Electronic Colloquium on Computational Complexity, Report No. 146 (2026)

Resolving the Complexity of Linear Secret Sharing

Oded Nir*

August 12, 2026

Abstract

A secret-sharing scheme allows a dealer to distribute a secret s among n parties such that only predefined "authorized" sets of parties can reconstruct the secret, and all other "unauthorized" sets learn nothing about s. Families of authorized sets are called access structures, and a scheme is called linear if its sharing map is linear in the secret and the dealer's randomness. We show that every n-party access structure can be realized by a linear secret-sharing scheme for one-bit secrets with maximal share size of $2^{\lceil n/2 \rceil - 1} + 1$ bits. A counting lower bound for monotone span programs shows that almost all access structures require linear share size $2^{n/2-o(n)}$, which makes our upper bound tight. Our scheme is considerably simpler than previous schemes that obtained share size $2^{cn+o(n)}$ with $1/2 \leq c < 1$.

We also present a variant of this linear construction that is tailored for monotone k-DNFs access structures (also known as k-upslices). Then, by combining it with a non-linear scheme of Applebaum et al. (STOC 2020), we derive a scheme for all access structures with share size $2^{0.496n+o(n)}$. This improves the previous upper bound of $2^{0.585n+o(n)}$ by Applebaum and Nir (CRYPTO 2021), and establishes a separation between the worst-case non-linear and linear exponents. Plugging the quadratic construction of Beimel, Othman, and Peter (CRYPTO 2021) into this framework yields quadratic schemes of share size $2^{0.4995n+o(n)}$, separating the quadratic and linear exponents.

The linear scheme for upslices and its proof were discovered in conversations prompted by the author with GPT-5.6 Sol and Claude Fable 5.

1 Introduction

Secret-sharing schemes allow a dealer to distribute a secret among n parties so that every *authorized* coalition can reconstruct the secret while every other coalition learns nothing about it. The family of authorized coalitions is a monotone collection, identified with a monotone function $f : \{0,1\}^n \to \{0,1\}$ and called an access structure. Throughout the paper, we treat access structures as either families of authorized sets or their corresponding functions, according to the view which best fits the context. Secret-sharing schemes were first introduced by Shamir [27] and Blakley [17] for threshold functions, and Ito, Saito, and Nishizeki [24] were the first to realize general functions.

A scheme is *linear* over a field $\mathbb{F}$ if the secret is an element in $\mathbb{F}$, the dealer's randomness is a vector of elements in $\mathbb{F}$, and every share is a vector of $\mathbb{F}$-linear combinations of the secret and the randomness[1]. Linear schemes are equivalent to the computational model of monotone span

*Ben-Gurion University, Beer Sheva, Israel. Email: odednir123@gmail.com. ORCID: 0009-0008-7860-8151

[1]Equivalently, a scheme is linear if every authorized coalition can reconstruct the secret as an $\mathbb{F}$-linear combination of its shares [8].

ISSN 1433-8092

programs [25]. Linearity is essential in many applications, e.g., secure multiparty computation [18] and attribute-based encryption [28, 6], since parties can locally add shares of two secrets and obtain shares of their sum.

The most important complexity measure for secret sharing is the size of the shares. Formally, given an access structure 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 $\mathcal{D}$. We compare asymptotic share sizes through their exponential rates, and we say that a construction whose worst-case share size is $2^{cn+o(n)}$ has exponent c. Formally, following [3], we define the *secret-sharing exponent* of a monotone function $f : \{0,1\}^n \to \{0,1\}$ as $\mathbf{S}(f) := n^{-1} \cdot \log_2 \mathsf{SSize}(f)$, and define the (worst-case) *secret-sharing exponent* of a family of functions $\mathcal{F}$ to be $\limsup_{n\to\infty} \max_{f\in\mathcal{F}} \mathbf{S}(f)$. Let $\mathbf{S}$ denote the exponent of the family of all monotone functions over $\{0,1\}^n$, and let $\mathbf{S}_\ell$ denote the *linear exponent*, which 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. Unless stated otherwise, these exponent notations are defined for schemes with a one-bit secret.

For general access structures, a sequence of works has progressively reduced these exponents. Liu and Vaikuntanathan [26] were the first to break the barrier of $2^{n-o(n)}$ and prove that both $\mathbf{S}$ and $\mathbf{S}_\ell$ are smaller than 1. Their construction was based on conditional disclosure of secrets protocols (CDS) [22] composed according to a monotone formula. Applebaum et al. [2] improved their results by replacing one of the ingredients in their construction with a recursive scheme, and Applebaum et al. [3] offered a further improvement by introducing and implementing robust conditional disclosure of secrets protocols (RCDS) (for more details about RCDS, see [3]). The schemes of Applebaum and Nir [5] were based on a decomposition of functions into upslices (equivalently, monotone k-DNFs) and downslices (equivalently, monotone k-CNFs), and Alon, Beimel, and Lasri [1] optimized one part of the linear schemes of [3, 5] to obtain another improvement. The table below lists the exponents of these schemes, along with the exponents of the schemes presented in this paper:

Work	Non-linear exponent	Linear exponent
Ito-Saito-Nishizeki (1987) [24]	1	1
Liu-Vaikuntanathan (2018) [26]	0.994	0.999
Applebaum et al. (2019) [2]	0.892	0.942
Applebaum et al. (2020) [3]	0.637	0.762
Applebaum-Nir (2021) [5]	$\log_2(3/2) \approx 0.585$	0.7576
Alon-Beimel-Lasri (2025) [1]	—	0.7563
Theorem 1.1 (this work)	0.5	0.5
Theorem 1.5 (this work)	0.496	—

Table 1: Exponents c in share-size bounds of the form $2^{cn+o(n)}$. A dash indicates that the work does not provide a new non-linear/linear construction.

On the lower bound front, for unrestricted schemes Csirmaz constructed n-party access structures for which the total share size is at least $\Omega(n^2/\log n)$ times the size of the secret [19]. For linear schemes, counting monotone span programs gives a dramatically stronger bound. Define the *share length* of a party in a linear scheme as the number of field elements in its share. For every fixed finite field $\mathbb{F}$, almost all n-party access structures require total share length $2^{n/2-o(n)}$ [7]. Moreover, a field-uniform version exists for bit-complexity: almost all n-party access structures require share size $2^{n/2-o(n)}$ in every finite field [11, 10]. In contrast, the best-known

lower bound on the share length that applies to all fields simultaneously is only $2^{n/3-o(n)}$ [11]. In this work we prove that the fixed finite field bound for linear schemes is tight.

1.1 Our results

1.1.1 Linear secret sharing

Our first result is the following:

Theorem 1.1 (Main theorem)**.** *For every finite field $\mathbb{F}$, every monotone function $f : \{0,1\}^n \to \{0,1\}$ can be realized by a linear secret-sharing scheme over $\mathbb{F}$ with maximal share length of $2^{\lceil n/2 \rceil - 1} + 1$ field elements. When the field is $\mathbb{F}_2$ the maximal share size is $2^{\lceil n/2 \rceil - 1} + 1$ bits.*

This theorem implies that for every finite field $\mathbb{F}$ every monotone function over n variables can be computed by a monotone span program over $\mathbb{F}$ of size at most $n\left(2^{\lceil n/2 \rceil - 1} + 1\right)$, since the size of the program corresponds to the total number of field elements given to the parties, which is at most n times the maximal share length. Combined with the counting lower bound (e.g., [14]), a direct consequence of Theorem 1.1 is that the worst-case linear exponent $\mathbf{S}_\ell$ (which, as other exponents, is defined for schemes with one-bit secrets) is exactly $1/2$.

Next, by introducing some modifications to our main construction we obtain more than the bound for general functions: we can prove an upper bound on the exponent of every *layer*. Following [5], we define (k,n)-upslices as functions over n bits that can be represented by logical formulas in a disjunctive normal form (DNF) in which each term consists of exactly k variables. These functions were studied in the context of secret sharing since 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)-upslice function that agrees with f on its a-weight inputs (hereafter referred to as the *a-upslice of f*). Hence, due to standard closure properties of secret sharing over OR gates (Definition A.6), the secret-sharing complexity of worst-case monotone functions is at most n times larger than the secret-sharing complexity of upslices. We prove the following theorem which resolves the complexity of "high" upslices, and will help us build the non-linear schemes with exponent below $1/2$.

Theorem 1.2 (Upslice bounds)**.** *For every finite field $\mathbb{F}$, and for all integers n, $1 \le k \le n$, and $0 \le q \le n-1$, with $t = \lceil kq/n \rceil$, every (k,n)-upslice can be realized by a linear secret-sharing scheme over $\mathbb{F}$ with total share length*

$$\left[\binom{n-q}{k-t} + \sum_{j=t}^{q} \binom{q}{j} \right] \cdot O(n^2 \log n).$$

Tightness for high upslices For $\alpha \in (0,1)$, let $\mathsf{U}_\ell(\alpha)$ denote the worst-case linear exponent of $\lceil \alpha n \rceil$-upslices, and define $H_2(\alpha)$ to be the binary entropy function of α. Then, by optimizing the choice of q for each k in Theorem 1.2, we prove that for upslices of constant density the following holds:

Corollary 1.3 (Upslice bounds for constant density)**.** *For every $\alpha \in (0,1)$, the linear exponent of $\lceil \alpha n \rceil$-upslices satisfies $\mathsf{U}_\ell(\alpha) \le u(\alpha)$, where*

$$u(\alpha) = \frac{H_2(\alpha)}{1 + H_2(\alpha)} \quad \text{for } 0 < \alpha \le \tfrac{1}{2}, \qquad u(\alpha) = \frac{H_2(\alpha)}{2} \quad \text{for } \tfrac{1}{2} \le \alpha < 1.$$

Proof. We apply Theorem 1.2 with $q = \lceil \lambda n \rceil$ for a constant $\lambda \in (0,1)$. By Claim 6.3 which approximates the binomial coefficients, the total share size of upslices of density α promised by Theorem 1.2 is

$$2^{\max\{(1-\lambda)h,\ \lambda\kappa\}\, n + o(n)},$$

where $h = H_2(\alpha)$ and $\kappa = \kappa(\alpha)$ equals h for $\alpha \in [1/2, 1)$ and 1 for $\alpha \in (0, 1/2)$. The maximum is minimized when the two terms are equal, at $\lambda = h/(h+\kappa)$, where it equals $h\kappa/(h+\kappa)$. Plugging in the two cases of κ gives the desired result. □

Since u attains its unique maximum $\frac{1}{2}$ at the middle layer, the worst layer is $\alpha = \frac{1}{2}$.

Combining the upper bound for αn-upslices with the existing counting lower bounds for one-bit secrets, we get that our results are tight for every $\alpha \geq 1/2$:

Corollary 1.4 (Upslice exponents)**.** *For every constant $\alpha \in [1/2, 1)$ it holds that $\mathsf{U}_\ell(\alpha) = \frac{H_2(\alpha)}{2}$.*

Proof. Beimel et al. define the rank of an access structure as the maximal size of its minterms, and prove in [14, Theorem 6.8] that in every family L of access structures with rank at most r, almost all access structures require shares of size $\Omega\left(\sqrt{\log |L|/rn}\right)$ from any linear secret-sharing scheme for one-bit secrets.

For every k, the family of k-upslices has rank at most k and size $2^{\binom{n}{k}}$, and therefore by approximating the constant-density binomial coefficient we get that almost every upslice of density α requires linear share size $\Omega\left(\sqrt{\binom{n}{\alpha n}/\alpha n^2}\right) = 2^{H_2(\alpha)n/2 - o(n)}$. □

1.1.2 Non-linear secret sharing

Theorem 1.1 already improves the best unrestricted exponent from $\log_2(3/2) \approx 0.585$ [5] to 1/2. One could have conjectured that this is also the worst-case complexity of general schemes, but in this part we show that this is not the true bound. To go below 1/2, we combine our linear scheme for upslices with a few building blocks and ideas developed in previous works, including the now-classical framework of Liu and Vaikuntanathan [26], schemes for downslices via duality [5], and a non-linear scheme of [3]. We prove the following theorem:

Theorem 1.5 (Beyond the linear exponent)**.** *Every monotone function $f : \{0,1\}^n \to \{0,1\}$ can be realized by a secret-sharing scheme for one-bit secrets with maximal share size $2^{0.496n + o(n)}$. Hence $\mathbf{S} \leq 0.496 < \frac{1}{2} = \mathbf{S}_\ell$, and the non-linear secret sharing exponent is strictly smaller than the linear one.*

Previously, a separation between the unrestricted and linear exponents was known only under unproven hypotheses [5, 13], or for restricted families of functions such as slices [26, 14]. We include the proof here in the introduction, but before doing so we need to define another family of functions called *downslices*, also used in [5]. A (b, n)-*downslice* is a function over n bits whose maxterms all have Hamming weight b. Crucially, downslices are *dual* functions of upslices. The dual of a function f is the function f^* defined by $f^*(x) = 1 - f(\overline{x})$ on every input, and it is known (e.g., [20]) that if f has a linear secret-sharing scheme with total share size t then its dual f^* has a linear scheme with the same total share size. Hence, writing $\mathsf{D}_\ell(\beta)$ for the worst-case linear exponent of (b, n)-downslices with $b = \lfloor \beta n \rfloor$, it holds that $\mathsf{D}_\ell(\beta) = \mathsf{U}_\ell(1 - \beta)$. Then, Corollary 1.3 gives the following.

Corollary 1.6 (Downslice bounds for constant density)**.** *For every $\beta \in (0,1)$, the linear exponent of $\lfloor \beta n \rfloor$-downslices satisfies $\mathsf{D}_\ell(\beta) \le d(\beta)$, where*

$$d(\beta) = \frac{H_2(\beta)}{2} \quad \text{for } 0 < \beta \le \tfrac{1}{2}, \qquad d(\beta) = \frac{H_2(\beta)}{1 + H_2(\beta)} \quad \text{for } \tfrac{1}{2} \le \beta < 1.$$

We note that the tightness of the bound for upslices with density above $1/2$ of Corollary 1.4 translates by duality to the tightness of the upper bound for downslices of density below $1/2$. We are now ready to prove Theorem 1.5.

Proof of Theorem 1.5. Let δ be a constant in $(0, 1/6)$ to be fixed later, and let $f : \{0,1\}^n \to \{0,1\}$ be a monotone function. Following [26], we realize f by decomposing it into three parts parametrized by δ. It holds that $f = f_{\text{top}} \wedge (f_{\text{mid}} \vee f_{\text{bot}})$, where:

- $\boldsymbol{f_{\text{bot}}}$ is the monotone function whose minterms are the minterms of f of size less than $(1/2-\delta)n$. Equivalently, $f_{\text{bot}}(x) = 1$ if and only if there exists a minterm y of f such that $\text{wt}(y) < (1/2-\delta)n$ and $y \le x$.
- $\boldsymbol{f_{\text{top}}}$ is the monotone function whose maxterms are the maxterms of f of size greater than $(1/2+\delta)n$. Equivalently, $f_{\text{top}}(x) = 0$ if and only if there exists a maxterm y of f such that $\text{wt}(y) > (1/2+\delta)n$ and $x \le y$.
- $\boldsymbol{f_{\text{mid}}}$ agrees with f on all inputs x of Hamming weight $\text{wt}(x) \in [(1/2-\delta)n, (1/2+\delta)n]$, outputs 0 on inputs of smaller weight, and outputs 1 on inputs of larger weight. We call such functions δ-midslice functions.

The equality $f = f_{\text{top}} \wedge (f_{\text{mid}} \vee f_{\text{bot}})$ can be verified on inputs of sizes below $(1/2-\delta)n$, above $(1/2+\delta)n$ and in between, as done in [26, Lemma 3.3]. By the closure properties of secret sharing over $\wedge$ and $\vee$, the share size of f is at most the sum of share sizes of $f_{\text{top}}, f_{\text{mid}}, f_{\text{bot}}$, and it is left to realize these three access structures. We realize f_{mid} according to the following theorem (this piece is the only non-linear one):

Theorem 1.7 (Midslice schemes [3, Lem. 5.10])**.** *For every constant $\delta \in (0, 1/2)$, every δ-midslice access structure over n parties can be realized by a secret-sharing scheme for one-bit secrets with total share size $2^{\mathsf{M}(\delta)\, n + o(n)}$, where*

$$\mathsf{M}(\delta) = \begin{cases} \left(\frac{1}{2}+\delta\right) H_2\left(\frac{1/2-\delta}{1/2+\delta}\right), & 0 < \delta \le \frac{1}{6}, \\ \frac{1}{2}+\delta, & \frac{1}{6} < \delta < \frac{1}{2}. \end{cases}$$

Then, grouping the authorized sets of f_{bot} by their cardinality, we can express f_{bot} as an OR of at most n upslices. Let $k_0 = \lceil (1/2-\delta)n \rceil - 1$, and for every $1 \le k \le k_0$ let f_k be the k-upslice of f. Then $f_{\text{bot}} = \bigvee_{k=1}^{k_0} f_k$. We realize these upslices separately using Theorem 1.2. The share size is increasing with k below the middle layer, so the largest cost is at most the share size of the (k_0+1)-upslice, whose share size is $2^{u(1/2-\delta)n + o(n)}$ by Corollary 1.3. Composing at most n schemes over an OR gate contributes a factor of n which does not change the asymptotic size.

Dually, f_{top} is an AND of at most n downslices of density at least $\beta \ge 1/2 + \delta$, realized with Corollary 1.6 with the same cost. The overall exponent is therefore $\max\{u(1/2-\delta), \mathsf{M}(\delta)\}$, which is minimized when $\delta^* \approx 0.0807$ and $u(1/2-\delta^*) = \mathsf{M}(\delta^*) < 0.496$. □

Quadratic schemes with exponent below one half. In a quadratic secret-sharing scheme, both sharing and reconstruction are computed by polynomials of degree at most two over the same field [15]. We obtain the following separation of quadratic secret sharing from linear secret sharing.

Theorem 1.8 (Quadratic schemes beyond the linear exponent)**.** *Every monotone access structure over n parties can be realized by a secret-sharing scheme with quadratic sharing and reconstruction with total share size at most $2^{0.4995n+o(n)}$. Hence the quadratic secret-sharing exponent is at most $0.4995 < \frac{1}{2} = \mathbf{S}_\ell$, and is strictly smaller than the linear one.*

Proof. Following the steps of the proof of Theorem 1.5, it suffices to replace the non-linear δ-midslice upper bound of Theorem 1.7 with a quadratic one. Indeed, the schemes used there for f_{bot} and f_{top} are linear and the standard compositions over OR and AND preserve linearity, and so all steps other than the δ-midslice construction have sharing and reconstruction degree at most one.

Such a δ-midslice scheme can be obtained by combining the quadratic RCDS protocol of [15, Thm. 6.5] with the RCDS-to-midslice compiler of [3, Lemmas 5.5 and 5.8], resulting in the following theorem (see Section 6.2 for the mentioned calculations):

Theorem 1.9 (Quadratic midslice schemes)**.** *For every constant $\delta \in (0, 1/2)$, every δ-midslice function over n parties can be realized by a secret-sharing scheme for one-bit secrets with quadratic sharing and reconstruction and total share size $2^{\mathsf{Q}(\delta)\, n+o(n)}$, where*

$$\mathsf{Q}(\delta) = \begin{cases} \frac{1}{3} + \frac{1+2\delta}{3} H_2\left(\frac{1-2\delta}{1+2\delta}\right), & 0 \le \delta \le \frac{1}{6}, \\ \frac{2}{3} + \frac{2\delta}{3}, & \frac{1}{6} \le \delta < \frac{1}{2}. \end{cases}$$

Similarly to the proof of Theorem 1.5, the exponent for general functions is therefore $\max\{u(1/2-\delta), \mathsf{Q}(\delta)\}$. Optimizing over δ gives an exponent of 0.4995, strictly below $1/2$, with $\delta^* \approx 0.02668$. □

In contrast to the linear case, this quadratic upper bound is not known to be tight: the best-known lower bound for schemes with reconstruction degree d is $2^{n/(d+1)-o(n)}$, which for $d = 2$ gives only $2^{n/3-o(n)}$ [15].

Remark 1.10 (Schemes with reconstruction of degree d)**.** The same argument as in Theorem 1.8 extends beyond quadratic reconstruction. Using the degree-d-reconstruction RCDS protocols of Beimel, Farràs, and Lasri [12, Corollary 7.2] in our construction gives a sequence of degree-d-reconstruction schemes whose exponents approach our unrestricted exponent of Theorem 1.5 as $d \to \infty$.

1.2 Our techniques

The linear scheme for general access structures. Our scheme is based on a relatively simple concept. In a nutshell, the n secret-sharing parties are partitioned into left and right parts L and R. Then, the dealer distributes to the left parties many additive shares of the secret masked with different sets of random pads, and the right parties receive different sets of the pads. The dealer determines according to the access structure how exactly these masked values and pads are assigned to each of the parties, in a way that ensures both correctness and privacy. The

same approach was used in the 2-server RCDS protocol of [3, Lemma B.1] (which in turn was inspired by the work of [21]), and our scheme can be seen as a natural development of it that uses different sets of pads for the right-side parties.

For simplicity, we describe in this part of the introduction the schemes over the field $\mathbb{F}_2$. Sections 3 and 4 give the constructions over an arbitrary finite field. We also note that it is straightforward to verify that the first construction works over any finite abelian group, as the construction and its analysis use only addition, subtraction, and the sampling of uniform elements.

We now give more details. Let F be an access structure over n parties, let $s \in \mathbb{F}_2$ be the secret and fix a partition $[n] = L \sqcup R$. We call L the left side or the *masking side* and R the right side or the *disclosure side*. For every $T \subseteq R$, the dealer samples an independent pad ω_T, and for every $U \subseteq L$ it computes a masked value of the secret $m_U = s + \sum_{T:\, F(U \cup T)=0} \omega_T$. The dealer then shares these masked values and the pads according to the following steps (note that $m_\varnothing$ is given to parties in the disclosure side).

- For every nonempty $U \subseteq L$, share m_U additively among the parties of U. Give a copy of $m_\varnothing$ to every party of R.
- For every $T \subseteq R$, give ω_T to every party in $R \setminus T$.

Correctness and privacy are relatively straightforward (see a formal proof in Section 3). Let B be a coalition, and write $C = B \cap L$ and $D = B \cap R$. If B is authorized, its parties can reconstruct m_C from the additive scheme (or receive $m_\varnothing$ directly), and they can also reconstruct every pad that masks the secret in m_C: indeed, if a pad ω_T masks m_C, then the coalition $C \cup T$ is unauthorized. Consequently, $D \nsubseteq T$, since otherwise $B = C \cup D$ would be contained in the unauthorized coalition $C \cup T$ and would therefore also be unauthorized.

If B is unauthorized, the pad ω_D masks every value m_U that the parties of B can reconstruct, since $U \cup D \subseteq B$ implies that $U \cup D$ is unauthorized by monotonicity. In addition, ω_D is not disclosed to the disclosure-side parties of B, since they are exactly the parties in D. Therefore, a single hidden pad masks the secret in the entire view of the coalition, which suffices for proving privacy. The formal construction and proof appear in Construction 3.1 and Theorem 3.2.

Each party of L receives one additive share for every subset $U \subseteq L$ that contains it, and hence holds $2^{|L|-1}$ bits. Each party of R receives $m_\varnothing$ and one pad for every T that does not contain it, and hence holds $2^{|R|-1} + 1$ bits. Choosing $|R| = \lceil n/2 \rceil$ gives the desired share size.

The linear scheme for upslices. Our linear scheme for upslices is based on a realization of a more structured family of functions we call *partitioned k-upslices*. In a partitioned k-upslice f_Π, parametrized by a partition Π of the inputs to left and right parts, every minterm has weight k, with exactly $k - t$ 1's in the left side and t in the right. Working with these functions allows us to adjust the mechanism behind the scheme for general functions in a way that enables exponential savings in the share size. Then, a general upslice can be realized by composing partitioned-upslices with only a multiplicative overhead of n. We describe these two steps.

Given a partition Π into L and R of sizes $n - q$ and q respectively, every minterm of a partitioned upslice f_Π is of the form $U \cup V$ with $|U| = k - t$, $|V| = t$ and $U \subseteq L$, $V \subseteq R$. We think of the parties of L and R as the masking-side parties and the disclosure-side parties in the general construction above.

Now, in contrast to the linear scheme for general functions, the dealer computes the masked values only for sets $U \subseteq L$ of size $k - t$, and samples pads only for sets in $\mathcal{T} = \{T \subseteq R$ with

$|T| \geq t\}$. To ensure that subsets of R of size smaller than t receive no information, we add one extra pad η that masks every m_U and is shared among the parties of R using a t-out-of-q threshold scheme (Definition A.4). That is, for every $U \in \binom{L}{k-t}$, the dealer computes

$$m_U = s + \eta + \sum_{T \in \mathcal{T} : f_\Pi(U \cup V) = 0 \text{ for every } V \in \binom{T}{t}} \omega_T.$$

The dealer then distributes the following shares:

- For every $U \in \binom{L}{k-t}$, share m_U additively among the parties of U.
- Share η among the parties of R using a t-out-of-q threshold scheme. For every $T \subseteq R$ with $|T| \geq t$, give ω_T to every party in $R \setminus T$.

Correctness and privacy follow from similar arguments to the general scheme, and the share size will now depend on k and decrease as k moves away from $n/2$. There are $\binom{n-q}{k-t}$ masked values m_U, and each is additively shared among $k - t \leq n$ parties, summing to at most $n\binom{n-q}{k-t}$ bits in total. For every set T of size j, the one-bit pad ω_T is given to the $q - j \leq n$ parties of $R \setminus T$, contributing at most $n\binom{q}{j}$ bits in total for all traces of size j. Finally, the total share size of the Shamir sharing of η is bounded by $O(n \log n)$. Thus, the total share size is at most

$$\left[\binom{n-q}{k-t} + \sum_{j=t}^{q} \binom{q}{j} \right] O(n \log n). \tag{1}$$

It remains to realize general upslices from partitioned ones. We construct a family of partitions $\Pi_1, \ldots, \Pi_z$ that have a covering property: every k-subset $A \subseteq [n]$ has profile $(k-t, t)$ in at least one partition. Given a (k, n)-upslice f_k, for every $i \in [z]$ let f_{Π_i} be the partitioned upslice whose minterms are precisely the minterms of f_k having profile $(k-t, t)$ in Π_i. By the covering property, every minterm of f_k is a minterm of at least one f_{Π_i}, while every minterm of each f_{Π_i} is a minterm of f_k. Therefore, $f_k = \bigvee_{i=1}^{z} f_{\Pi_i}$, which results in share size (1) times z by the standard closure of secret sharing under OR.

We then construct an explicit family of $z = n$ partitions with this covering property, obtained using the classical sliding-window idea that also appeared in discrete necklace splitting [23]. This leads to the desired share size.

1.3 Open problems

Improved exponent via optimal linear schemes for low upslices. By Corollary 1.3 and Corollary 1.4, it holds that the exponent $\mathsf{U}_\ell(\alpha)$ of upslices with density α below $1/2$ satisfies

$$\frac{H_2(\alpha)}{2} \;\leq\; \mathsf{U}_\ell(\alpha) \;\leq\; u(\alpha) = \frac{H_2(\alpha)}{1 + H_2(\alpha)}.$$

Hence, it remains open whether every $(\alpha n, n)$-upslice with $\alpha < \frac{1}{2}$ can be realized by a linear scheme with total share size $2^{H_2(\alpha)n/2 + o(n)}$. By duality, a positive answer would also close the analogous gap in the exponents of downslices. Such optimal low upslices and downslices can be plugged directly into the proof of Theorem 1.5, and lead to an improved unrestricted exponent smaller than 0.491 instead of 0.496, with δ^* that is roughly 0.079.

Monotone span programs vs. formulas over slices. As mentioned before, linear secret-sharing schemes are equivalent to the computational model of monotone span programs (MSPs). In contrast, all the known nontrivial upper bounds for non-linear secret sharing for general functions arise from constructions in a different computational model, named formulas over slices (FOS) [4]. Prior to this work, the FOS constructions for general functions were stronger than the MSP ones, peaking at FOS of size $1.5^{n+o(n)}$[5]. Following our results, MSPs are now in the lead, and a combined FOS+MSP model breaks the MSP lower bound. This brings forward the following questions, some of them already discussed in [4]: 1) Is the FOS model stronger than MSPs for general functions? More concretely, does every function have an FOS of size $2^{(0.5-\epsilon)n+o(n)}$ for some constant $\epsilon > 0$? 2) Can a computational model of formulas with both MSP and slice gates help circumvent the existing FOS lower bound of $2^{\Omega(n/\log^2 n)}$ of [4]? Alternatively, can we prove lower bounds in this stronger model?

1.4 Organization

Section 2 fixes notation. Section 3 presents the linear scheme for general access structures and proves Theorem 1.1. Section 4 presents the scheme for a single partitioned upslice and proves its correctness, privacy, and share-size bound. Section 5 constructs the explicit family of partitions and combines it with the results of the previous section to prove Theorem 1.2. Section 6 collects the binomial estimates used to evaluate the upslice bounds of constant density in Corollary 1.3, and derives the quadratic midslice bound of Theorem 1.9. Finally, Appendix A contains the formal definitions of secret-sharing schemes, basic secret-sharing tools, and function families used in the paper.

1.5 Statement on AI Use

The upslice construction and the proof of Theorem 1.2 were developed through author-prompted conversations with GPT-5.6 Sol and Claude Fable 5. We reached the rest of the results later based on this scheme.

We asked GPT-5.6 Sol to devise a research plan to improve the share size of linear secret sharing for general access structures. A few rounds of prompting led to a linear scheme with exponent 0.73 based on schemes for upslices, implemented with two-server RCDS protocols similar to that of [3]. We then prompted both GPT-5.6 Sol and Fable 5 to improve the result by suggesting specific techniques, copying text from conversation with one model to another. This led GPT-5.6 Sol to output a linear scheme with exponent 2/3, based on an optimization of the previous RCDS-based upslice scheme. Asking it to improve the exponent further led to a linear scheme with exponent 1/2 based on a K-server RCDS protocol with $K = \Theta(n^{1/3})$. We then identified several ways to simplify the scheme, and feeding these simplifications back to GPT-5.6 Sol led to more simplifications and to the scheme presented in the paper.

All of the text in the paper was written by the author, sometimes with the aid of drafts generated by the two models. The author manually verified all of the proofs.

2 Preliminaries

Standard background on secret sharing and formal definitions of slices, multislices, midslices, upslices and downslices is deferred to Appendix A.

2.1 Notation

All logarithms are base two. We identify a coalition with a subset of $[n]$. For a finite set R and an integer r, $\binom{R}{r}$ denotes the family of all r-subsets of R. The binary entropy function is $H_2(\rho) = -\rho \log \rho - (1-\rho)\log(1-\rho)$. We denote by $\kappa(\rho)$ the function that equals 1 for $\rho \in (0, 1/2)$ and $H_2(\rho)$ for $\rho \in [1/2, 1)$.

Notation on Monotone Boolean Functions. The *weight* of an input $x \in \{0,1\}^n$, denoted $\mathrm{wt}(x)$, is the number of bits in x that are one, i.e., $\mathrm{wt}(x) = |\{i : x_i = 1\}|$. For two strings $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \{0,1\}^n$, we say that $x \leq y$ if $x_i \leq y_i$ for every $1 \leq i \leq n$. A function $f : \{0,1\}^n \to \{0,1\}$ is *monotone* if $x \leq y$ implies $f(x) \leq f(y)$.

A *minterm* of a monotone function f is a minimal input $x \in \{0,1\}^n$ such that $f(x) = 1$, i.e., for every $y \neq x$ if $y \leq x$ then $f(y) = 0$. A *maxterm* of a monotone function f is a maximal input $x \in \{0,1\}^n$ such that $f(x) = 0$, i.e., for every $y \neq x$ if $y \geq x$ then $f(y) = 1$.

3 Linear Secret Sharing for General Access Structures

Let $\mathbb{F}$ be a finite field, and let F be an access structure over $[n]$. Let $L \sqcup R$ be a partition of $[n]$ into nonempty sets with $|L| = \ell$ and $|R| = q$. For every $U \subseteq L$ and $T \subseteq R$, define the public coefficient $\gamma_U(T) \in \{0,1\} \in \mathbb{F}$ by

$$\gamma_U(T) = 1 \iff F(U \cup T) = 0. \tag{2}$$

We next describe the scheme. Its correctness, privacy, and share size are established in Theorem 3.2, which implies Theorem 1.1.

Construction 3.1 (Linear scheme for general access structures)**.**

Let $s \in \mathbb{F}$ be the secret. The dealer samples independent uniform field elements $(\omega_T)_{T \subseteq R}$, and distributes the following shares over $\mathbb{F}$.

Masking side. For every $U \subseteq L$, compute

$$m_U \;=\; s + \sum_{T \subseteq R} \gamma_U(T)\, \omega_T. \tag{3}$$

1. For every nonempty $U \subseteq L$, share m_U among the parties of U using additive secret sharing.

Disclosure side. Do the following over the parties of R:

1. Give a copy of $m_\varnothing$ to every party of R.
2. For every $T \subseteq R$, give ω_T to each party in $R \setminus T$.

Theorem 3.2 (The general linear scheme)**.** *For every finite field $\mathbb{F}$, every access structure F over $[n]$, and every partition $[n] = L \sqcup R$ into nonempty sets with $|L| = \ell$ and $|R| = q$, Construction 3.1 is a linear secret-sharing scheme over $\mathbb{F}$ for F, in which every party of L holds $2^{\ell-1}$ elements of $\mathbb{F}$ and every party of R holds $2^{q-1}+1$ elements of $\mathbb{F}$. Consequently, taking $q = \lceil n/2 \rceil$, every n-party access structure can be realized over every finite field $\mathbb{F}$ by a linear secret-sharing scheme with maximal share length $2^{\lceil n/2 \rceil - 1} + 1$ field elements. In particular, taking $\mathbb{F} = \mathbb{F}_2$ proves Theorem 1.1.*

Proof. We first notice that the scheme is linear over $\mathbb{F}$, as every distributed value is an $\mathbb{F}$-linear combination of the secret and the dealer's random field elements. For the share size, a party of L holds one field element for each of the $2^{\ell-1}$ nonempty sets $U \subseteq L$ containing it, and a party of R holds a copy of $m_\varnothing$, together with the field element ω_T for each of the 2^{q-1} sets $T \subseteq R$ not containing it. Thus, these shares contain respectively $2^{\ell-1}\log_2|\mathbb{F}|$ and $(2^{q-1}+1)\log_2|\mathbb{F}|$ bits. The "Consequently" clause follows since for $q = \lceil n/2 \rceil$ both $2^{\ell-1}$ and $2^{q-1}+1$ are at most $2^{\lceil n/2 \rceil - 1} + 1$. Specializing to $\mathbb{F}_2$ gives the binary share-size bound claimed in Theorem 1.1.

Correctness. Let B be authorized, and set $C = B \cap L$ and $D = B \cap R$. We first claim that the parties of B can compute m_C. If $C \neq \varnothing$, the parties of C hold all the additive shares of m_C and reconstruct it. If $C = \varnothing$, then $B = D$ is nonempty (as it is an authorized coalition), and each of its parties holds a copy of $m_\varnothing = m_C$.

Next, if D is empty, then $C = B$ is authorized. By monotonicity, $F(C \cup T) = 1$ for every $T \subseteq R$, so all the coefficients $\gamma_C(T)$ vanish and $m_C = s$. Otherwise, consider any $T \subseteq R$ with $\gamma_C(T) = 1$, i.e., $F(C \cup T) = 0$ by (2), so that ω_T masks the secret. It cannot hold that $D \subseteq T$, since monotonicity would then give $F(B) = F(C \cup D) \leq F(C \cup T) = 0$, contradicting that B is authorized. Hence, $D \nsubseteq T$, and a party in $D \setminus T \subseteq B$ has ω_T. Subtracting in $\mathbb{F}$ from m_C every masking pad ω_T yields s.

Privacy. Let B be unauthorized, and set $C = B \cap L$ and $D = B \cap R$. The general proof idea is to show that ω_D masks the secret in every visible linear combination in which the secret appears, and that ω_D is not released to the parties and is independent of all the other random elements. Lemma 3.3 below then shows that this suffices for privacy.

Formally, for every nonempty $U \nsubseteq C$, the parties of B hold only a strict subset of the additive shares of m_U. By the privacy of additive sharing, and the fact that these sharings are done with mutually independent fresh randomness, the joint view of all these incomplete sharings is distributed as $N\rho_1$ for some matrix N and a random vector ρ_1 that is independent of the secret, the pads, and the randomness used in all remaining shares.

Let ρ_2 collect all dealer randomness occurring in the remaining view of B, except for the pad ω_D. This pad is uniform and independent of (ρ_1, ρ_2), and it does not appear by itself in the view of B: disclosure-side item (2) gives ω_D only to parties in $R \setminus D$, whereas the disclosure-side parties of B are exactly those in D.

We claim that, in every linear combination in the remaining view, the coefficient of s equals the coefficient of ω_D. Consider first the complete additive sharing associated with a nonempty $U \subseteq C$. Since $U \cup D \subseteq B$, monotonicity and $F(B) = 0$ imply that $F(U \cup D) = 0$. Hence, $\gamma_U(D) = 1$ by (2), so m_U contains s and ω_D with the same coefficient. It follows that every additive share of m_U also has equal coefficients on s and ω_D: the fresh random shares have coefficient zero on both, while the remaining share has coefficient one on both. If $D \neq \varnothing$, the same argument with $U = \varnothing$ shows that every visible copy of $m_\varnothing$ has coefficient one on both s and ω_D. Finally, every individually disclosed pad other than ω_D has coefficient zero on both.

Therefore, for some vector a and matrix M, the entire view of B is distributed as

$$\mathsf{View}_B(s) \overset{\mathrm{d}}{=} \big(N\rho_1,\ a(s+\omega_D) + M\rho_2\big).$$

The conditions of Lemma 3.3 are satisfied, and hence the view of B is independent of the secret. This concludes the proof.

□

Lemma 3.3 (Common-pad privacy)**.** *Let Π be a linear share-distribution procedure over a finite field $\mathbb{F}$ for a scalar secret $s \in \mathbb{F}$, and fix a coalition B. Denote the joint view of B when the*

secret is s by $\mathsf{View}_B(s)$. Suppose that there exist a uniform random pad $\omega \in \mathbb{F}$, random vectors $\rho_1 \in \mathbb{F}^{r_1}$ and $\rho_2 \in \mathbb{F}^{r_2}$ such that ω is independent of the pair (ρ_1, ρ_2), matrices $N \in \mathbb{F}^{m_0 \times r_1}$ and $M \in \mathbb{F}^{m_1 \times r_2}$, and a vector $a \in \mathbb{F}^{m_1}$ such that, for every $s \in \mathbb{F}$,

$$\mathsf{View}_B(s) \stackrel{\mathrm{d}}{=} \big(N\rho_1,\ a(s+\omega) + M\rho_2\big).$$

Then the distribution of $\mathsf{View}_B(s)$ is independent of s.

Proof. Fix two secrets $s_0, s_1 \in \mathbb{F}$ and define $\omega' = \omega + s_0 - s_1$. Since translation by $s_0 - s_1$ is a bijection of $\mathbb{F}$, the variable ω' is uniform over $\mathbb{F}$. Moreover, because ω is independent of (ρ_1, ρ_2), the triple $(\omega', \rho_1, \rho_2)$ has the same distribution as (ω, ρ_1, ρ_2). Using the same values of ρ_1 and ρ_2, and the definition $\omega' = \omega + s_0 - s_1$, we have the pointwise identity

$$\begin{aligned}\big(N\rho_1,\ a(s_1+\omega') + M\rho_2\big) &= \big(N\rho_1,\ a(s_1+\omega+s_0-s_1) + M\rho_2\big)\\ &= \big(N\rho_1,\ a(s_0+\omega) + M\rho_2\big).\end{aligned}$$

The left-hand side has the distribution of $\mathsf{View}_B(s_1)$, and the right-hand side has the distribution of $\mathsf{View}_B(s_0)$. Hence these two views are identically distributed. Since s_0 and s_1 were arbitrary, the view of B is independent of the secret. □

4 A Linear Scheme for One Partitioned Upslice

In this section we show how to build secret-sharing schemes over any finite field for partitioned upslices. In Section 5, we will show how to combine such schemes with a suitable set of partitions in order to realize k-upslice functions, thus proving Theorem 1.2. Throughout this section, fix a finite field $\mathbb{F}$, integers $1 \le k \le n$, a partition $\Pi : [n] = L \sqcup R$ with $|R| = q$, and an integer t with $1 \le t \le \min(k, q)$ and $1 \le k - t \le n - q$. We call L the *masking side* and R the *disclosure side*. A *partitioned upslice* f_Π with profile $(k-t, t)$ is a k-upslice in which every minterm M satisfies

$$|M \cap L| = k - t, \qquad |M \cap R| = t.$$

Thus, for $U \in \binom{L}{k-t}$ and $V \in \binom{R}{t}$, we have $f_\Pi(U \cup V) = 1$ if and only if $U \cup V$ is a minterm of f_Π. A *trace* is a set $T \subseteq R$ with $|T| \ge t$. We let $\mathcal{T}$ denote the family of traces, and for every $U \in \binom{L}{k-t}$ and $T \in \mathcal{T}$ define the public coefficient $\gamma_U(T) \in \{0,1\} \in \mathbb{F}$ by

$$\gamma_U(T) = 1 \iff f_\Pi(U \cup V) = 0 \ \text{ for every } V \in \binom{T}{t}. \tag{4}$$

We next describe the scheme. Its correctness, privacy, and share size are established in Theorem 4.2.

Construction 4.1 (Linear secret sharing for a partitioned upslice)**.**

Let $s \in \mathbb{F}$ be the secret. The dealer samples independent uniform field elements η and $(\omega_T)_{T\in\mathcal{T}}$, and distributes the following shares over $\mathbb{F}$.

Masking side. For every $U \in \binom{L}{k-t}$, compute

$$m_U \;=\; s + \eta + \sum_{T\in\mathcal{T}} \gamma_U(T)\,\omega_T. \tag{5}$$

1. Share m_U among the parties of U using additive secret sharing.

Disclosure side. Do the following over the parties of R:

1. Share η using the $\mathbb{F}$-linear t-out-of-q Shamir threshold scheme of Definition A.4.
2. For every $T \in \mathcal{T}$, give ω_T to each party in $R \setminus T$.

Theorem 4.2 (A linear scheme for partitioned upslices)**.** *For every finite field $\mathbb{F}$, Construction 4.1 is a linear secret-sharing scheme over $\mathbb{F}$ realizing f_Π. Setting $m = \left\lceil \log_{|\mathbb{F}|}(q+1) \right\rceil$, its total share length is at most*

$$(k-t)\binom{n-q}{k-t} \;+\; qm + q\sum_{j=t}^{q}\binom{q}{j}$$

elements of $\mathbb{F}$, and hence its total share size in bits is at most this quantity times $\log_2|\mathbb{F}|$. In particular, for $\mathbb{F}=\mathbb{F}_2$ the total share size is at most

$$(k-t)\binom{n-q}{k-t} + q\lceil \log_2(q+1)\rceil + q\sum_{j=t}^{q}\binom{q}{j}.$$

Proof. The proof is very similar to that of Theorem 3.2. We first notice that the scheme is linear over $\mathbb{F}$, as every distributed value is an $\mathbb{F}$-linear combination of the secret and the dealer's randomness, and the threshold scheme of Definition A.4 is $\mathbb{F}$-linear. For the share length, a party in L holds one field element for each of the $\binom{n-q-1}{k-t-1}$ sets U containing it, for a total of $(n-q)\binom{n-q-1}{k-t-1} = (k-t)\binom{n-q}{k-t}$ field elements over all parties in L. The parties in R hold together qm field elements from the threshold scheme. In addition, every trace pad is given to at most q parties, and $|\mathcal{T}| = \sum_{j=t}^{q}\binom{q}{j}$. This proves the claimed field-element bound; multiplying by $\log_2|\mathbb{F}|$ gives the bit bound.

Correctness. Let B be authorized in f_Π. Hence, B contains some minterm M of f_Π. Let $U = M \cap L$ and $V = M \cap R$, so that $|V| = t$. The parties first reconstruct m_U from the additive shares of the masking side. Next, since $|V| = t$, the parties on the disclosure side can reconstruct η. For every trace T with $\gamma_U(T) = 1$ that masks the secret in m_U it cannot hold that $V \subseteq T$, since that would imply that $f_\Pi(U \cup V) = 0$ by (4). Hence, $V \nsubseteq T$, and some party in $V \setminus T$ receives ω_T by disclosure-side item (2). Subtracting in $\mathbb{F}$ the element η and every pad occurring in (5) from m_U yields s.

Privacy. Let B be unauthorized in f_Π, and denote $C = B \cap L$ and $D = B \cap R$. For every $U \in \binom{L}{k-t}$ with $U \nsubseteq C$, the parties of B hold only a strict subset of the additive shares of m_U. By the privacy of additive sharing (Definition A.5), the joint view of all these incomplete sharings can be treated as a part of the first, secret-independent block of Lemma 3.3. It remains to identify a common uniform field element that appears as a pad in every relevant additive sharing on the masking side, and to verify that this pad is independent of the rest of the view. This

pad will be η when $|D| < t$ and ω_D when $|D| \geq t$, and in both cases Lemma 3.3 will serve as the formal framework.

Case $|D| < t$. The privacy of the threshold scheme implies that the vector Z_D of threshold shares visible to D is independent of η. Since the threshold sharing is independent of all trace pads and additive-sharing randomness, we can include Z_D with the incomplete additive sharings in the first block of Lemma 3.3. Let ρ_1 represent this first block, and let ρ_2 consist of all the trace pads and the fresh randomness used in the complete additive sharings. Then, η is independent of (ρ_1, ρ_2). Outside the first block, the visible coordinates consist of complete additive shares and separately disclosed trace pads. In every complete additive sharing of $m_U = s + \eta + \sum_{T \in \mathcal{T}} \gamma_U(T)\omega_T$, each share consisting only of fresh randomness has coefficient zero on both s and η, while the remaining share has coefficient one on both. Every separately disclosed trace pad has coefficient zero on both. Thus, every coordinate outside the first block has equal coefficients on s and η. Therefore, for suitable matrices N, M and a vector a, the view of B can be represented as

$$\mathsf{View}_B(s) \stackrel{\mathrm{d}}{=} \big(N\rho_1,\ a(s+\eta) + M\rho_2\big).$$

Applying Lemma 3.3 with the pad η proves privacy in this case.

Case $|D| \geq t$. Take the pad ω_D (note that $D \in \mathcal{T}$ since $|D| \geq t$, so ω_D is defined). It is not released to B, since disclosure-side item (2) gives ω_D only to parties in $R \setminus D$. Moreover, ω_D is uniform and independent of all the remaining dealer randomness. Let (ρ_1, ρ_2) represent the incomplete additive sharings and all remaining randomness in the view of B, excluding ω_D.

Fix $U \in \binom{C}{k-t}$. For every $V \in \binom{D}{t}$, the set $U \cup V$ is contained in the unauthorized coalition B, so $f_\Pi(U \cup V) = 0$. Hence, $\gamma_U(D) = 1$ by (4). It follows that, in every coordinate of the complete additive sharing of m_U, the coefficient of s equals the coefficient of ω_D. Since ω_D is not disclosed separately, the entire view has a representation

$$\mathsf{View}_B(s) \stackrel{\mathrm{d}}{=} \big(N\rho_1,\ a(s+\omega_D) + M\rho_2\big)$$

for suitable matrices N, M and a vector a. Applying Lemma 3.3 with the pad ω_D proves privacy in this case and completes the proof. □

5 Linear Secret Sharing for One Upslice

Fix an arbitrary finite field $\mathbb{F}$. In this section we show how to decompose an upslice into partitioned upslices and realize it by a linear secret-sharing scheme over $\mathbb{F}$, thus proving Theorem 1.2. We describe the partition family in Section 5.1 and the decomposition in Section 5.2.

5.1 Window partitions

Lemma 5.1 (Cover by window partitions)**.** *Let $1 \leq k \leq n$ and $0 \leq q \leq n-1$, and set $t = \lceil kq/n \rceil$. Identify $[n]$ with $\mathbb{Z}_n$, and for every $i \in \mathbb{Z}_n$ let the i'th partition be defined by $R_i = \{i, i+1, \ldots, i+q-1\}$ (residues modulo n) and $L_i = [n] \setminus R_i$. Then, every $T \in \binom{[n]}{k}$ satisfies $|T \cap R_i| = t$ for at least one $i \in \mathbb{Z}_n$.*

Proof. Let $g(i) = |T \cap R_i|$. Since $R_{i+1} = (R_i \setminus \{i\}) \cup \{i+q\}$, consecutive values of $g(i)$ can differ by at most one: $g(i+1) - g(i) \in \{-1, 0, 1\}$. Each of the k elements of T belongs to exactly q of the n R_i windows, so $\sum_{i \in \mathbb{Z}_n} g(i) = kq$. Hence, the average of g over $\mathbb{Z}_n$ is

kq/n. As $\min_i g(i)$ and $\max_i g(i)$ are integers bounding this average from below and above, $\min_i g(i) \le \lfloor kq/n \rfloor \le t \le \max_i g(i)$. Since g is integer-valued and changes by at most one along the cycle, it attains every integer between its minimum and its maximum. In particular, it holds that $g(i) = t$ for some i. □

We note that the number of partitions is n, and that they can be computed explicitly and deterministically.

5.2 The upslice theorem

We now show how to realize (k, n)-upslices, proving Theorem 1.2 and the following Theorem 5.2. In most cases we will use the construction for partitioned-upslices of Section 4, and in two edge cases a formula-based scheme of Benaloh and Leichter [16]. Their construction is linear over every finite field and has total share length at most the formula size, which for k-upslices is at most $k\binom{n}{k}$ by the monotone DNF representation.

Theorem 5.2 (Layerwise upslice theorem)**.** *For every finite field $\mathbb{F}$ and integers n, $1 \le k \le n$, and $0 \le q \le n-1$, set $t = \lceil kq/n \rceil$. Then, every (k, n)-upslice can be realized by a linear secret-sharing scheme over $\mathbb{F}$ with total share length at most*

$$\left[\binom{n-q}{k-t} + \sum_{j=t}^{q} \binom{q}{j} \right] \cdot O(n^2 \log n). \tag{6}$$

Proof. Let f_k be a (k, n)-upslice. If $q = 0$, then $t = 0$ and the first term of (6) is $\binom{n}{k}$. The monotone DNF representing f_k has one term of size k for each minterm, and hence size at most $k\binom{n}{k}$. The DNF-based scheme of [16] is therefore within the claimed bound. Assume from now on $q \ge 1$, so that $t = \lceil kq/n \rceil \ge 1$. We also note that $t \le q$ always holds, and that

$$k - t \;\le\; k - \frac{kq}{n} \;=\; \frac{k(n-q)}{n} \;\le\; n - q.$$

Let $\Pi_0, \ldots, \Pi_{n-1}$ be the window partitions promised by Lemma 5.1. For each i, let f_{Π_i} be the partitioned upslice whose minterms are the minterms M of f_k satisfying $|M \cap R_i| = t$. By Lemma 5.1, every minterm of f_k is a minterm of at least one f_{Π_i}, while every minterm of each f_{Π_i} is a minterm of f_k. Hence, the two sides below have the same minterms, and therefore they define the same monotone function:

$$f_k \;=\; \bigvee_{i \in \mathbb{Z}_n} f_{\Pi_i}.$$

Hence, by the closure of linear secret sharing over $\mathbb{F}$ under OR gates, it suffices to realize f_{Π_i} by sharing the same secret independently according to each partitioned upslice:

If $k - t \ge 1$: use Construction 4.1 over $\mathbb{F}$ for the partition Π_i. By Theorem 4.2, setting $m = \lceil \log_{|\mathbb{F}|}(q+1) \rceil$, its total share length is at most

$$(k-t)\binom{n-q}{k-t} + qm + q\Big(\sum_{j=t}^{q} \binom{q}{j}\Big) = \left[\binom{n-q}{k-t} + \sum_{j=t}^{q} \binom{q}{j} \right] \cdot O(n \log n),$$

where the equality holds since q and $k - t$ are smaller than n and $m = O(\log n)$ for every finite field $\mathbb{F}$. *If $k - t = 0$:* every minterm of f_{Π_i} is a k-subset of R_i, so f_{Π_i} is an upslice over the q

parties of R_i. Its monotone DNF has size at most $k\binom{q}{k} = t\binom{q}{k} \le q\binom{q}{t} \le q\sum_{j=t}^{q}\binom{q}{j}$, and the DNF scheme of [16] achieves this bound.

In either case the total share length of f_{Π_i} is at most $[\binom{n-q}{k-t} + \sum_{j=t}^{q}\binom{q}{j}]\cdot O(n\log n)$. Summing over the n partitions of Lemma 5.1 gives (6) for the total share length. □

6 Technical Lemmas

6.1 Binomial estimates

To evaluate the combinatorial bound of Theorem 1.2 at constant densities, we will use the final claim of this subsection, which in turn relies on the preceding claims.

We first note that changing either argument of a binomial coefficient by one changes the coefficient by at most a polynomial factor. We will use this fact repeatedly to absorb the $O(1)$-rounding required when converting densities to integers.

Fact 6.1 (Unit shifts)**.** *For all integers $0 \le r \le m$, each of the ratios $\binom{m}{r\pm1}/\binom{m}{r}$ and $\binom{m\pm1}{r}/\binom{m}{r}$ that is defined and nonzero equals one of*

$$\frac{m-r}{r+1}, \qquad \frac{r}{m-r+1}, \qquad \frac{m+1}{m+1-r}, \qquad \frac{m-r}{m},$$

and lies in $[\,1/(m{+}1),\, m{+}1\,]$. Hence, changing either argument by one changes $\log\binom{m}{r}$ by at most $\log(m{+}1)$.

Together with a comparison to the binomial distribution, Fact 6.1 yields the following estimate for binomial coefficients when the normalized index j/m differs from a fixed density by $O(1/m)$.

Claim 6.2 (Binomial coefficients near a fixed density)**.** *Let $\beta \in (0,1)$ and $c > 0$ be constants. There exists a constant $C > 0$, depending only on β and c, such that for all integers $m \ge 1$ and $0 \le j \le m$ with $|j - \beta m| \le c$,*

$$\left|\log\binom{m}{j} - H_2(\beta)\, m\right| \le C\log(m+1).$$

Proof. Consider the $m+1$ nonnegative numbers

$$p_i = \binom{m}{i}\beta^i(1-\beta)^{m-i}, \qquad 0 \le i \le m,$$

which sum to one by the binomial theorem. Taking logarithms and rearranging we get for every i that

$$\log\binom{m}{i} = \log p_i + H_2(\beta)\, m + (i-\beta m)\log\tfrac{1-\beta}{\beta}. \tag{7}$$

For $i = j$ the last term has absolute value at most $c\left|\log\frac{1-\beta}{\beta}\right|$. Since $p_j \le 1$, (7) therefore bounds $\log\binom{m}{j} - H_2(\beta)m$ from above by a constant depending only on β and c. For the lower bound, the ratio $p_{i+1}/p_i = \frac{m-i}{i+1}\cdot\frac{\beta}{1-\beta}$ is at least one precisely when $i \le \beta(m+1)-1$, so the sequence $(p_i)_i$ increases up to some index $i^* = \beta m + O(1)$ and decreases afterwards. As the $m+1$ numbers sum to one, $p_{i^*} \ge 1/(m+1)$, and (7) with $i = i^*$ gives

$$\log\binom{m}{i^*} - H_2(\beta)m \ge -\log(m+1) - O(1).$$

Since both j and i^* are a constant away from βm it holds that $|j - i^*| = O(1)$. Applying Fact 6.1 $O(1)$ times yields

$$\log \binom{m}{j} - H_2(\beta)m \geq -O(\log(m+1)).$$

Combining the two bounds and choosing a sufficiently large constant C proves the claim. □

Combining the estimates above yields the asymptotic evaluation at linear densities of the combinatorial bound of Theorem 1.2. Recall that $\kappa(\rho) = 1$ for $\rho \in (0, 1/2)$ and $\kappa(\rho) = H_2(\rho)$ for $\rho \in [1/2, 1)$ (note that the two branches agree at $\rho = 1/2$). We now prove the asymptotic estimate needed above.

Claim 6.3 (Evaluation of the layer bound)**.** *Fix constants $\alpha, \lambda \in (0,1)$, and for every n set $k = \lceil \alpha n \rceil$, $q = \lceil \lambda n \rceil$, and $t = \lceil kq/n \rceil$. Then*

$$\binom{n-q}{k-t} + \sum_{j=t}^{q} \binom{q}{j} \;=\; 2^{\max\{(1-\lambda)H_2(\alpha),\ \lambda\kappa(\alpha)\}\, n + o(n)}.$$

Proof. Throughout the proof, the constants hidden in the O-notation may depend on α and λ, and n is assumed to be sufficiently large. Since $k = \alpha n + O(1)$ and $q = \lambda n + O(1)$, we have $t = \lceil kq/n \rceil = \alpha\lambda n + O(1)$, and therefore

$$n - q = (1-\lambda)n + O(1), \qquad k - t = \alpha(n-q) + O(1), \qquad t = \alpha q + O(1).$$

The first term. By Claim 6.2, applied with $\beta = \alpha$,

$$\log \binom{n-q}{k-t} = H_2(\alpha)\,(n-q) + O(\log n) = (1-\lambda)\,H_2(\alpha)\,n + O(\log n).$$

The second term. Let $s = \max(t, \lceil q/2 \rceil)$. Then it holds that $s = \max(\alpha, \frac{1}{2})\,q + O(1)$, and by the definition above, $\kappa(\alpha) = H_2(\max(\alpha, \frac{1}{2}))$. Since $\binom{q}{s}$ is the largest binomial coefficient among $\binom{q}{t}, \ldots, \binom{q}{q}$, we have $\binom{q}{s} \leq \sum_{j=t}^{q} \binom{q}{j} \leq (q+1)\binom{q}{s}$. Consequently,

$$\log \sum_{j=t}^{q} \binom{q}{j} = \log \binom{q}{s} + O(\log q) = H_2\big(\max(\alpha, \tfrac{1}{2})\big)\, q + O(\log q) = \kappa(\alpha)\,\lambda\, n + O(\log n),$$

where the middle equality is Claim 6.2 with $\beta = \max(\alpha, \frac{1}{2})$.

Finally, the sum is within a factor of two of its larger term. Therefore, its exponent is the maximum of the two exponents, while the $O(\log n)$ error terms are absorbed into the $o(n)$ term. □

6.2 Quadratic Midslice Schemes

Proof of Theorem 1.9. We plug the quadratic RCDS protocol of Beimel, Othman, and Peter [15, Thm. 6.5] into the RCDS-to-midslice construction of Applebaum et al. [3, Lemmas 5.5 and 5.8]. We use the parameters from the proof of [3, Lem. 5.10], which performs the same procedure as we do here with their RCDS protocols.

Up to adding $o(n)$ dummy parties and rounding the parameters (which changes the share size by only a $2^{o(n)}$ factor), assume that $n = K\ell$ with $K = \ell = \sqrt{n}$. Set $\varepsilon = n^{-0.1}$ and

$$a = \left(\frac{1}{2} - \delta - \varepsilon\right)\ell, \qquad b = \left(\frac{1}{2} + \delta + \varepsilon\right)\ell.$$

The RCDS input domain of each server has size $N = 2^\ell$, and the robustness required by the compiler is

$$T = \sum_{j=a}^{b} \binom{b}{j}.$$

If the RCDS messages have length m, Lemmas 5.5 and 5.8 of [3] give a δ-midslice scheme of total share size $m\,2^{o(n)}$.

Theorem 6.5 of [15] gives a quadratic K-server T-RCDS protocol over $\mathbb{F}_2$ for Ts that satisfy $T < \min\{N/2K, 2^{\sqrt{N}/K}\}$ with

$$m = O\Big(N^{(K-1)/3} T^{\,2(K-1)/3+1} K^{2K} \log^2 N \log^{(4K-1)/3} T\Big)$$

The requirement for T is satisfied for all sufficiently large n: indeed, $T \le 2^b = N^{1/2+\delta+o(1)} = o(N/K)$ since $\delta < 1/2$, and $\log T = O(\ell) = o(\sqrt{N}/K)$.

We next compute the midslice share size, beginning with an estimate of T. The usual entropy bound for binomial sums yields

$$\log T = \tau(\delta)\ell + o(\ell), \qquad \tau(\delta) = \begin{cases} \left(\frac{1}{2}+\delta\right) H_2\left(\frac{1/2-\delta}{1/2+\delta}\right), & 0 \le \delta \le \frac{1}{6}, \\ \frac{1}{2} + \delta, & \frac{1}{6} \le \delta < \frac{1}{2}. \end{cases}$$

For the second range, the interval $[a, b]$ contains the middle binomial coefficient and the exponent is b, and for the first range the exponent is dominated by the expression $\binom{b}{a}$ with $a \ge b/2$.

Taking logarithms in the RCDS bound yields

$$\begin{aligned} \log m &\le \frac{K-1}{3}\ell + \left(\frac{2(K-1)}{3} + 1\right)\big(\tau(\delta)\ell + o(\ell)\big) + o(n) \\ &= \left(\frac{1}{3} + \frac{2}{3}\tau(\delta)\right) n + o(n), \end{aligned}$$

where the equality is implied by $K\ell = n$, and by the fact that the factors K^{2K} and the logarithmic factors contribute only $O(\sqrt{n}\log n) = o(n)$. Substituting the two values of $\tau(\delta)$ gives

$$\frac{1}{3} + \frac{2}{3}\tau(\delta) = \begin{cases} \frac{1}{3} + \frac{1+2\delta}{3} H_2\left(\frac{1-2\delta}{1+2\delta}\right), & 0 \le \delta \le \frac{1}{6}, \\ \frac{2}{3} + \frac{2\delta}{3}, & \frac{1}{6} \le \delta < \frac{1}{2}, \end{cases}$$

which is $\mathsf{Q}(\delta)$.

Finally, the RCDS protocol of [15, Thm. 6.5] has quadratic sharing and reconstruction. The compiler of [3, Lemmas 5.5 and 5.8] distributes and recovers these messages using linear secret-sharing schemes. Composing these linear maps with the quadratic RCDS maps preserves the degree to be at most two, so the resulting midslice scheme has quadratic sharing and reconstruction. Its total share size is $m\,2^{o(n)} = 2^{\mathsf{Q}(\delta)n + o(n)}$, as claimed. □

Acknowledgments

We thank Amos Beimel for useful comments. This work was supported by ISF grant 1614/25.

References

[1] Bar Alon, Amos Beimel, and Or Lasri. Simplified PIR and CDS protocols and improved linear secret-sharing schemes. In Benny Applebaum and Huijia (Rachel) Lin, editors, *Theory of Cryptography - 23rd International Conference, TCC 2025, Aarhus, Denmark, December 1-5, 2025, Proceedings, Part II*, volume 16269 of *Lecture Notes in Computer Science*, pages 365–398. Springer, 2025.

[2] 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, Part III*, volume 11478 of *Lecture Notes in Computer Science*, pages 441–471. Springer, 2019.

[3] 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, *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, STOC 2020*, pages 280–293. ACM, 2020.

[4] Benny Applebaum, Amos Beimel, Oded Nir, Naty Peter, and Toniann Pitassi. Secret sharing, slice formulas, and monotone real circuits. *ACM Transactions on Computation Theory*, 18(2):1–32, 2026.

[5] Benny Applebaum and Oded Nir. Upslices, downslices, and secret-sharing with complexity of 1.5^n. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Part III*, volume 12827 of *Lecture Notes in Computer Science*, pages 627–655. Springer, 2021.

[6] Nuttapong Attrapadung. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*, pages 557–577. Springer, 2014.

[7] László Babai, Anna Gál, and Avi Wigderson. Superpolynomial lower bounds for monotone span programs. *Comb.*, 19(3):301–319, 1999.

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

[9] Amos Beimel. Secret-sharing schemes: A survey. In Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing, editors, *Coding and Cryptology - Third International Workshop, IWCC 2011*, volume 6639 of *Lecture Notes in Computer Science*, pages 11–46. Springer, 2011.

[10] Amos Beimel. Secret-sharing schemes for general access structures: An introduction. *IACR Cryptol. ePrint Arch.*, 2025:518, 2025.

[11] 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*, volume 12552 of *Lecture Notes in Computer Science*, pages 499–529. Springer, 2020.

[12] Amos Beimel, Oriol Farràs, and Or Lasri. Improved polynomial secret-sharing schemes. In Guy N. Rothblum and Hoeteck Wee, editors, *Theory of Cryptography - 21st International Conference, TCC 2023, Taipei, Taiwan, November 29 - December 2, 2023, Proceedings, Part II*, volume 14370 of *Lecture Notes in Computer Science*, pages 374–405. Springer, 2023.

[13] Amos Beimel, Oriol Farràs, Or Lasri, and Oded Nir. Secret-sharing schemes for high slices. In Elette Boyle and Mohammad Mahmoody, editors, *Theory of Cryptography - 22nd International Conference, TCC 2024, Milan, Italy, December 2-6, 2024, Proceedings, Part IV*, volume 15367 of *Lecture Notes in Computer Science*, pages 581–613. Springer, 2024.

[14] 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.

[15] Amos Beimel, Hussien Othman, and Naty Peter. Quadratic secret sharing and conditional disclosure of secrets. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Part III*, volume 12827 of *Lecture Notes in Computer Science*, pages 748–778. Springer, 2021.

[16] Josh Cohen Benaloh and Jerry Leichter. Generalized secret sharing and monotone functions. In Shafi Goldwasser, editor, *Advances in Cryptology – CRYPTO '88, 8th Annual International Cryptology Conference*, volume 403 of *Lecture Notes in Computer Science*, pages 27–35. Springer, 1988.

[17] George R. Blakley. Safeguarding cryptographic keys. In Richard E. Merwin, Jacqueline T. Zanca, and Merlin Smith, editors, *Proceedings of the 1979 AFIPS National Computer Conference*, volume 48 of *AFIPS Conference proceedings*, pages 313–317. AFIPS Press, 1979.

[18] Ronald Cramer, Ivan Damgård, and Ueli M. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*, pages 316–334. Springer, 2000.

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

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

[21] Romain Gay, Iordanis Kerenidis, and Hoeteck Wee. Communication complexity of conditional disclosure of secrets and attribute-based encryption. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 485–502. Springer, 2015.

[22] Yael Gertner, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. Protecting data privacy in private information retrieval schemes. *J. Comput. Syst. Sci.*, 60(3):592–629, 2000.

[23] Charles H Goldberg and Douglas B West. Bisection of circle colorings. *SIAM Journal on Algebraic Discrete Methods*, 6(1):93–106, 1985.

[24] Mitsuru Ito, Akira Saito, and Takao 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. Cryptol.*, 6(1):15-20, 1993.

[25] Mauricio Karchmer and Avi Wigderson. On span programs. In *Proceedings of the Eighth Annual Structure in Complexity Theory Conference, San Diego, CA, USA, May 18-21, 1993*, pages 102–111. IEEE Computer Society, 1993.

[26] 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*, pages 699–708. ACM, 2018.

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

[28] Hoeteck Wee. Dual system encryption via predicate encodings. In Yehuda Lindell, editor, *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings*, volume 8349 of *Lecture Notes in Computer Science*, pages 616–637. Springer, 2014.

A Omitted Preliminaries

A.1 Secret-sharing schemes

We define a secret-sharing scheme similarly to the definitions given in [13]. For more information about this definition and secret-sharing in general, see [9]. We start by defining an access structure, which is the collection of sets of parties that are authorized to reconstruct the secret. We describe an access structure by a monotone Boolean function.

Definition A.1 (Access Structures)**.** An n-party access structure is a monotone function $f : \{0,1\}^n \to \{0,1\}$ such that $f(0^n) = 0$. Let $P = \{P_1, \ldots, P_n\}$ be a set of parties. For an input $x = (x_1, \ldots, x_n) \in \{0,1\}^n$, we define the set of parties that it represents as $I_x = \{P_i : x_i = 1\}$. For every $x \in \{0,1\}^n$, if $f(x) = 1$, then we say that I_x is authorized; if $f(x) = 0$, then we say that I_x is unauthorized.

Definition A.2 (Secret-Sharing Schemes)**.** A *secret-sharing scheme* Π with domain of secrets S, such that $|S| \geq 2$, is a mapping from $S \times R$, where R is some finite set called the set of random strings, to a tuple of n-sets $S_1 \times S_2 \times \cdots \times S_n$, where S_j is called the *domain of shares* of P_j.

For an input $x \in \{0,1\}^n$, we denote $\Pi_x(s;r)$ as the restriction of $\Pi(s;r)$ to its I_x-entries, i.e., $(\mathsf{sh}_j)_{j:x_j=1}$.

A secret-sharing scheme Π with domain of secrets S realizes an access structure $f : \{0,1\}^n \to \{0,1\}$ if the following two requirements hold:

Correctness. For any input $x \in \{0,1\}^n$ such that $f(x) = 1$ there exists a *reconstruction function* $\mathrm{Recon}_x : \prod_{\{i:x_i=1\}} S_i \to S$ such that $\mathrm{Recon}_x(\Pi_x(s;r)) = s$ for every secret $s \in S$ and every random string $r \in R$.

Privacy. For any input $x \in \{0,1\}^n$ such that $f(x) = 0$ and every pair of secrets $s, s' \in S$, the distributions $\Pi_x(s;r)$ and $\Pi_x(s';r)$ are identical, where the distributions are over the choice of r from R with uniform distribution.

Given a secret-sharing scheme Π, define the *size* of the secret as $\log|S|$, the *share size* of party P_j as $\log|S_j|$, the *share size* as $\max_{1\le j\le n}\{\log|S_j|\}$, the *total share size* as $\sum_{j=1}^{n}\log|S_j|$, and the *information ratio* as $\frac{\max_{1\le j\le n}\{\log|S_j|\}}{\log|S|}$.

By default, when we talk about the share size of secret-sharing schemes for an access structure, we consider schemes for one-bit secrets.

We next define linear secret-sharing schemes, which are schemes in which the mapping that the dealer uses to generate the shares is linear.

Definition A.3 (Linear Secret-Sharing Schemes)**.** Let Π be a secret-sharing scheme with domain of secrets S. We say that Π is a *linear* secret-sharing scheme over a finite field $\mathbb{F}$ if there are integers $\ell_r, \ell_1, \ldots, \ell_n$ such that $S = \mathbb{F}$, $R = \mathbb{F}^{\ell_r}$, $S_1 = \mathbb{F}^{\ell_1}, \ldots, S_n = \mathbb{F}^{\ell_n}$, and the mapping Π is a *linear* mapping over $\mathbb{F}$ from $\mathbb{F}^{1+\ell_r}$ to $\mathbb{F}^{\ell_1+\cdots+\ell_n}$. The *share length* of party P_i is ℓ_i, the *maximal share length* of the scheme is $\max_{i\in[n]}\ell_i$, and its *total share length* is $\sum_{i=1}^{n}\ell_i$. These quantities count elements of $\mathbb{F}$.

Definition A.4 (Shamir threshold secret sharing [27])**.** Let $1 \le t \le q$, let $P_1, \ldots, P_q$ be parties, and let $\mathbb{F}$ be a finite field with $|\mathbb{F}| > q$. Shamir's construction gives a linear secret-sharing scheme over $\mathbb{F}$ for the t-out-of-q threshold access structure, with one element of $\mathbb{F}$ per share.

For an arbitrary finite field $\mathbb{F}$, let $m = \left\lceil \log_{|\mathbb{F}|}(q+1) \right\rceil$ and run Shamir's construction over the degree-m extension field $\mathbb{K}$ of $\mathbb{F}$, which has $|\mathbb{K}| = |\mathbb{F}|^m > q$. Restricting the secret to the subfield $\mathbb{F} \subseteq K$ preserves correctness and privacy, and the $\mathbb{K}$-linear sharing map is also $\mathbb{F}$-linear. Since one element of $\mathbb{K}$ is represented by m elements of $\mathbb{F}$, this gives a linear t-out-of-q threshold scheme over $\mathbb{F}$ with share length m field elements per party. In particular, for $\mathbb{F} = \mathbb{F}_2$ the share size is $\lceil \log_2(q+1) \rceil$ bits per party.

Definition A.5 (Additive secret sharing)**.** Let $U = \{P_1, \ldots, P_q\}$ be parties, and let $a \in \mathbb{F}$. To share a additively among the parties of U, the dealer samples independent uniform elements $r_1, \ldots, r_{q-1} \in \mathbb{F}$, gives r_j to party P_j for every $j < q$, and gives

$$a - \sum_{j=1}^{q-1} r_j$$

to party P_q. The parties in U can reconstruct a by summing their shares, while the shares held by every strict subset of U are independent uniform elements of $\mathbb{F}$, independently of a. Hence, additive secret sharing is a linear scheme for the q-out-of-q access structure.

Definition A.6 (Closure under OR and AND)**.** Let $f_1, \ldots, f_m$ be monotone functions over the same parties, each realized by a secret-sharing scheme. Then both $\bigvee_{i=1}^{m} f_i$ and $\bigwedge_{i=1}^{m} f_i$ can be realized by secret-sharing schemes whose total and maximal share sizes are at most the sums of the corresponding share sizes of the original schemes. If the original schemes are linear over the same field, then the resulting schemes are linear as well.

Complexity conventions [5]. 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 is $n^{-1} \cdot \log_2 \mathsf{SSize}(f)$, and it is denoted by $\mathbf{S}(f)$. 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 $\mathbf{S}(\mathcal{F}) := \limsup_{n\to\infty} \mathbf{S}(\mathcal{F}_n)$. For an access structure F, let $\mathsf{LSSize}(F)$ denote the minimum total share size of a linear scheme realizing F. All the above definitions extend to the linear setting by replacing SSize with LSSize.

We denote by $\mathbf{D}(b,n)$ (resp., $\mathbf{D}_\ell(b,n)$) the secret-sharing exponent (resp., the linear exponent) of (b,n)-downslices and by $\mathbf{D}(\beta)$ (resp., $\mathbf{D}_\ell(\beta)$) the secret-sharing exponent (resp., the linear 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 linear exponents of (a,n)-upslices and $(\alpha n, n)$-upslices. Unless stated otherwise, exponents are defined for schemes with a one-bit secret.

A.2 Function families

We define slices, multislices, midslices, upslices and downslices, as defined in [5].

Definition A.7 (Slices, Multislices and δ-Midslices)**.** For $a \le b \in [n]$, 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 referred to as an a-*slice*.

For a constant $\delta \in (0,1/2)$, the δ-*midslice* of an n-party access structure f is its $(a:b)$-multislice with $a = \left\lceil \left(\frac{1}{2} - \delta\right) n \right\rceil, b = \left\lfloor \left(\frac{1}{2} + \delta\right) n \right\rfloor$. We call an access structure obtained this way a δ-*midslice access structure*.

Definition A.8 (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

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

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 minterms are at level a.

Definition A.9 (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-downslice of some n-party access structure f.

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

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il