Breaking the Circuit-Size Barrier in Secret Sharing

Tianren Liu
MIT[*]

Vinod Vaikuntanathan
MIT[†]

April 4, 2018

Abstract

We study secret sharing schemes for general (non-threshold) access structures. A general secret sharing scheme for n parties is associated to a monotone function $\mathsf{F} : \{0,1\}^n \to \{0,1\}$. In such a scheme, a dealer distributes shares of a secret s among n parties. Any subset of parties $T \subseteq [n]$ should be able to put together their shares and reconstruct the secret s if $\mathsf{F}(T) = 1$, and should have no information about s if $\mathsf{F}(T) = 0$. One of the major long-standing questions in information-theoretic cryptography is to minimize the (total) size of the shares in a secret-sharing scheme for arbitrary monotone functions F.

There is a large gap between lower and upper bounds for secret sharing. The best known scheme for general F has shares of size $2^{n-o(n)}$, but the best lower bound is $\Omega(n^2/\log n)$. Indeed, the exponential share size is a direct result of the fact that in all known secret-sharing schemes, the share size grows with the size of a circuit (or formula, or monotone span program) for F. Indeed, several researchers have suggested the existence of a *representation size barrier* which implies that the right answer is closer to the upper bound, namely, $2^{n-o(n)}$.

In this work, we overcome this barrier by constructing a secret sharing scheme for any access structure with shares of size $2^{0.994n}$ and a linear secret sharing scheme for any access structure with shares of size $2^{0.999n}$. As a contribution of independent interest, we also construct a secret sharing scheme with shares of size $2^{\tilde{O}(\sqrt{n})}$ for $2^{\binom{n}{n/2}}$ monotone access structures, out of a total of $2^{\binom{n}{n/2}\cdot(1+O(\log n/n))}$ of them. Our construction builds on recent works that construct better protocols for the conditional disclosure of secrets (CDS) problem.

[*] `liutr@mit.edu`. Research supported in part by NSF Grants CNS-1350619 and CNS-1414119.

[†] `vinodv@csail.mit.edu`. Research supported in part by NSF Grants CNS-1350619 and CNS-1414119, Alfred P. Sloan Research Fellowship, Microsoft Faculty Fellowship, the NEC Corporation, a Steven and Renee Finn Career Development Chair from MIT. This work was also sponsored in part by the Defense Advanced Research Projects Agency (DARPA) and the U.S. Army Research Office under contracts W911NF-15-C-0226 and W911NF-15-C-0236.

1 Introduction

Secret sharing [Sha79, Bla79] is a powerful cryptographic technique that allows a dealer to distribute shares of a secret to n parties such that certain authorized subsets of parties, and only they, can recover the secret. The original definition of secret sharing is what we now call a (n, t)-threshold secret sharing scheme, where any set of t or more parties can recover the secret, and no subset of fewer than t parties can learn any information about the secret whatsoever.

Later on, this was generalized in [ISN89] to the notion of a secret-sharing scheme realizing a monotone function $\mathsf{F} : \{0,1\}^n \to \{0,1\}$. This is simply a randomized algorithm that on input a secret s, outputs n shares $s_1, \ldots, s_n$ such that for any $(x_1, \ldots, x_n) \in \{0,1\}^n$, the collection of shares $\{s_i : x_i = 1\}$ determine the secret if $\mathsf{F}(x_1, \ldots, x_n) = 1$ and reveal nothing about the secret otherwise.[1] It is easy to see that (n, t)-threshold secret sharing corresponds to the special case where F is the (monotone) threshold function that outputs 1 if and only if at least t of the n input bits are 1.

While the landscape of threshold secret sharing is relatively well-understood, even very basic information-theoretic questions about the more general notion of secret sharing remain embarrassingly open. It is simple to construct a secret sharing scheme realizing any monotone function $\mathsf{F} : \{0,1\}^n \to \{0,1\}$ where each share is at most 2^n bits; the share size can be improved to $O(2^n/\sqrt{n})$ bits [BL88]. We also know that there is an (explicit) monotone function $\mathsf{F} : \{0,1\}^n \to \{0,1\}$ that requires a total share size of $\Omega(n^2/\log n)$ bits [Csi97], a far cry from the upper bound. No better lower bounds are known, even in a non-explicit sense (except for the restricted class of linear secret-sharing schemes).

The Representation Barrier. Closing the exponential gap between the afore-mentioned upper bounds and lower bounds is a long-standing open problem in cryptography. The general consensus appears to be that the upper bound is almost tight; see, e.g., [Bei11]. The main reason for this pessimism appears to be the fact that all known constructions of secret sharing schemes for classes of access structures use a representation of the corresponding monotone function F in a concrete computational model, be it (monotone) circuits, formulas, branching programs or span programs [ISN89, KW93]. As a result, the share size in these schemes *grows with the size of the representation* which, for general monotone functions, is $2^{\Omega(n)}$ in all these computational models (and, for circuits and formulas, even $2^{n-o(n)}$).[2]

Very recently, a work by [LVW17b] achieved sub-exponential $2^{O(\sqrt{n}\log n)}$ share size for a large number of monotone functions, namely $2^{2^{n/2}}$ out of a total of $2^{\binom{n}{n/2}\cdot(1+O(\log n/n))} \approx 2^{2^{n-O(\log n)}}$ of them (where n is the number of parties) [KM75]. Still, the question of whether one can construct secret sharing schemes *supporting all monotone functions* F with share size $2^{(1-\epsilon)n}$ for some constant $\epsilon > 0$ remained wide open. In this work, we resolve this open question.

Theorem 1.1 (Informal)**.** *For every monotone access structure (function), there is a secret sharing scheme with total share size* $2^{0.994n}$.

[1] The typical formulation of secret-sharing refers to a dealer that holds a secret distributing shares to n parties, such that only certain subsets of parties –described by a so-called access structure– can reconstruct the secret. In our formulation, the randomized algorithm corresponds to the dealer, s_i corresponds to the share given to party i, $x_i \in \{0,1\}$ indicates whether party i is present in a subset, and F corresponds to the access structure.

[2] We remark that this state of affairs appears to be true even for the relaxed notion of computationally secure secret sharing schemes.

We remark that the constant in the exponent comes from a delicate balancing argument; we have not made an attempt to optimize it.

1.1 An Overview of Our Techniques

Conditional Disclosure of Secrets and Its Connection to Secret Sharing. Our starting point is the results of [LVW17a, LVW17b] who view the problem of secret sharing through the lens of the conditional disclosure of secrets (CDS) problem introduced by Gertner, Ishai, Kushilevitz and Malkin [GIKM00]. In the multiparty version of CDS associated to a (not necessarily monotone) predicate $\mathsf{F} : \{0,1\}^n \to \{0,1\}$, there are $n+1$ parties, the first n of who each hold an input bit x_i and all of them have a secret bit s; the last party called a referee knows the entire input $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ but does not know s. In addition, the first n parties have access to a common random string that is unknown to the referee. The goal is for the first n parties to each send a single message to the referee such that: (a) the referee can recover s if $\mathsf{F}(x_1, \ldots, x_n) = 1$; and (b) the referee has no information about s otherwise.

CDS looks superficially similar to secret sharing and indeed, it does give us a secret sharing scheme for a limited class of access structures introduced by Beimel and Ishai [BI01] that we will refer to as *paired-up access structures*. The collection of authorized sets in a paired-up access structure corresponding to a (not necessarily monotone) predicate F have one of the following two forms. Think of the n parties as split up into pairs $(P_{1,0}, P_{1,1}), \ldots, (P_{n/2,0}, P_{n/2,1})$. (For this discussion, assume that n is even.)

(a) any subset that contains both $P_{i,0}$ and $P_{i,1}$ is authorized; and

(b) any subset that contains a set $\{P_{1,x_1}, P_{2,x_2}, \ldots, P_{n/2,x_{n/2}}\}$ where $\mathsf{F}(x_1, x_2, \ldots, x_{n/2}) = 1$ is authorized as well.

Constructing a secret sharing scheme for a paired-up access structure using CDS is simple: the dealer takes the secret bit s and computes all possible messages in a CDS protocol for the function F. That is, the two messages $m_{i,0}$ and $m_{i,1}$ that each CDS party P_i computes given input bits $x_i = 0$ and $x_i = 1$ respectively. Now, give $m_{i,b}$ as the share for the party $P_{i,b}$ in the secret sharing scheme. Additionally, the dealer additively shares s between every pair of parties $P_{i,0}$ and $P_{i,1}$. It is not hard to see that this is indeed a secret sharing scheme for the access structure described above.

There are a total of roughly $2^{2^{n/2}}$ paired-up access structures, out of the total possible $2^{2^{n-O(\log n)}}$ monotone access structures. [LVW17b] constructed a CDS protocol with communication complexity $2^{\tilde{O}(\sqrt{n})}$ for all functions F which immediately translates to a secret sharing scheme with share size $2^{\tilde{O}(\sqrt{n})}$ for all paired-up access structures. However, the fact remains that paired-up access structures are but a really tiny fraction of all monotone access structures.

Looking ahead, we remark that a major limitation in translating CDS, a *non-monotone notion*, into secret-sharing, a *monotone notion*, is that in a CDS scheme, the referee can reconstruct the secret only if he receives messages from *all* the parties. On the other hand, if he catches hold of *both* the possible messages $m_{i,0}$ and $m_{i,1}$ of any one party, the CDS privacy guarantee is null and void. This will turn out to be the major impediment in converting a CDS scheme into a secret sharing scheme, one that we take steps to overcome in this paper. Indeed, non-monotone models are known to be (sometimes exponentially) more powerful than monotone models, and thus, constructing a secret-sharing scheme for any monotone access structure given a general-purpose CDS scheme seems like a highly non-trivial endeavor.

We describe a simplified version of our techniques in this introduction.

Secret Sharing for Monotone Slice Functions. Our first step is to reduce secret sharing for arbitrary (monotone) functions to ones for slice functions, defined as follows. A slice function on n input bits assigns 0 to every input with Hamming weight $n/2-1$ or less, and 1 to every input with Hamming weight $n/2+1$ or more. (In between, namely on inputs of Hamming weight exactly $n/2$, the slice function is arbitrary.)

Slice functions are a generalization of paired-up access functions. Moreover, there are $2^{\binom{n}{n/2}}$ many slice functions out of a total of $2^{\binom{n}{n/2}\cdot(1+O(\log n/n))}$ monotone functions, which brings us much closer to realizing a secret sharing scheme for all monotone access structures. Indeed, we will construct a secret sharing scheme for all slice functions with share size $2^{\tilde{O}(\sqrt{n})}$.

Theorem 1.2 (Informal, [LVW17b, BKN18])**.** *For every slice access structure (function), there is a secret sharing scheme with total share size $2^{\tilde{O}(\sqrt{n})}$.*

We will first go over how to construct a secret sharing scheme with share size $2^{\tilde{O}(\sqrt{n})}$ for all slice functions (proving Theorem 1.2). We then show how to use secret sharing for fat-slice functions — a generalization of slice functions — to construct a secret sharing scheme for all monotone functions (proving Thoerem 1.1), in the process increasing the share size to $2^{(1-\epsilon)n}$ for some constant $\epsilon > 0$. Let us remark that it remains a major open question whether we can translate our gains for slice functions to hold also for all monotone functions.

The first key idea in our construction for slice functions is the notion of being balanced w.r.t. partitions. Let Π be an even partition of n parties into $k = \sqrt{n}$ buckets each of size $n/k = \sqrt{n}$. A set $T \subseteq [n]$ with $|T| = n/2$ is *balanced* w.r.t. partition Π if each bucket of Π contains the same number of parties from T (here and in the rest of the introduction, imagine that $\sqrt{n}$ is an integer). That is, each bucket contains $\sqrt{n}/2$ parties from T.

Given a monotone slice function F, define the monotone slice function F_Π corresponding to a partition Π as follows:

$$\mathsf{F}_\Pi(T) = \begin{cases} 0, & \text{if } |T| = n/2 \text{ and } T \text{ is not balanced w.r.t. } \Pi \\ \mathsf{F}(T), & \text{otherwise} \end{cases}$$

That is, F_Π "kills" all sets of size $n/2$ which are not balanced w.r.t. the partition Π but is otherwise the same as F.

By a simple probabilistic argument, we show that there is a collection of $L = 2^{\tilde{O}(\sqrt{n})}$ partitions $\mathcal{P} = \{\Pi^1, \ldots, \Pi^L\}$ such that every subset $T \subseteq [n]$ with $|T| = n/2$ is balanced w.r.t. some partition Π^ℓ. Therefore, $\mathsf{F} = \bigvee_{\ell=1}^{L} \mathsf{F}_{\Pi^\ell}$. In other words, to construct a secret sharing scheme for F, it suffices to construct a scheme for each of the F_{Π^ℓ}. Once we have such a scheme for all F_{Π^ℓ}, the dealer for the F-secret sharing scheme simply shares the secret s w.r.t. each F_{Π^ℓ}.

The second key idea is to use a CDS scheme to construct a secret sharing scheme for each of the functions F_{Π^ℓ}. Recall that Π^ℓ has k buckets with b parties in each bucket. To construct the scheme to share a secret bit s, we use a CDS scheme with $k = \sqrt{n}$ parties where each party has as input a string $\mathbf{x} \in \{0,1\}^{n/k}$, and all parties have the same bit (to be defined below). The construction works as follows.

- The dealer picks a random bit σ_j for each of the k buckets.

  She shares σ_j using a $b/2$-out-of-b secret sharing scheme among parties in the bucket.

- The dealer then defines $\sigma^* = s \oplus \sigma_1 \oplus \ldots \oplus \sigma_k$. She chooses a common random string R for the CDS protocol, and generates for each bucket j, the messages

$$\left\{\mu_{j,\mathbf{x}} := \mathsf{CDS.Msg}_j(\mathbf{x}, \sigma^*; R)\right\}_{j\in[k],\mathbf{x}\in\{0,1\}^b}$$

  That is, for each party j in the CDS protocol, enumerate over all its possible inputs $\mathbf{x}$, using the same bit σ^* and the same randomness R.

  She additively shares each $\mu_{j,\mathbf{x}}$ among parties indexed by $\mathbf{x}$ in the bucket j.

- Finally, the dealer shares the secret s using a $(n/2+1)$-out-of-n threshold secret sharing scheme.

So, why does this construction work? Let us first verify privacy. That is, consider a set T which is either (a) too small, namely $|T| < n/2$; or (b) $|T| = n/2$ but it is not balanced w.r.t. Π^ℓ; or (c) $|T| = n/2$ but it is not authorized w.r.t. F, namely $\mathsf{F}(T) = 0$.

- If $|T| < n/2$, at least one of the buckets j has fewer than $b/2$ parties, meaning that σ_j is hidden. Since σ_j is hidden, so is s.

- If $T = n/2$ but not balanced w.r.t. Π^ℓ, it is the same story all over again. That is, at least one of the buckets j has fewer than $b/2$ parties which means that σ_j, and therefore s, is hidden.

- The final case is that $|T| = n/2$ and it is balanced w.r.t. Π^ℓ, but $\mathsf{F}(T) = 0$. In this case, the parties in T will manage to recover all σ_j, but the privacy guarantee of CDS implies that they will have no information about σ^*.

  It is absolutely crucial here that the parties in T will only manage to recover a single CDS message per CDS party; that is a single message $\mu_{j,\mathbf{x}}$ for any bucket j; without this property, we would not have been able to invoke the CDS privacy guarantee.

We will leave it to the reader to verify correctness, which goes along much the same lines as our argument for privacy.

The total share size in the scheme is

$$\underbrace{2^{\tilde{O}(\sqrt{n})}}_{\#\text{ partitions}} \cdot \left(\underbrace{2^{O(\sqrt{n})}}_{\#\text{ inputs per bucket}} \cdot \underbrace{2^{\tilde{O}(\sqrt{n})}}_{\text{CDS msg size}} + \underbrace{O(n\log n)}_{\text{threshold SS}} \right) = 2^{\tilde{O}(\sqrt{n})}$$

Secret Sharing for All Monotone Functions via Fat-Slice Functions. Now, we would like to convert the secret sharing scheme described above for slice functions into one for all monotone functions. The initial idea is to partition each access structure $\mathcal{A}$ into two access structures: a slice access structure $\mathcal{A}_1$; and a top-and-bottom access structure $\mathcal{A}_2$ which captures sets of size either less or more than $n/2$. The plan then is to use our slice secret sharing scheme for $\mathcal{A}_1$ and a trivial secret sharing scheme for $\mathcal{A}_2$ which has share size proportional to the number of sets in $\mathcal{A}_2$.

This runs into trouble right away because the top-and-bottom access structure $\mathcal{A}_2$ has way too many sets; indeed about $2^n \cdot (1 - 1/\sqrt{n})$ many of them.

The solution is to mitigate this issue by implementing a more refined version of this program where we construct a secret sharing scheme for what we call *fat-slice functions*. These are access functions on n bits that assign 0 to all sets of size less than a and 1 for all sets of size more than b, for some parameters $a \leq b$. A slice function is the special case of a fat-slice function with $a = b = n/2$. The size of the shares in our final secret sharing scheme come in because of a delicate balancing between (a) the fat-slice secret sharing scheme which becomes more expensive as the size of the slice $b - a$ grows; and (b) the top-and-bottom secret sharing scheme which becomes more expensive as $b - a$ shrinks.

Inherently, for every monotone function, we construct a small (i.e. size $2^{(1-\epsilon)n}$) constant-depth monotone boolean formula computing it using AND gate, OR gate and all *slice gates*[3]. A slice gate is an n-bit-to-1-bit monotone gate that computes a slice function. Such a formula can be converted into a secret sharing scheme via composition in a standard way. Notice that previous results constructing secret sharing scheme realizing slice functions follow the same paradigm. They inherently construct small (i.e. size $2^{\tilde{O}(\sqrt{n})}$) monotone formulas computing any slice functions using AND gate, OR gate and all *CDS gates*, which can be formally defined as paired-up functions.

2 Preliminaries and Definitions

We start with some notation that we will use throughout the paper.

- For a positive integer m, let $[m] := \{1, \ldots, m\}$.
- For a set T, let 2^T denote the set consisting of all subsets of T. For a set T and non-negative integer k, let $\binom{T}{k}$ be the set consisting of all size-k subsets of T.

2.1 Secret Sharing

Definition 1 (general secret sharing)**.** A general secret sharing scheme over n parties is specified by a a monotone boolean function $\mathsf{F} : 2^{[n]} \to \{0,1\}$. For any monotone $\mathsf{F} : 2^{[n]} \to \{0,1\}$, an information-theoretic secret-sharing scheme realizing access function F is a randomized algorithm

$$\mathsf{Share} : \{0,1\} \times \mathcal{W} \to (\{0,1\}^{\mathsf{ss}})^n$$

that on input a secret bit, outputs n shares $s_1, \ldots, s_n \in \{0,1\}^{\mathsf{ss}}$ satisfying the following properties:

(correctness.) For all $T \subseteq [n]$ that $\mathsf{F}(T) = 1$, there exists a reconstruction algorithm $\mathsf{C}_T : (\{0,1\}^{\mathsf{ss}})^{|T|} \to \{0,1\}$ such that for all $\sigma \in \{0,1\}, w \in \mathcal{W}$,

$$\mathsf{Share}(\sigma; w) = (s_1, \ldots, s_n) \implies \mathsf{C}_T((x_i)_{i \in T}) = \sigma.$$

(privacy.) For all $T \subseteq [n]$ that $\mathsf{F}(T) = 0$, there exists a simulator whose output on empty input is perfectly indistinguishable from the joint distribution of $(s_i)_{i \in T}$ for any secret $\sigma \in \{0,1\}$, where $(s_1, \ldots, s_n) := \mathsf{Share}(\sigma; w)$ and the randomness are taken over $w \overset{\text{R}}{\leftarrow} \mathcal{W}$ and the coin tosses of the simulator.

[3] Actually, the circuit implicitly constructed is made of AND/OR gates and CDS gates (mentioned later). But slice gates has clearer definition, and they are equivalently powerful as CDS gates.

ss is the share size of this secret sharing scheme Share.

Definition 2 (linear secret sharing)**.** A linear secret sharing scheme is a secret sharing scheme where all operations are linear. For example, $\mathsf{Share} : \{0,1\} \times \mathcal{W} \to (\{0,1\}^{\mathsf{ss}})^n$ is a linear secret sharing scheme over binary field if $\mathcal{W}$ is a vector space over binary field and Share is a linear function.

Definition 3 (share size complexity)**.** For any monotone boolean function F, the share size of F, denoted by $\mathsf{ss}(\mathsf{F})$, is the minimum integer such that there exists a secret sharing scheme realizing F whose share size is $\mathsf{ss}(\mathsf{F})$.

Similarly, the linear secret-sharing share size of F, denoted by $\mathsf{ss}_{\mathsf{lin}}(\mathsf{F})$, is defined as the minimum integer such that there exists a linear secret sharing scheme realizing F whose share size is $\mathsf{ss}_{\mathsf{lin}}(\mathsf{F})$. By definition, $\mathsf{ss}_{\mathsf{lin}}(\mathsf{F}) \leq \mathsf{ss}(\mathsf{F})$.

Definition 4 (minimal authorized sets, maximal unauthorized sets)**.** For any monotone function F, a subset $T \subseteq [n]$ is an authorized set according to F if $\mathsf{F}(T) = 1$, and T is unauthorized set otherwise. Let $\mathsf{F}^{-1}(1)$ denote all authorized subsets according to F and $\mathsf{F}^{-1}(0)$ denote all unauthorized subsets according to F.

T is a *minimal authorized set* if T is an authorized set and all proper subsets of T are unauthorized sets. T is a *maximal unauthorized set* if T is an unauthorized set and all proper supersets of T are authorized sets. Let $\min \mathsf{F}^{-1}(1)$ denote all minimal authorized subsets according to F and $\max \mathsf{F}^{-1}(0)$ denote all maximal unauthorized subsets according to F.

Access function families. An access function family over n parties is a collection of monotone functions $\mathsf{F} : 2^{[n]} \to \{0,1\}$. For any access function family $\mathfrak{F}$, the share size of $\mathfrak{F}$, denoted by $\mathsf{ss}(\mathfrak{F})$, is defined as $\mathsf{ss}(\mathfrak{F}) := \max_{\mathsf{F}\in\mathfrak{F}} \mathsf{ss}(\mathsf{F})$.

In the introduction, we already mentioned the following access function families. A few auxiliary access function families will also be defined on demand in Section 3.

- **All monotone functions:** $\mathfrak{F}^n$ contains all function $\mathsf{F} : 2^{[n]} \to \{0,1\}$ satisfying $\forall T \subseteq T' \subseteq [n], \mathsf{F}(T) \leq \mathsf{F}(T')$.
- **Fat-slice functions:** $\mathfrak{F}^n_{[a,b]}$ contains all monotone function $\mathsf{F} \in \mathfrak{F}^n$ such that $\forall T \subseteq [n], (|T| < a \implies \mathsf{F}(T) = 0) \wedge (|T| > b \implies \mathsf{F}(T) = 1)$.
- **Threshold functions:** $\mathfrak{F}^n_{\text{thrsh}}$ contains all threshold function $\mathsf{F}_{\text{thres-}t}$ for $t \in [1,n]$ where $\mathsf{F}_{\text{thres-}t}$ is defined as and $\forall T \subseteq [n], \mathsf{F}_{\text{thres-}t}(T) = 1 \iff |T| \geq t$.

Previous results on information-theoretic secret sharing.

Lemma 2.1 (conjunction and disjunction)**.** *For any access functions* $\mathsf{F}_1, \mathsf{F}_2 \in \mathfrak{F}^n$*,*

$$\mathsf{ss}(\mathsf{F}_1 \vee \mathsf{F}_2) \leq \mathsf{ss}(\mathsf{F}_1) + \mathsf{ss}(\mathsf{F}_2), \qquad \mathsf{ss}(\mathsf{F}_1 \wedge \mathsf{F}_2) \leq \mathsf{ss}(\mathsf{F}_1) + \mathsf{ss}(\mathsf{F}_2),$$
$$\mathsf{ss}_{\mathit{lin}}(\mathsf{F}_1 \vee \mathsf{F}_2) \leq \mathsf{ss}_{\mathit{lin}}(\mathsf{F}_1) + \mathsf{ss}_{\mathit{lin}}(\mathsf{F}_2), \qquad \mathsf{ss}_{\mathit{lin}}(\mathsf{F}_1 \wedge \mathsf{F}_2) \leq \mathsf{ss}_{\mathit{lin}}(\mathsf{F}_1) + \mathsf{ss}_{\mathit{lin}}(\mathsf{F}_2).$$

Theorem 2.2 (threshold, [Sha79, KN90, BGK16])**.** *For all* $n \in \mathbb{N}$*,* $\mathsf{ss}_{\mathit{lin}}(\mathfrak{F}^n_{\text{thrsh}}) \leq \lfloor \log n \rfloor$*, which is optimal as* $\mathsf{ss}(\mathfrak{F}^n_{\text{thrsh}}) = \Theta(\log n)$.

Lemma 2.3. *For any non-trivial access function* $\mathsf{F} \in \mathfrak{F}^n$*, for each authorized set* A *according to* F*, there exists a minimal authorized set* A' *such that* $A' \subseteq A$*. Symmetrically, for each unauthorized set* B *according to* F*, there exists a maximal unauthorized set* B' *such that* $B' \supseteq B$*.*

Lemma 2.4 (slice functions [LVW17b, BKN18])**.** *For all* $n \in \mathbb{N}$*,* $\mathsf{ss}(\mathfrak{F}^n_{[\frac{n}{2},\frac{n}{2}]}) \leq 2^{O(\sqrt{n}\log n)}$*.*

2.2 Conditional Disclosure of Secrets

In a k-party CDS scheme, there are k parties who know a secret message σ and jointly hold input x. These parties cannot communicate with each other, but instead they have access to a common random string (CRS). Their goal is to send a single message to the CDS referee Charlie, at the end of which Charlie, who already knows x, should learn σ if and only if $\mathsf{P}(x) = 1$, for a fixed predicate P.

Definition 5 (conditional disclosure of secrets (CDS) [GIKM00])**.** Let input spaces $\mathcal{X}_1, \ldots, \mathcal{X}_k$, secret space $\{0,1\}$ and randomness space $\mathcal{W}$ be finite sets. Fix a predicate $\mathsf{P} : \mathcal{X}_1 \times \mathcal{X}_2 \times \ldots \times \mathcal{X}_k \to \{0,1\}$. A cc-*conditional disclosure of secrets (CDS)* protocol for P is a tuple of deterministic functions $(\mathsf{B}_1, \ldots, \mathsf{B}_k, \mathsf{C})$

$$\text{Transmitting functions } \mathsf{B}_i : \{0,1\} \times \mathcal{X}_i \times \mathcal{W} \to \{0,1\}^{\mathsf{cc}}$$
$$\text{Reconstruction function } \mathsf{C} : \mathcal{X}_1 \times \ldots \times \mathcal{X}_k \times \{0,1\}^{\mathsf{cc} \times k} \to \{0,1\}$$

satisfying the following properties:

(reconstruction.) For all $(x_1, \ldots, x_k) \in \mathcal{X}_1 \times \ldots \times \mathcal{X}_k$ such that $\mathsf{P}(x_1, \ldots, x_k) = 1$, for all $w \in \mathcal{W}$, and for all $\sigma \in \{0,1\}$:

$$\mathsf{C}(x_1, \ldots, x_k, \mathsf{B}_1(\sigma, x_1; w), \ldots, \mathsf{B}_k(\sigma, x_k; w)) = \sigma \ .$$

(privacy.) There exists a randomized algorithm S such that for all input tuple $(x_1, \ldots, x_k) \in \mathcal{X}_1 \times \ldots \times \mathcal{X}_k$ satisfying $\mathsf{P}(x_1, \ldots, x_k) = 0$ and for any secret $\sigma \in \{0,1\}$, the joint distribution of $\big(\mathsf{B}_1(\sigma, x_1; w), \ldots, \mathsf{B}_k(\sigma, x_k; w)\big)$ is perfectly indistinguishable from $\mathsf{S}(x_1, \ldots, x_k)$, where the randomness are taken over $w \overset{\mathrm{R}}{\leftarrow} \mathcal{W}$ and the coin tosses of S.

Definition 6 (linear CDS)**.** An CDS scheme $(\mathsf{B}_1, \ldots, \mathsf{B}_k, \mathsf{C})$ is linear over binary field if the randomness space $\mathcal{W}$ is a vector space over binary field and B_i is a linear function on the secret and the randomness, i.e. for all $i \in [k], x_i \in \mathcal{X}_i$, the mapping $(\sigma, w) \mapsto \mathsf{B}_i(\sigma, x_i, w)$ is linear.

Previous results on CDS.

Theorem 2.5 ([LVW17b])**.** *For any predicate* $\mathsf{P} : \mathcal{X}_1 \times \ldots \times \mathcal{X}_k \to \{0,1\}$*, let* $\mathcal{X} := \mathcal{X}_1 \times \ldots \times \mathcal{X}_k$ *be the whole input space, there exists a CDS scheme for* P *with communication complexity* $\mathsf{cc} = 2^{O(\sqrt{\log|\mathcal{X}| \log\log|\mathcal{X}|})}$*, there exists a linear CDS scheme for* P *with communication complexity* $\mathsf{cc} = O(\sqrt{|\mathcal{X}|})$*.*

2.3 Partitions

Definition 7. A k-partition of $[n]$ is a tuple of d disjoint subsets $P_1, \ldots, P_k \subseteq [n]$ such that $\bigcup_{t=1}^{k} P_t = [n]$.

Definition 8. For an integer k divides n, an even k-partition of $[n]$ is a k-partition $(P_1, \ldots, P_k)$ such that $|P_1| = \ldots = |P_k| = n/k$.

3 Proof of the Main Theorem: A Chain of Reductions

Our goal in this section is to show the following (main) theorem which constructs a secret sharing scheme for any monotone access structure with shares of size $2^{0.994n}$.

Theorem 3.1. *For any access function $\mathsf{F} \in \mathfrak{F}^n$, there exists a secret sharing scheme realizing F with share size $O(2^{0.994n})$, and a linear secret sharing scheme realizing F with share size $O(2^{0.999n})$.*

Along the way, we will also show a secret sharing scheme *with sub-exponential share size* for the class of all *fat-slice functions* defined below. A fat-slice function is one which outputs 0 on all sets of size less than a (that is, the access structure rejects all such sets) and outputs 1 on all sets of size more than b (that is, the access structure accepts all such sets).

Theorem 3.2. *For $\delta(n) = o(n/\log n)$, and for any access function $\mathsf{F} \in \mathfrak{F}^n_{[\frac{n}{2}-\delta(n), \frac{n}{2}+\delta(n)]}$, there exists a secret sharing scheme realizing F with share size $\mathsf{ss} = 2^{O(\sqrt{n\delta(n)\log n}+\sqrt{n}\log n)} = 2^{o(n)}$, and a linear secret sharing scheme realizing F with share size $2^{n/2+o(n)}$.*

The proof of Theorem 3.1 and 3.2 repeatedly reduce the secret sharing for a comparatively general family to a more restricted family, by showing that any monotone function in the former family can be computed by combining several functions in the latter family with basic boolean operations (AND, OR), until the function family we need to deal with is so restricted that secret sharing for it can be constructed using an existing conditional disclosure of secrets (CDS) scheme.

More precisely, in each of the monotone function families we considered, the input domain $\{0,1\}^n$ is inherently split into a restricted zone and an unrestricted zone. Functions in this family can map inputs in the unrestricted zone any value, but are enforced to map all inputs in the restricted zone according to a fixed simple formula. As the proof goes, we keep considering a more restricted function family in the sense that its unrestricted zone is smaller than the former one. In the most restricted function family we considered, all the inputs in the unrestricted zone has same size. We have knowledge on how to construct non-trivial secret sharing for monotone functions in such restricted family using CDS (e.g. Lemma 2.4 for slide functions [LVW17b, BKN18]).

The monotone function families we considered are (in the order from general to specific)

- $\mathfrak{F}^n$: The family of all monotone functions. That is, the unrestricted zone is the whole input domain $\{0,1\}^n$.
- $\mathfrak{F}^n_{[a,b]}$ (fat-slice function family): The family of every monotone function F satisfying $|T| < a \implies \mathsf{F}(T) = 0$ and $|T| > b \implies \mathsf{F}(T) = 1$. That is, the unrestricted zone consists of all subsets of size between a and b.

- $\mathfrak{D}^n_{a,b,k\text{-part}}$ (auxiliary family formally defined in Section 3.2): Every function $\mathsf{F} \in \mathfrak{D}^n_{a,b,k\text{-part}}$ is associated with an even k-partition $\Pi = (P_1, \ldots, P_k)$. Besides the constraints enforced by $\mathfrak{F}^n_{[a,b]}$, a function $\mathsf{F} \in \mathfrak{D}^n_{a,b,k\text{-part}}$ satisfies an extra constraint that if $\exists t, |T \cap P_t| < a/k$, then $\mathsf{F}(T) = 0$. Note that this constraint is not compatible with the constraint $|T| > b \implies \mathsf{F}(T) = 1$ introduced by $\mathfrak{F}^n_{[a,b]}$, these constraints actually have different priorities that will be specified later in their formal definitions. In this family, the unrestricted zone consists of all subsets that 1) the subset size is no greater than b, 2) the subset assigns at least a/k elements to every bucket of Π.

- $\mathfrak{C}^n_{a,k\text{-part},m}$ (auxiliary family formally defined in Section 3.3): In addition to an even k-partition $\Pi = (P_1, \ldots, P_k)$, every function $\mathsf{F} \in \mathfrak{C}^n_{a,k\text{-part},m}$ is also associated with subset $\Omega \subseteq [k]$. Besides the constraints enforced by $\mathfrak{D}^n_{a,b,k\text{-part}}$, a function $\mathsf{F} \in \mathfrak{C}^n_{a,k\text{-part},m}$ satisfies an extra constraints that if $\exists t \notin \Omega, |T \cap P_t| > a/k$, then $\mathsf{F}(T) = 1$. In this family, the unrestricted zone consists of all subsets such that 1) the subset assign at least a/k elements to every bucket of Π, 2) the subset assign exactly a/k elements to every bucket P_i that $i \notin \Omega$.

- $\mathfrak{B}^n_{a,k\text{-part},m}$ (auxiliary family formally defined in Section 3.4). In addition to an even k-partition $\Pi = (P_1, \ldots, P_k)$ and subset $\Omega \subseteq [k]$, every function $\mathsf{F} \in \mathfrak{B}^n_{a,k\text{-part},m}$ is also associated with subset $A \subseteq \bigcup_{i \in \Omega} P_i$. Besides the constraints enforced by $\mathfrak{C}^n_{a,k\text{-part},m}$, a function in $\mathfrak{B}^n_{a,k\text{-part},m}$ satisfies extra constraints so that the unrestricted zone constraints of all subsets T that 1) $T \cap P_i = A \cap P_i$ for every $i \in \Omega$, 2) T assign exactly a/k elements to every bucket P_i that $i \notin \Omega$.

3.1 Reduction: Step 1

In the first step, we show how to construct a secret sharing scheme for any access structure in $\mathfrak{F}^n$ given a secret sharing scheme for all access structures in $\mathfrak{F}^n_{[a,b]}$.

Auxiliary access functions. For any $S \subseteq [n]$, define monotone function $\mathsf{E}_{\wedge S}$ as

$$\mathsf{E}_{\wedge S}(T) = 1 \iff T \supseteq S,$$

such that $\mathsf{E}_{\wedge S}$ is the smallest[4] monotone function satisfying $\mathsf{E}_{\wedge S}(S) = 1$. Then $\mathsf{ss}_{\mathsf{lin}}(\mathsf{E}_{\wedge S}) = 1$ as there is a simple scheme realizing $\mathsf{E}_{\wedge S}$ by additively share the secret bit σ among all parties in S: $\mathsf{Share}(\sigma) \to (s_1, \ldots, s_n)$ outputs a random vector satisfying $\bigoplus_{i \in S} s_i = \sigma$.

For any $S \subseteq [n]$, define monotone function $\mathsf{E}_{\vee \bar{S}}$ as

$$\mathsf{E}_{\vee \bar{S}}(T) = 1 \iff T \cap \bar{S} \neq \varnothing.$$

such that $\mathsf{E}_{\vee \bar{S}}$ is the greatest[5] monotone function satisfying $\mathsf{E}_{\vee \bar{S}}(S) = 0$. Then $\mathsf{ss}_{\mathsf{lin}}(\mathsf{E}_{\vee \bar{S}}) = 1$ as there is a simple scheme realizing $\mathsf{E}_{\vee \bar{S}}$ by sending the secret bit σ to every party outside S: $\mathsf{Share}(\sigma) = (s_1, \ldots, s_n)$ that $s_i = \sigma$ if $i \notin S$ and $s_i = 0$ otherwise.

[4] Formally, $\mathsf{E}_{\wedge S}$ is the conjunction of all monotone function F satifying $\mathsf{F}(S) = 1$, and it is easy to prove that the conjunction also satifies $\mathsf{E}_{\wedge S}(S) = 1$.

[5] Formally, $\mathsf{E}_{\vee \bar{S}}$ is the disjunction of all monotone function F satifying $\mathsf{F}(S) = 0$, and it is easy to prove that the disjunction also satifies $\mathsf{E}_{\vee \bar{S}}(S) = 0$.

Lemma 3.3. *For any $0 < \delta < n/2$ and for any monotone function $\mathsf{F} \in \mathfrak{F}^n$, there exist monotone functions $\mathsf{F}_{\text{top}}, \mathsf{F}_{\text{mid}}, \mathsf{F}_{\text{bot}}$ satisfying $\mathsf{F}_{\text{mid}} \in \mathfrak{F}^n_{[\frac{n}{2}-\delta, \frac{n}{2}+\delta]}$ and $\mathsf{ss}_{\mathit{lin}}(\mathsf{F}_{\text{top}}), \mathsf{ss}_{\mathit{lin}}(\mathsf{F}_{\text{bot}}) \leq \binom{n}{\frac{n}{2}-\delta}$ such that $\mathsf{F} = \mathsf{F}_{\text{top}} \wedge (\mathsf{F}_{\text{mid}} \vee \mathsf{F}_{\text{bot}})$.*

Corollary 3.4. For any $0 < \delta < n/2$,

$$\mathsf{ss}(\mathfrak{F}^n) \leq \mathsf{ss}(\mathfrak{F}^n_{[\frac{n}{2}-\delta, \frac{n}{2}+\delta]}) + 2 \cdot \binom{n}{\frac{n}{2}-\delta},$$
$$\mathsf{ss}_{\mathsf{lin}}(\mathfrak{F}^n) \leq \mathsf{ss}_{\mathsf{lin}}(\mathfrak{F}^n_{[\frac{n}{2}-\delta, \frac{n}{2}+\delta]}) + 2 \cdot \binom{n}{\frac{n}{2}-\delta}.$$

Proof of Lemma 3.3. For any $\mathsf{F} \in \mathfrak{F}^n$, define $\mathsf{F}_{\text{top}}, \mathsf{F}_{\text{mid}}, \mathsf{F}_{\text{bot}}$ as the following

- F_{top} is the greatest monotone function satisfying $\mathsf{F}_{\text{top}}(T) = \mathsf{F}(T)$ for all $|T| > \frac{n}{2} + \delta$.

$$\mathsf{F}_{\text{top}}(T) = 0 \iff \exists T' \supseteq T, (|T'| > \frac{n}{2} + \delta) \wedge (\mathsf{F}(T') = 0).$$

- F_{bot} is the smallest monotone function satisfying $\mathsf{F}_{\text{bot}}(T) = \mathsf{F}(T)$ for all $|T| < \frac{n}{2} - \delta$.

$$\mathsf{F}_{\text{bot}}(T) = 1 \iff \exists T' \subseteq T, (|T'| < \frac{n}{2} - \delta) \wedge (\mathsf{F}(T') = 1).$$

- F_{mid} is the unique monotone function in $\mathfrak{F}^n_{[\frac{n}{2}-\delta, \frac{n}{2}+\delta]}$ satisfying $\mathsf{F}_{\text{top}}(T) = \mathsf{F}(T)$ for all $|T| \in [\frac{n}{2} - \delta, \frac{n}{2} + \delta]$.

$$\mathsf{F}_{\text{mid}}(T) = \begin{cases} 1, & \text{if } |T| > \frac{n}{2} + \delta \\ \mathsf{F}(T), & \text{if } |T| \in [\frac{n}{2} - \delta, \frac{n}{2} + \delta] \\ 0, & \text{if } |T| < \frac{n}{2} - \delta \end{cases}$$

In order to prove Lemma 3.3, we first show F is a simple composition of $\mathsf{F}_{\text{top}}, \mathsf{F}_{\text{mid}}, \mathsf{F}_{\text{bot}}$

$$\mathsf{F} = \mathsf{F}_{\text{top}} \wedge (\mathsf{F}_{\text{mid}} \vee \mathsf{F}_{\text{bot}}). \tag{1}$$

Then finish the proof by showing $\mathsf{ss}_{\mathsf{lin}}(\mathsf{F}_{\text{top}}), \mathsf{ss}_{\mathsf{lin}}(\mathsf{F}_{\text{bot}}) \leq \binom{n}{\frac{n}{2}-\delta}$.

To prove equation (1), consider different cases depending on the size of the input set. For any $T \subseteq [n]$

If $|T| > \frac{n}{2} + \delta$: We have $\mathsf{F}_{\text{top}}(T) = \mathsf{F}(T)$ and $\mathsf{F}_{\text{mid}}(T) = 1$, therefore

$$\mathsf{F}_{\text{top}}(T) \wedge (\mathsf{F}_{\text{mid}}(T) \vee \mathsf{F}_{\text{bot}}(T)) = \mathsf{F}(T) \wedge (1 \vee \mathsf{F}_{\text{bot}}(T)) = \mathsf{F}(T).$$

If $|T| \in [\frac{n}{2} - \delta, \frac{n}{2} + \delta]$: We have $\mathsf{F}_{\text{mid}}(T) = \mathsf{F}(T)$. Moreover, by definition, $\mathsf{F}_{\text{bot}} \leq \mathsf{F} \leq \mathsf{F}_{\text{top}}$. Therefore

$$\mathsf{F}_{\text{top}}(T) \wedge (\mathsf{F}_{\text{mid}}(T) \vee \mathsf{F}_{\text{bot}}(T)) = \mathsf{F}_{\text{top}}(T) \wedge (\mathsf{F}(T) \vee \mathsf{F}_{\text{bot}}(T)) = \mathsf{F}(T).$$

If $|T| < \frac{n}{2} - \delta$: We have $\mathsf{F}_{\text{bot}}(T) = \mathsf{F}(T)$ and $\mathsf{F}_{\text{mid}}(T) = 0$. Moreover, by definition, $\mathsf{F}_{\text{top}} \geq \mathsf{F}$. Therefore

$$\mathsf{F}_{\text{top}}(T) \wedge (\mathsf{F}_{\text{mid}}(T) \vee \mathsf{F}_{\text{bot}}(T)) = \mathsf{F}_{\text{top}}(T) \wedge (0 \vee \mathsf{F}(T)) = \mathsf{F}(T).$$

As F_{top} can be decomposed as

$$\mathsf{F}_{\text{top}} = \bigwedge_{\substack{S \in \mathsf{F}^{-1}(0) \\ |S| > \frac{n}{2}+\delta}} \mathsf{E}_{\vee \bar{S}} = \bigwedge_{\substack{S \in \max \mathsf{F}^{-1}(0) \\ |S| > \frac{n}{2}+\delta}} \mathsf{E}_{\vee \bar{S}}.$$

We have

$$\mathsf{ss}_{\mathsf{lin}}(\mathsf{F}_{\text{top}}) \leq \left| \left\{ S \in \max \mathsf{F}^{-1}(0) \middle| |S| > \frac{n}{2} + \delta \right\} \right| \leq \binom{n}{\frac{n}{2}+\delta}.$$

As F_{bot} can be decomposed as

$$\mathsf{F}_{\text{bot}} = \bigvee_{\substack{S \in \mathsf{F}^{-1}(1) \\ |S| < \frac{n}{2}-\delta}} \mathsf{E}_{\wedge S} = \bigvee_{\substack{S \in \min \mathsf{F}^{-1}(1) \\ |S| < \frac{n}{2}-\delta}} \mathsf{E}_{\wedge S}.$$

We have

$$\mathsf{ss}_{\mathsf{lin}}(\mathsf{F}_{\text{bot}}) \leq \left| \left\{ S \in \min \mathsf{F}^{-1}(1) \middle| |S| < \frac{n}{2} - \delta \right\} \right| \leq \binom{n}{\frac{n}{2}-\delta}. \qquad \square$$

3.2 Reduction: Step 2

In the second step, we show how to construct a secret sharing scheme for any access structure in $\mathfrak{F}^n_{[a,b]}$ given one for any access structure in $\mathfrak{D}^n_{a,b,k\text{-part}}$.

Auxiliary definitions and lemmas. Here we introduce notations to denote when a set is evenly split among a partition. Informally, a subset $T \subseteq [n]$ *is balanced with respect to* an even k-partition $(P_1, \ldots, P_k)$ if for all $t \in [k]$, $|P_t \cap T| = |T|/k$. Notice that this informal definition only works when k divides $|T|$. We introduce an extra notation to describe the case where $|T|$ is not divided by k but the elements in T is almost evenly split among an even k-partition.

For integers a, k, t s.t. $t \leq k$, define[6]

$$\lfloor a/k \rceil_t := \begin{cases} \lceil a/k \rceil, & \text{if } t \leq a \bmod k \\ \lfloor a/k \rfloor, & \text{if } t > a \bmod k. \end{cases}$$

Then $a = \lfloor a/k \rceil_1 + \ldots + \lfloor a/k \rceil_k$ is the most even way to split a as the sum of k integers.

Definition 9 (Balanced with respect to a partition.)**.** Let $(P_1, \ldots, P_k)$ be an even k-partition of $[n]$, a size-a subset $T \subseteq [n]$ is balanced w.r.t. the partition $(P_1, \ldots, P_k)$ if $|T \cap P_t| = \lfloor a/k \rceil_t$ for all $t \in [k]$.

For integer n and real number $\alpha \in [0, n]$, let $\binom{n}{\alpha}$ denotes

$$\binom{n}{\alpha} := \binom{n}{\lceil \alpha \rceil}^{\alpha - \lfloor \alpha \rfloor} \binom{n}{\lfloor \alpha \rfloor}^{1-(\alpha - \lfloor \alpha \rfloor)},$$

which is a weighted geometric average of $\binom{n}{\lceil \alpha \rceil}$ and $\binom{n}{\lfloor \alpha \rfloor}$.

[6] Notation "$\lfloor a/k \rceil_t$" denotes a function of a, k and t. It should not be viewed as a function of a/k and t.

Lemma 3.5. *For integers n, k, a s.t. $a \le n$ and k divides n, there exists a sequence of $L = \frac{O(n)\cdot\binom{n}{a}}{\binom{n/k}{a/k}^k}$ even k-partitions $(P_1^t, \dots, P_k^t)_{t=1}^L$ such that for any set $T \subseteq [n]$ of size a, there exists $t \le L$ such that T is balanced w.r.t. $(P_1^t, \dots, P_k^t)$.*

Proof. Fix a set $T \subseteq [n]$ s.t. $|T| = a$ and sample a random even k-partition $(P_1, \dots, P_k)$. Then probability that T is balance w.r.t. partition $(P_1, \dots, P_k)$ is

$$\frac{\prod_{t=1}^k \binom{n/k}{\lfloor a/k \rceil_t}}{\binom{n}{a}} = \frac{\binom{n/k}{\lceil a/k \rceil}^{a \bmod k} \binom{n/k}{\lfloor a/k \rfloor}^{k-(a \bmod k)}}{\binom{n}{a}} = \frac{\binom{n/k}{a/k}^k}{\binom{n}{a}}.$$

Therefore, by i.i.d. sampling $L = \frac{O(n)\cdot\binom{n}{a}}{\binom{n/k}{a/k}^k}$ random even k-partition, T is balance w.r.t. one of the partition is at least $1 - 2^{-n}$. The proof is completed by a union bound over T. □

Auxiliary access function families. For $0 \le a \le b \le n$ and k divides n, the function family $\mathfrak{D}^n_{a,b,k\text{-part}}$ contains all function F such that there exists $\Pi = (P_1, \dots, P_k)$ an even k-partition of $[n]$ and F satisfies

$$\mathsf{F}(T) = \begin{cases} 1, & \text{if } |T| > b \\ 0, & \text{else if } \exists t \in [k], |T \cap P_t| < \lfloor a/k \rceil_t \\ \mathsf{F}(T), & \text{otherwise} \end{cases} \tag{2}$$

Lemma 3.6. *For integers $a \le b < n$ and k divides n, for any function $\mathsf{F} \in \mathfrak{F}^n_{[a,b]}$, there exists a sequence of $L = \frac{O(n)\cdot\binom{n}{a}}{\binom{n/k}{a/k}^k}$ functions $\mathsf{F}_1, \dots, \mathsf{F}_L \in \mathfrak{D}^n_{a,b,k\text{-part}}$ such that $\mathsf{F} = \bigvee_{\ell=1}^L \mathsf{F}_\ell$.*

Corollary 3.7. For integers $a \le b < n$ and k divides n,

$$\mathsf{ss}(\mathfrak{F}^n_{[a,b]}) \le \frac{O(n)\cdot\binom{n}{a}}{\binom{n/k}{a/k}^k} \cdot \mathsf{ss}(\mathfrak{D}^n_{a,b,k\text{-part}}),$$

$$\mathsf{ss}_{\mathsf{lin}}(\mathfrak{F}^n_{[a,b]}) \le \frac{O(n)\cdot\binom{n}{a}}{\binom{n/k}{a/k}^k} \cdot \mathsf{ss}_{\mathsf{lin}}(\mathfrak{D}^n_{a,b,k\text{-part}}).$$

Proof of Lemma 3.6. By Lemma 3.5, there exists $L = \frac{O(n)\cdot\binom{n}{a}}{\binom{n/k}{a/k}^k}$ and L even k-partitions $\Pi^\ell = (P_1^\ell, \dots, P_k^\ell)$ for $\ell \in [L]$, such that for any set $T \subseteq \binom{[n]}{a}$, set T is balanced w.r.t. Π^ℓ for some $\ell \in [L]$.

For any $\mathsf{F} \in \mathfrak{F}^n_{[a,b]}$, and for any even k-partition $\Pi = (P_1, \dots, P_k)$, define F_Π as

$$\mathsf{F}_\Pi(T) = \begin{cases} 1, & \text{if } |T| > b \\ 0, & \text{else if } \exists t \in [k], |T \cap P_t| < \lfloor a/k \rceil_t \\ \mathsf{F}(T), & \text{otherwise} \end{cases} \tag{3}$$

then $\mathsf{F}_\Pi \in \mathfrak{D}^n_{a,b,k\text{-part}}$. Compare F with $\bigvee_{\ell=1}^L \mathsf{F}_{\Pi^\ell}$.

- On one hand, $\mathsf{F} \ge \mathsf{F}_{\Pi^\ell}$ for each $\ell \in [L]$, thus $\mathsf{F} \ge \bigvee_{\ell=1}^L \mathsf{F}_{\Pi^\ell}$.

- On the other hand, for each $T \subseteq [n]$ s.t. $|T| \leq b$ and $\mathsf{F}(T) = 1$, consider one size-a subset $T' \subseteq T$. There exists $\ell^* \in [L]$ that T' is balanced w.r.t. Π^{ℓ^*}, which implies $|T \cap P_t^{\ell^*}| \geq |T' \cap P_t^{\ell^*}| = \lfloor a/k \rceil_t$ for all $t \in [k]$, thus $\bigvee_{\ell=1}^{L} \mathsf{F}_{\Pi^\ell}(T) \geq \mathsf{F}_{\Pi^{\ell^*}}(T) = 1$.

Combining both directions, $\mathsf{F} = \bigvee_{\ell=1}^{L} \mathsf{F}_{\Pi^\ell}$. □

3.3 Reduction: Step 3

In the third step, we show how to construct a secret sharing scheme for any access structure in $\mathfrak{D}^n_{a,b,k\text{-part}}$ given one for any access structure in $\mathfrak{C}^n_{a,k\text{-part},m}$ (to be defined below).

Auxiliary access function families. For integers n, a, k, m s.t. $a \leq n$ and $m \leq k$ and k divides n, the monotone function family $\mathfrak{C}^n_{a,k\text{-part},m}$ contains all monotone function F such that there exists an even k-partition $\Pi = (P_1, \ldots, P_k)$ and subset $\Omega \in \binom{[k]}{m}$ such that

$$\mathsf{F}(T) = \begin{cases} 0, & \text{if } \exists t \in [k], |T \cap P_t| < \lfloor a/k \rceil_t \\ 1, & \text{else if } \exists t \notin \Omega, |T \cap P_t| > \lfloor a/k \rceil_t \\ \mathsf{F}(T), & \text{otherwise} \end{cases} \tag{4}$$

Lemma 3.8. *For n, a, b, k that $a + k \leq b \leq n$ and k divides n, for any monotone function $\mathsf{F} \in \mathfrak{D}^n_{a,b,k\text{-part}}$, there exist $L = \binom{k}{b-a}$ functions $\mathsf{F}_1, \ldots, \mathsf{F}_L \in \mathfrak{C}^n_{a,k\text{-part},(b-a)}$ such that $\mathsf{F} = \bigwedge_{i=1}^{L} \mathsf{F}_i \vee \mathsf{F}_{\text{thres-}(b+1)}$.*

Corollary 3.9. For n, a, b, k that $a + k \leq b \leq n$ and k divides n

$$\mathsf{ss}(\mathfrak{D}^n_{a,b,k\text{-part}}) \leq \binom{k}{b-a} \cdot \mathsf{ss}(\mathfrak{C}^n_{a,k\text{-part},(b-a)}) + \lceil \log n \rceil,$$
$$\mathsf{ss}_{\mathsf{lin}}(\mathfrak{D}^n_{a,b,k\text{-part}}) \leq \binom{k}{b-a} \cdot \mathsf{ss}_{\mathsf{lin}}(\mathfrak{C}^n_{a,k\text{-part},(b-a)}) + \lceil \log n \rceil.$$

Proof of Lemma 3.8. For any $\mathsf{F} \in \mathfrak{D}^n_{a,b,k\text{-part}}$, let $\Pi = (P_1, \ldots, P_k)$ be its associated even k-partition. For any $\Omega \in \binom{[k]}{b-a}$, define F_Ω as

$$\mathsf{F}_\Omega(T) := \begin{cases} 0, & \text{if } \exists t \in [k], |T \cap P_t| < \lfloor a/k \rceil_t \\ 1, & \text{else if } \exists t \notin \Omega, |T \cap P_t| > \lfloor a/k \rceil_t \\ \mathsf{F}(T), & \text{otherwise} \end{cases}$$

Then $\mathsf{F}_\Omega \in \mathfrak{C}^n_{a,k\text{-part},(b-a)}$.

Compare F with $\bigwedge_{\Omega \in \binom{[k]}{b-a}} \mathsf{F}_\Omega \vee \mathsf{F}_{\text{thres-}(b+1)}$.

- On one hand, for any Ω

$$\begin{aligned} \mathsf{F}_\Omega(T) \vee \mathsf{F}_{\text{thres-}(b+1)}(T) &= \begin{cases} 1, & \text{if } |T| > b \\ 0, & \text{else if } \exists t \in [k], |T \cap P_t| < \lfloor a/k \rceil_t \\ 1, & \text{else if } \exists t \notin \Omega, |T \cap P_t| > \lfloor a/k \rceil_t \\ \mathsf{F}(T), & \text{otherwise} \end{cases} \\ &\geq \begin{cases} 1, & \text{if } |T| > b \\ 0, & \text{else if } \exists t \in [k], |T \cap P_t| < \lfloor a/k \rceil_t \\ \mathsf{F}(T), & \text{otherwise} \end{cases} \\ &= \mathsf{F}(T), \end{aligned}$$

thus $\mathsf{F} \leq \bigwedge_{\Omega \in \binom{[k]}{b-a}} \mathsf{F}_\Omega \vee \mathsf{F}_{\text{thres-}(b+1)}$.

- On the other hand, for every $T \subseteq [n]$ that $|T| \leq b$ and $\mathsf{F}(T) = 0$: **a)** If $\exists t \in [k], |T \cap P_t| < \lfloor a/k \rceil_t$, then $\mathsf{F}_\Omega(T) = 0$ for any Ω. **b)** Otherwise $\forall t \in [k], |T \cap P_t| \geq \lfloor a/k \rceil_t$, define $\Omega' := \{t \in [k] : |T \cap P_t| > \lfloor a/k \rceil_t\}$. Then $b \geq |T| \geq a + |\Omega'|$, which implies $|\Omega'| \leq b - a$. Let Ω'' be a size-$(b-a)$ superset of Ω', we have $\mathsf{F}_{\Omega''}(T) = \mathsf{F}(T) = 0$.

Combining both directions, $\mathsf{F} = \bigwedge_{\Omega \in \binom{[k]}{b-a}} \mathsf{F}_\Omega \vee \mathsf{F}_{\text{thres-}(b+1)}$. □

3.4 Reduction: Step 4

In the fourth step, we show how to construct a secret sharing scheme for any access structure in $\mathfrak{C}^n_{a,k\text{-part},m}$ given one for any access structure in $\mathfrak{B}^n_{a,k\text{-part},m}$ (to be defined below).

Auxiliary definitions and lemmas. For any even k-partition $\Pi = (P_1, \ldots, P_k)$ and subset $\Omega \subseteq [k]$, define

$$P_\Omega := \bigcup_{t \in \Omega} P_t.$$

For any monotone function $\mathsf{F} \in \mathfrak{F}^n$, for any $A \subseteq B \subseteq [n]$, define $\mathsf{F}_{\text{inter-}B\text{-eq-}A}$ as

$$\mathsf{F}_{\text{inter-}B\text{-eq-}A}(T) := \begin{cases} 0, & \text{if } A \not\subseteq T \\ \mathsf{F}(T \setminus (B \setminus A)), & \text{otherwise} \end{cases}$$

which is the smallest monotone function that satifies $\forall T \subseteq [n], T \cap B = A \implies \mathsf{F}_{\text{inter-}B\text{-eq-}A}(T) = \mathsf{F}(T)$.

Lemma 3.10. *For any $\mathsf{F} \in \mathfrak{F}^n$ and any $B \subseteq [n]$,*

$$\mathsf{F} = \bigvee_{A \subseteq B} \mathsf{F}_{\textit{inter-}B\textit{-eq-}A}.$$

Proof. On one hand, $\mathsf{F}_{\text{inter-}B\text{-eq-}A} \leq \mathsf{F}$, thus $\bigvee_{A \subseteq B} \mathsf{F}_{\text{inter-}B\text{-eq-}A} \leq \mathsf{F}$.

On the other hand, for any $T \subseteq [n]$,

$$\mathsf{F}_{\text{inter-}B\text{-eq-}(B \cap T)}(T) = \mathsf{F}(T).$$

Thus $\bigvee_{A \subseteq B} \mathsf{F}_{\text{inter-}B\text{-eq-}A} \geq \mathsf{F}$. □

Auxiliary access function families. The function family $\mathfrak{B}^n_{a,k\text{-part},m}$ contains all monotone function F such that there exists an even k-partition $\Pi = (P_1, \ldots, P_k)$ and sets $\Omega \in \binom{[k]}{m}, A \subseteq P_\Omega$ such that

$$\mathsf{F}(T) = \begin{cases} 0, & \text{if } A \not\subseteq T \\ 0, & \text{else if } \exists t \notin \Omega, |T \cap P_t| < \lfloor a/k \rceil_t \\ 1, & \text{else if } \exists t \notin \Omega, |T \cap P_t| > \lfloor a/k \rceil_t \\ \mathsf{F}(T \setminus (P_\Omega \setminus A)), & \text{otherwise} \end{cases} \tag{5}$$

The first and last conditions in (5) imply the following in the secret sharing setting: to recover the secret, every party in A is necessary, every party in $P_\Omega \setminus A$ is useless.

Lemma 3.11. *For any integers $a \leq n$ and k divides n and $m \leq k$, for any function $\mathsf{F} \in \mathfrak{C}^n_{a,k\text{-part},m}$, there exists a sequence of $L \leq 2^{mn/k}$ monotone functions $\mathsf{F}_1, \dots, \mathsf{F}_L$ such that $\mathsf{F} = \bigvee_{i=1}^{L} \mathsf{F}_i$.*

Corollary 3.12. For any integers $a \leq n$ and k divides n and $m \leq k$,

$$\mathsf{ss}(\mathfrak{C}^n_{a,k\text{-part},m}) \leq 2^{mn/k}\mathsf{ss}(\mathfrak{B}^n_{a,k\text{-part},m}),$$
$$\mathsf{ss}_{\mathsf{lin}}(\mathfrak{C}^n_{a,k\text{-part},m}) \leq 2^{mn/k}\mathsf{ss}_{\mathsf{lin}}(\mathfrak{B}^n_{a,k\text{-part},m}).$$

Proof of Lemma 3.11. For any $\mathsf{F} \in \mathfrak{C}^n_{a,k\text{-part},m}$, let $\Pi = (P_1, \dots, P_k)$ be its associated even k-partition and $\Omega \in \binom{[k]}{m}$ be its associated subset such that (4) is satisfied. For every $A \subseteq P_\Omega$

$$\mathsf{F}_{\text{inter-}P_\Omega\text{-eq-}A}(T) := \begin{cases} 0, & \text{if } A \not\subseteq T \\ 0, & \text{else if } \exists t \in \Omega, |A \cap P_t| < \lfloor a/k \rceil_t \\ 0, & \text{else if } \exists t \notin \Omega, |T \cap P_t| < \lfloor a/k \rceil_t \\ 1, & \text{else if } \exists t \notin \Omega, |T \cap P_t| > \lfloor a/k \rceil_t \\ \mathsf{F}(T \setminus (P_\Omega \setminus A)), & \text{otherwise} \end{cases} \quad (6)$$

which is a function in $\mathfrak{B}^n_{a,k\text{-part},m}$. The proof is completed by using Lemma 3.10. □

The complexity can be improved slightly if we only enumerate $\mathsf{F}_{\text{inter-}P_\Omega\text{-eq-}A}$ for $A \subseteq P_\Omega$ such that $\forall t \in \Omega, |A \cap P_t| \geq \lfloor a/k \rceil_t$.

3.5 Reduction to CDS

In the fifth and final step, we show how to construct a secret sharing scheme for any access structure in $\mathfrak{B}^n_{a,k\text{-part},m}$ given a multiparty conditional disclosure of secrets (CDS) protocol as constructed in [LVW17b].

Lemma 3.13. *For k divides n and $m \leq k$,*

$$\mathsf{ss}(\mathfrak{B}^n_{a,k\text{-part},m}) \leq 2^{n/k + O(\sqrt{n}\log n)},$$
$$\mathsf{ss}_{lin}(\mathfrak{B}^n_{a,k\text{-part},m}) \leq 2^{n/k} \cdot O(\binom{n/k}{a/k}^{k/2}).$$

Proof. For any $\mathsf{F} \in \mathfrak{B}^n_{a,k\text{-part},m}$, there exists an even k-partition $\Pi = (P_1, \dots, P_k)$ and set $\Omega \in \binom{[k]}{m}$, $A \subseteq P_\Omega$ such that (5) is satisfied.

W.l.o.g. assume $\Omega = \{k-m+1, \dots, k\}$. Let $k' := k - m$. Define a predicate for a k'-party CDS as the following:

- The input space of the t-th party $\mathcal{X}_t = \binom{P_t}{\lfloor a/k \rceil_t}$
- On input tuple $(S_1, \dots, S_{k'}) \in \mathcal{X} = \binom{P_1}{\lfloor a/k \rceil_1} \times \dots \times \binom{P_{k'}}{\lfloor a/k \rceil_{k'}}$

$$\mathsf{P}_\mathsf{F}(S_1, \dots, S_{k'}) := \mathsf{F}(S_1 \cup \dots \cup S_{k'} \cup A).$$

By Theorem 2.5, there exists a CDS scheme $(\mathsf{B}_1, \dots, \mathsf{B}_{k'}, \mathsf{C})$ realizing P_F with communication complexity $\mathsf{cc} = 2^{O(\sqrt{\log \mathcal{X}}\log\log \mathcal{X})} \leq 2^{O(\sqrt{n}\log n)}$. A secret sharing scheme realizing F can be constructed as the following, On input a secret bit $\sigma \in \{0,1\}$

1. Sample random bits s_i for $i \in A$, let $\sigma' := \sigma \oplus \bigoplus_{i \in A} s_i$.
2. Sample random bits $\mu_1, \ldots, \mu_{k'}$, let $\sigma'' := \sigma' \oplus \mu_1 \oplus \ldots \oplus \mu_{k'}$.
   For each $t \in [k']$, let $(\theta_{t,i})_{i \in P_t}$ be $\lfloor a/k \rceil_t$-out-of-$\frac{n}{k}$ threshold secret sharing of μ_t.
3. For each $t \in [k']$, let $(\theta'_{t,i})_{i \in P_t}$ be $(\lfloor a/k \rceil_t + 1)$-out-of-$\frac{n}{k}$ threshold secret sharing of σ''.
4. Sample a random tape w.
   For each $t \in [k']$, for each $S \in \mathcal{X}_t = \binom{P_t}{\lfloor a/k \rceil_t}$, compute
   $$m_{t,S} = \mathsf{B}_t(\sigma, S; w),$$
   let $\{\alpha_{t,S,i}\}_{i \in S}$ be additive secret sharing of $m_{t,S}$.
5. Output shares $(s_1, \ldots, s_n)$ such that for $t \in [n]$:
   If $i \in A$, s_i is a random bit sample in step 1;
   If $i \in P_\Omega \setminus A$, s_i is empty;
   Otherwise, there exists unique $t \in [k']$ that $i \in P_t$,
   $$s_t = (\theta_{t,i}, \theta'_{t,i}, (\alpha_{t,S,i})_{S \in \mathcal{X}_t, S \ni i}).$$

For every $T \subseteq [n]$, the tuple $(s_i)_{i \in T}$ perfectly hides σ when $\mathsf{F}(T) = 0$ and reveals σ when $\mathsf{F}(T) = 1$ as

- If $A \not\subseteq T$, $\mathsf{F}(T) = 0$. In this case there exists $i^* \in A \setminus T$ and σ is perfectly hidden as it's one-time padded by s_{i^*}.
- Otherwise $A \subseteq T$ and $\sigma \oplus \sigma' = \bigoplus_{i \in A} s_i$ can be learned from $(s_i)_{i \in T}$. In such case, hiding (revealing) σ is equivalent to hiding (revealing) σ'.
  - If there exists $t \in [k'] = \bar{\Omega}$ that $|T \cap P_t| < \lfloor a/k \rceil_t$, then $\mathsf{F}(T) = 0$. In this case σ' is perfectly hidden as it's one-time padded by μ_t.
  - Otherwise, for all $t \in [k'] = \bar{\Omega}$ we have $|T \cap P_t| \geq \lfloor a/k \rceil_t$ and $\sigma' \oplus \sigma'' = \bigoplus_{t \in [k']} \mu_t$ can be learned from $(s_i)_{i \in T}$. In such case, hiding (revealing) σ' is equivalent to hiding (revealing) σ''.
    - $*$ If there $\exists t \in [k'] = \bar{\Omega}$ that $|T \cap P_t| > \lfloor a/k \rceil_t$, then $\mathsf{F}(T) = 1$. In such case, σ'' can be learned from $(\theta'_{t,i})_{i \in T \cap P_t}$, which is contained by $(s_i)_{i \in T}$.
    - $*$ Otherwise, $|T \cap P_t| = \lfloor a/k \rceil_t$ for all $t \in [k'] = \bar{\Omega}$. In such case, $(\theta'_{t,i})_{i \in T, P_t \ni i}$ can be simulated. And $(\alpha_{t,S,i})_{S \ni i, \mathcal{X}_t \ni S}$ reveals $m_{1,T \cap P_1}, \ldots, m_{k',T \cap P_{k'}}$ and nothing else. As
    $$\mathsf{P}_\mathsf{F}(T \cap P_1, \ldots, T \cap P_k) = \mathsf{F}(T \setminus P_\Omega \cup A) = \mathsf{F}(T \setminus (P_\Omega \setminus A)) = \mathsf{F}(T),$$
    tuple $(m_{1,T \cap P_1}, \ldots, m_{k',T \cap P_{k'}})$ reveals σ'' when $\mathsf{F}(T) = 1$ and perfectly hides σ'' when $\mathsf{F}(T) = 0$.

The sharing size complexity of F is bounded by

$$\mathsf{ss}(\mathsf{F}) \le \underbrace{\lceil \log n \rceil}_{\theta_{t,i}} + \underbrace{\lceil \log n \rceil}_{\theta'_{t,i}} + \underbrace{2^{n/k}}_{\substack{\text{enumerate}\\ S \in \mathcal{X}_t}} \cdot \underbrace{2^{O(\sqrt{n}\log n)}}_{\text{c.c. of CDS}} \le 2^{n/k+O(\sqrt{n}\log n)}.$$

To construct a linear secret sharing scheme realizing F, we need a linear CDS scheme instead. By Theorem 2.5, there exists a linear CDS scheme $(\mathsf{B}_1, \ldots, \mathsf{B}_{k'}, \mathsf{C})$ realizing P_F with communication complexity $\mathsf{cc} = O(\sqrt{|\mathcal{X}|}) \le O(\binom{n/k}{a/k}^{k/2})$. Thus

$$\mathsf{ss}_{\mathsf{lin}}(\mathsf{F}) \le 2^{n/k} \cdot O(\binom{n/k}{a/k}^{k/2}). \qquad \square$$

The complexity of the linear secret sharing scheme can be improved slightly if we compute $|\mathcal{X}|$ more accurately. In the later part of this paper, we will choose n, k, a such that $\binom{n/k}{\lfloor a/k \rfloor} = \binom{n/k}{\lceil a/k \rceil}$. In such case, $|\mathcal{X}| = \binom{n/k}{a/k}^{k-m}$.

3.6 Better secret sharing schemes

Finally, we put together all the steps to first prove Theorem 3.2 and then somewhat optimize the parameters to obtain a proof of Theorem 3.1.

Proof of Theorem 3.2. Combine Lemma 3.13, Corollary 3.12, Corollary 3.9 and Corollary 3.7 sequentially, we get

$$\begin{aligned}
\mathsf{ss}(\mathfrak{C}^n_{a,k\text{-part},m}) &\le 2^{mn/k} \cdot \mathsf{ss}(\mathfrak{B}^n_{a,k\text{-part},m}) \le 2^{(m+1)n/k+O(\sqrt{n}\log n)} \\
\mathsf{ss}(\mathfrak{D}^n_{a,b,k\text{-part}}) &\le \binom{k}{b-a} \cdot \mathsf{ss}(\mathfrak{C}^n_{a,k\text{-part},(b-a)}) + \lceil \log n \rceil \\
&\le \binom{k}{b-a} \cdot 2^{(b-a+1)n/k+O(\sqrt{n}\log n)} \\
\mathsf{ss}(\mathfrak{F}^n_{[a,b]}) &\le \frac{O(n) \cdot \binom{n}{a}}{\binom{n/k}{a/k}^k} \cdot \mathsf{ss}(\mathfrak{D}^n_{a,b,k\text{-part}}) \\
&\le \frac{\binom{n}{a} \cdot \binom{k}{b-a}}{\binom{n/k}{a/k}^k} \cdot 2^{(b-a+1)n/k+O(\sqrt{n}\log n)} \qquad (7)
\end{aligned}$$

For any $\delta(n) = o(n/\log n)$, let $k(n) = \sqrt{\frac{n\delta(n)}{\log n}}$. Then

$$\begin{aligned}
\mathsf{ss}(\mathfrak{F}^n_{[\frac{n}{2}-\delta(n),\frac{n}{2}+\delta(n)]}) &\le (n/k)^k \cdot \binom{k}{2\delta(n)} \cdot 2^{(2\delta(n)+1)n/k+O(\sqrt{n}\log n)} \\
&\le 2^{k\log n} \cdot 2^k \cdot 2^{(2\delta(n)+1)n/k+O(\sqrt{n}\log n)} \\
&\le 2^{O(k\log n + n\delta(n)/k + \sqrt{n}\log n)} \\
&\le 2^{O(\sqrt{n\delta(n)\log n} + \sqrt{n}\log n)}.
\end{aligned}$$

Similar to (7), for linear secret sharing, we have

$$\mathsf{ss}_{\mathsf{lin}}(\mathfrak{F}^n_{[a,b]}) \leq \frac{\binom{n}{a} \cdot \binom{k}{b-a}}{\binom{n/k}{a/k}^{k/2}} \cdot 2^{(b-a+1)n/k}.$$

For any $\delta(n) = o(n/\log n)$, let $k(n) = \sqrt{\frac{n\delta(n)}{\log n}}$. Then

$$\begin{aligned} \mathsf{ss}_{\mathsf{lin}}(\mathfrak{F}^n_{[\frac{n}{2}-\delta(n),\frac{n}{2}+\delta(n)]}) &\leq \sqrt{\binom{n}{\frac{n}{2}-\delta(n)}} \cdot (n/k)^{k/2} \cdot \binom{k}{2\delta(n)} \cdot 2^{(2\delta(n)+1)n/k} \\ &\leq 2^{n/2+o(n)}. \end{aligned}$$

□

Proof of Theorem 3.1. Combining formula (7) and Lemma 3.3, we get

$$\mathsf{ss}(\mathfrak{F}^n) \leq 2 \cdot \binom{n}{(\frac{1}{2}+\delta)n} + \frac{\binom{n}{(\frac{1}{2}-\delta)n} \cdot \binom{k}{2\delta n}}{\binom{n/k}{(\frac{1}{2}-\delta)n/k}^k} \cdot 2^{(2\delta n+1)n/k+O(\sqrt{n}\log n)} \tag{8}$$

for any k divides n and $2\delta n \leq k$. By choosing $k = n/C$ for a sufficiently large constant C, and choosing δ be a sufficiently small constant, equation (8) would yields $\mathsf{ss}(\mathfrak{F}^n) \leq 2^{(1-c)n}$ for some constant $c > 0$.

For example, let $k = n/5$, then δ need to satisfies $\delta < \frac{1}{10}$, and we have

$$\binom{n/k}{(\frac{1}{2}-\delta)n/k} = \binom{5}{(\frac{1}{2}-\delta)\cdot 5} = 10$$

as $\binom{5}{(\frac{1}{2}-\delta)\cdot 5}$ is a geometric average of $\binom{5}{2}$ and $\binom{5}{3}$. Then

$$\begin{aligned} \mathsf{ss}(\mathfrak{F}^n) &\leq 2 \cdot \binom{n}{(\frac{1}{2}+\delta)n} + \frac{\binom{n}{(\frac{1}{2}-\delta)n} \cdot \binom{k}{2\delta n}}{\binom{n/k}{(\frac{1}{2}-\delta)n/k}^k} \cdot 2^{(2\delta n+1)n/k+O(\sqrt{n}\log n)} \\ &\leq 2^{h(\frac{1}{2}+\delta)\cdot n+o(n)} + \frac{2^{h(\frac{1}{2}-\delta)\cdot n} \cdot 2^{h(10\delta)\cdot n/5}}{10^{n/5}} \cdot 2^{10\delta n+o(n)} \\ &\leq 2^{h(\frac{1}{2}+\delta)\cdot n+o(n)} + 2^{(h(\frac{1}{2}-\delta)+\frac{1}{5}h(10\delta)+10\delta-\frac{1}{5}\log(10))n+o(n)} \end{aligned} \tag{9}$$

By letting δ be a sufficiently small constant, we have $h(\frac{1}{2}+\delta) = 1-c$ for a constant $c > 0$ and $h(\frac{1}{2}-\delta) + \frac{1}{5}h(10\delta) + 10\delta - \frac{1}{5}\log(10) \approx 1 - \frac{1}{5}\log(10)$, thus $\mathsf{ss}(\mathfrak{F}^n) \leq 2^{(1-c)n+o(n)}$.

The right side of the inequality (9) is minimized when $\delta \approx 0.0465$, which gives us $\mathsf{ss}(\mathfrak{F}^n) \leq O(2^{0.994n})$.

Similarly to (8), for linear secret sharing, we get

$$\mathsf{ss}_{\mathsf{lin}}(\mathfrak{F}^n) \leq 2 \cdot \binom{n}{(\frac{1}{2}+\delta)n} + \frac{\binom{n}{(\frac{1}{2}-\delta)n} \cdot \binom{k}{2\delta n}}{\binom{n/k}{(\frac{1}{2}-\delta)n/k}^{k/2}} \cdot 2^{(2\delta n+1)n/k+O(1)} \tag{10}$$

for any k divides n and $2\delta n \leq k$. Let $k = n/5$ and $\delta = 0.019$, then (10) gives us $\mathsf{ss}_{\mathrm{lin}}(\mathfrak{F}^n) \leq O(2^{0.999n})$. □

We did not make our best effort to optimize the constant factor. And we would like to point out that the share size can not be improved to better than $2^{n/2}$ with minor improvements. In the first step (Section 3.1), the monotone function computed by a circuit of size $\binom{n}{a} + \binom{n}{b}$ with a single call to a fat-slice function in $\mathfrak{F}_{[a,b]}$. To make sure the circuit size is smaller than $2^{n/2}$, we have to set $a \leq 11\%n$ and $b \geq 89\%n$. In the second step (Section 3.2), to make sure we did not sample more than $2^{n/2}$ partitions, we require the bucket size to be greater than 2, i.e. there are no more than $n/2$ buckets in each partition. In later steps, in order to have non-trivial saving, we require $b - a$ to be smaller than the number of buckets. As $89\%n - 11\%n > n/2$, such requirements can not be satisfied simultaneously.

Acknowledgments. The authors gratefully acknowledge delightful discussions with Hoeteck Wee that shaped our thinking about secret sharing. We thank the anonymous STOC 2018 reviewers for their insightful comments.

References

[Bei11] Amos Beimel. *Secret-Sharing Schemes: A Survey*, pages 11–46. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[BGK16] Andrej Bogdanov, Siyao Guo, and Ilan Komargodski. Threshold secret sharing requires a linear size alphabet. In *Theory of Cryptography - 14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part II*, pages 471–484, 2016.

[BI01] Amos Beimel and Yuval Ishai. On the power of nonlinear secret-sharing. In *Proceedings of the 16th Annual IEEE Conference on Computational Complexity, Chicago, Illinois, USA, June 18-21, 2001*, pages 188–202. IEEE Computer Society, 2001.

[BKN18] Amos Beimel, Eyal Kushilevitz, and Pnina Nissim. The complexity of multiparty PSM protocols and related models. *IACR Cryptology ePrint Archive*, 2018:148, 2018.

[BL88] Josh Cohen Benaloh and Jerry Leichter. Generalized secret sharing and monotone functions. In *Advances in Cryptology - CRYPTO '88, 8th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1988, Proceedings*, pages 27–35, 1988.

[Bla79] George Robert Blakley. Safeguarding cryptographic keys. In *Proc. AFIPS 1979 National Computer Conference*, pages 313–317, 1979.

[Csi97] László Csirmaz. The size of a share must be large. *J. Cryptology*, 10(4):223–231, 1997.

[GIKM00] 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.

[ISN89] Mitsuru Ito, Akira Saito, and Takao Nishizeki. Secret sharing scheme realizing general access structure. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 72(9):56–64, 1989.

[KM75] D. Kleitman and G. Markowsky. On dedekind's problem: The number of isotone boolean functions. ii. *Transactions of the American Mathematical Society*, 213:373–390, 1975.

[KN90] Joe Kilian and Noam Nisan. private communication. 1990.

[KW93] Mauricio Karchmer and Avi Wigderson. On span programs. In *Structure in Complexity Theory Conference*, pages 102–111. IEEE Computer Society, 1993.

[LVW17a] Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Conditional disclosure of secrets via non-linear reconstruction. In *CRYPTO Part I*, pages 758–790, 2017.

[LVW17b] Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Towards breaking the exponential barrier for general secret sharing. *IACR Cryptology ePrint Archive*, 2017.

[Sha79] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.