j/n)$ is monotonically non-decreasing in u. Therefore if they intersect, the minimum of the maximums between them will be their value at their intersection point. For every $b \in [0.135n, 0.58n]$, we verify numerically that the RHS of (19) and $\mathrm{H}_2(u/n) - 0.534u/n$ intersect on some $u^* < 0.465n$. Furthermore, $u^* > b/2$ and $\max_{j\le u^*}(\mathrm{H}_2(j/n) - 0.534j/n) = (\mathrm{H}_2(u^*/n) - 0.534u^*/n)$. Therefore we can simplify the last expression to the desired one and conclude the proof of Claim C.6. □

This completes the proof of Theorem C.3. □