Lower Bounds for Secret-Sharing Schemes for k-Hypergraphs[*]

Amos Beimel
Department of Computer Science,
Ben-Gurion University of the Negev,
Beer-Sheva, Israel.
E-mail: amos.beimel@gmail.com

May 16, 2023

Abstract

A secret-sharing scheme enables a dealer, holding a secret string, to distribute shares to parties such that only pre-defined authorized subsets of parties can reconstruct the secret. The collection of authorized sets is called an access structure. There is a huge gap between the best known upper bounds on the share size of a secret-sharing scheme realizing an arbitrary access structure and the best known lower bounds on the size of these shares. For an arbitrary n-party access structure, the best known upper bound on the share size is $2^{O(n)}$. On the other hand, the best known lower bound on the total share size is much smaller, i.e., $\Omega(n^2/\log(n))$ [Csirmaz, *Studia Sci. Math. Hungar.*]. This lower bound was proved more than 25 years ago and no major progress has been made since.

In this paper, we study secret-sharing schemes for k-hypergraphs, i.e., for access structures where all minimal authorized sets are of size exactly k (however, unauthorized sets can be larger). We consider the case where k is small, i.e., constant or at most $\log(n)$. The trivial upper bound for these access structures is $O(n\cdot\binom{n-1}{k-1})$ and this can be slightly improved. If there were efficient secret-sharing schemes for such k-hypergraphs (e.g., 2-hypergraphs or 3-hypergraphs), then we would be able to construct secret-sharing schemes for arbitrary access structures that are better than the best known schemes. Thus, understanding the share size required for k-hypergraphs is important. Prior to our work, the best known lower bound for these access structures was $\Omega(n\log(n))$, which holds already for graphs (i.e., 2-hypergraphs).

We improve this lower bound, proving a lower bound of $\Omega(n^{2-1/(k-1)}/k)$ on the total share size for some explicit k-hypergraphs, where $3 \leq k \leq \log(n)$. For example, for 3-hypergraphs we prove a lower bound of $\Omega(n^{3/2})$. For $\log(n)$-hypergraphs, we prove a lower bound of $\Omega(n^2/\log(n))$, i.e., we show that the lower bound of Csirmaz holds already when all minimal authorized sets are of size $\log(n)$. Our proof is simple and shows that the lower bound of Csirmaz holds for a simple variant of the access structure considered by Csirmaz. Using our results, we prove a near quadratic separation between the required share size for realizing an explicit access structure and the monotone circuit size describing the access structure, i.e., the share size in $\Omega(n^2/\log(n))$ and the monotone circuit size is $O(n\log(n))$ (where the circuit has depth 3).

keywords. Secret Sharing, Share Size, Lower Bounds, Monotone Circuits.

[*]Research supported by ERC grant 742754 (project NTSC) and Israel Science Foundation grant no. 391/21.

1 Introduction

Secret-sharing schemes are a tool used in many cryptographic protocols. A secret-sharing scheme involves a dealer who has a secret, a set of n parties, and an access structure Γ – a collection of (authorized) subsets of the parties. A secret-sharing scheme for Γ is a method by which the dealer distributes strings (called shares) to the parties such that: (1) any subset in Γ can reconstruct the secret from its shares, and (2) any subset not in Γ cannot reveal any partial information on the secret. The share size of a scheme is the maximum share size in the scheme (i.e., the maximum length of the strings representing the shares). Originally motivated by the problem of secure information storage, secret-sharing schemes have found numerous other applications in cryptography, distributed computing, and complexity, e.g., Byzantine agreement [54], secure multiparty computations [13, 24, 26], threshold cryptography [36], access control [51], attribute-based encryption [42, 62], generalized oblivious transfer [56, 61], and proving NP-hardness of the partial minimum circuit size problem [43].

Secret-sharing schemes were introduced by Blakley [16] and Shamir [55] for the threshold case. Secret-sharing schemes for general access structures were introduced and constructed by Ito, Saito, and Nishizeki [44]. More efficient construction for specific families of access structure were given in [14, 57, 20, 45, 15, 17, 37]. For general n-party access structures, the share size in the schemes of [44] is 2^n; for 30 years no schemes with share size better than $2^{n-o(n)}$ were known. Liu and Vaikuntanathan [47], in a breakthrough paper, constructed for every access structure a secret-sharing scheme with share size $2^{0.994n}$. This was improved in a sequence of works [3, 5, 7], where the currently best known scheme has share size $(3/2)^{(1+o(1))n} < 2^{0.585n}$ [7]. The best known lower bound was proved by Csirmaz [28, 29], stating that, for every n, there is an n-party access structure such that sharing ℓ-bit secrets requires that the the total share size (i.e., the sum of sizes of the n shares) is $\Omega((n^2/\log(n)) \cdot \ell)$. The question if there exist more efficient schemes, or if there exist access structures that do not have (space) efficient schemes remains open.

In this paper, we consider a natural class of access structure – k-hypergraph access structures, in which the size of the minimal authorized sets is exactly k. Two-hypergraph access structures are called graph access structures and they have been studied extensively, e.g., [21, 22, 23, 38, 18, 30, 35, 31, 32, 10, 40, 33]. k-hypergraph access structures for $k > 2$ have also been studied previously (although not as much as graph secret sharing), e.g., [58, 60, 52, 27, 34, 10, 9]. The naive way to construct a secret-sharing scheme for a k-hypergraph is to share the secret independently for each minimal authorized set; this results in a scheme with total share size $k \cdot \binom{n}{k}$. A result of Erdös and Pyber [39] implies that every n-vertex graph can be realized by a secret-sharing scheme with ℓ-bit secrets and total share size $O((n^2/\log(n))\ell)$ (for secrets of size $\ell \geq \log(n)$). Using this result and Stinson's decomposition technique [59], every n-party k-hypergraph can be realized by a secret-sharing scheme with ℓ-bit secrets and total share size $O((\binom{n}{k}/\log(n)) \cdot \ell)$ (for secrets of size $\ell \geq k^4 \log(n)$ and for $k \leq n/2$) (see Remark 2.6). In contrast, the best known lower bound on the total share size in secret-sharing realizing a graph with an ℓ-bit secret is $\Omega(n \log(n)\ell)$ [38, 30]. Prior to our work, this was the best known lower bound for k-hypergraphs. Blundo et al. [18] showed a lower bound of $\Omega(n/\log(n) \cdot \ell)$ on the max share size for an access structure in which the size of the minimal authorized sets is *at most* $\log n$. In Table 1, we summarize the known upper bounds and lower bounds on the share size in secret-sharing schemes.

One reason for studying secret-sharing schemes for k-hypergraphs is that they can be used to construct secret-sharing schemes for arbitrary access structures. Every n-party access structure is a union of k-hypergraph access structures, thus, to construct more efficient secret-sharing

	Upper bound	Lower bounds
Arbitrary access structures	$O(2^{0.585n})$ [7]	$\Omega(n^2/\log(n))$ [29]
Graph access structures	$O(n^2/\log(n))$ [39]	$\Omega(n\log(n))$ [38, 30]
k-hypergraph access structures for $k \leq \log(n)$	$\binom{n}{k}\frac{k^2}{\log(n)}$	$\Omega(n^{2-1/(k-1)}/k)$ **[This paper]**

Table 1: Summary of known results on upper and lower bounds on the total share size for secret-sharing schemes.

schemes for arbitrary access structures, it suffices to construct efficient secret-sharing schemes for k-hypergraphs. Moreover, even if we have efficient secret-sharing schemes for k-hypergraphs for a small k, then, as described in the next lemma, for every access structure there is a secret-sharing scheme that is better than the best known secret-sharing schemes (the proof of the lemma for $k = 2$ appears in [53]; for completeness the proof of this lemma appears in Appendix A).

Lemma 1.1. *Assume that there exists constants k, c such that every N-party k-hypergraph access structure can be realized by a secret-sharing scheme with total share size $O(N^c)$. Then every n-party access structure can be realized by a secret-sharing scheme with total share size $\tilde{O}(2^{cn/k})$.*

Another reason for studying secret-sharing schemes for k-hypergraphs is that there were no improvements in their share size for more than two decades and the share size in the best known schemes for them is almost as big as the naive scheme for them. This should be compared with the new secret-sharing schemes for arbitrary access structures [47, 3, 5, 7] and the new CDS protocols and secret-sharing schemes for uniform access structures [11, 41, 48, 2, 49, 12, 1, 3]. Furthermore, k-hypergraph access structures resemble k-uniform access structures, in which all sets of size smaller than k are unauthorized, all sets of size larger than k are authorized, and some sets of size k are authorized and some are not. The best known share size for k-uniform access structure is $2^{\tilde{O}(\sqrt{k\log(n)})}$ [49, 3], i.e., it is much smaller than the best known share size for k-hypergraphs. It is interesting to understand if the difference in the share size is inherent.

1.1 Our Results

Our main result is a new lower bound on the share size in secret-sharing schemes for k-hypergraphs.

Theorem 1.2 (Informal)**.** *For every n, every $3 \leq k \leq \log(n)$, there is an explicit n-party k-hypergraph access structure such that for every secret length ℓ in every secret-sharing scheme realizing the access structure the total share size is at least $\Omega\left(\frac{n^{2-1/(k-1)}}{k}\cdot\ell\right)$.*

Our lower bound applies to k-partite hypergraph access structures, i.e., access structures in which the parties are partitioned to k parts and each minimal authorized set contains exactly one party from each part. k-partite hypergraph access structures are very useful, i.e., they are used in the proof of Lemma 1.1. The uniform access structure that are equivalent to CDS protocols are also k-partite.

For $k = 3$, we get a 3-partite hypergraph access structure that requires total share size $\Omega(n^{3/2} \cdot \ell)$. This implies that the applying Lemma 1.1 with $k = 3$ cannot result in a secret-sharing scheme with share size smaller than $2^{n/2}$. For $k = \log(n)$, we get a $\log(n)$-partite hypergraph access structure that requires total share size $\Omega((n^2/\log(n)) \cdot \ell)$, i.e., the best known lower bound on the share size.

For the interesting case of graph secret-sharing schemes, i.e., $k = 2$, our lower bound is $\Omega(n \cdot \ell)$; this is a trivial lower bound as Karnin et al. [46] proved that the size of the share of any non-redundant party is $\Omega(\ell)$. Improving the lower bound of $\Omega(n \log(n) \cdot \ell)$ for graph secret sharing, or constructing better schemes for graphs, is left as an open question.

We observe that the $\log(n)$-partite access structure for which we prove a lower bound of $O(n^2/\log(n))$ on the total share size can be described by a monotone *circuit* of size $O(n \log(n))$ and depth 3 (where we count the number of wires in the circuit). That is, we prove a near quadratic separation between the required share size and the monotone circuit size. In contrast, the size of the monotone *formula* describing an access structure is an upper bound on the share size required to realize the access structure [14]. Monotone *circuits* describing an access structure imply a computational secret-sharing scheme for the access structure [63];[1] our result raises the question if monotone circuits can be used to construct secret-sharing schemes with information-theoretic security.

To prove Theorem 1.2, we take the access structure used by Csirmaz in [28, 29] and transform it to a k-hypergraph access structure. The access structures that we construct to prove the lower bounds are quite simple. For example, for $k = 3$, we take two parts D_1, D_2 of size $\sqrt{n}$ and a third part D_3 of size $n - 2\sqrt{n}$; for every $a_1 \in D_1, a_2 \in D_2$ we take a distinct party $c_3 \in D_3$ and add the minimal authorized set $\{a_1, a_2, c_3\}$. See Figure 1 for an illustration of this construction.

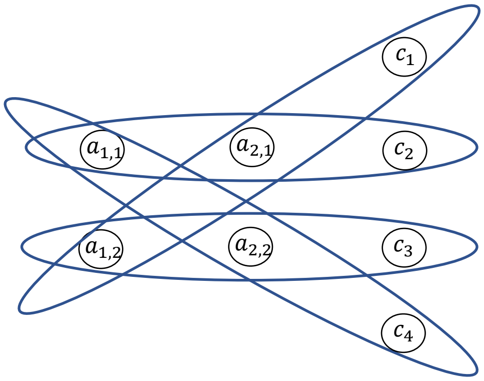

Figure 1: Illustration of the 3-partite hypergraph access structure 3-$\mathtt{CSI}^8$. The parties are $\{a_{1,1}, a_{1,2}, a_{2,1}, a_{2,2}, c_1, c_2, c_3, c_4\}$ and the 4 minimal authorized sets are described by blue circles.

As explained above, the lower bound of Csirmaz [28, 29] of $\Omega((n^2/\log(n)) \cdot \ell)$ on the total size of shares for a some access structure is the best known lower bound on the share size in secret-sharing schemes. This lower bound was used to derive a separation between the size of monotone real formulas and the size of shares in secret-sharing schemes [6] and a separation between the size

[1] The size of the public information in this scheme is the number of wires in the monotone circuit and the size of each share is the security parameter.

of shares in information theoretic secret-sharing schemes and the size of shares in computational secret-sharing schemes [4]. Recently, in a work that inspired this work, it was used to prove exponential lower bounds on the size of the shares in *evolving* secret-sharing schemes [50]. The result we use to derive our lower bound (Theorem 3.2) was generalized by Blundo et al. [18] with the so-called independent sequence method. They constructed, using this method, an access structure in which the size of the minimal authorized sets is *at most* $\log n$ and the maximum share size is $\Omega((n/\log(n)) \cdot \ell)$.

2 Preliminaries

In this section, we define secret-sharing schemes realizing general access structures. We start by defining a secret-sharing scheme, which is a randomized mapping whose input is a string, called the secret, and output is the n strings, called shares.

Definition 2.1 (Secret-Sharing Schemes). *Let $\{p_1, \ldots, p_n\}$ be a set of parties. A* secret-sharing scheme *Π with domain of secrets S is a* randomized *mapping from S to a set of n-tuples $S_1 \times S_2 \times \cdots \times S_n$, where S_j is called the* domain of shares *of p_j, that is, given a secret $s \in S$, the secret-sharing scheme outputs the shares $\mathsf{sh}_1, \ldots, \mathsf{sh}_n$. For a set $A \subseteq \{p_1, \ldots, p_n\}$, we denote $\Pi_A(s)$ as the restriction of $\Pi(s)$ to its A-entries, i.e. $\langle \mathsf{sh}_i \rangle_{p_i \in A}$.*

Informally, in a secret-sharing scheme, we consider a dealer that distributes a secret $s \in S$ according to Π by first sampling a vector of *shares* $\langle \mathsf{sh}_1, \ldots, \mathsf{sh}_n \rangle \leftarrow \Pi(s)$, and privately communicating each share sh_j to party p_j.

Definition 2.2 (Access Structures). *Let $\{p_1, \ldots, p_n\}$ be a set of parties. A collection $\Gamma \subseteq 2^{\{p_1,\ldots,p_n\}}$ is* monotone *if $B \in \Gamma$ and $B \subseteq C$ imply that $C \in \Gamma$. An* access structure *is a monotone collection $\Gamma \subseteq 2^{\{p_1,\ldots,p_n\}}$ of non-empty subsets of $\{p_1, \ldots, p_n\}$. Sets in Γ are called* authorized*, and sets not in Γ are called* unauthorized.

We next define the correctness and perfect security of a secret-sharing scheme realizing a general access structure; we require that such scheme is secure against an unbounded adversary, i.e., its security is information-theoretic. The definition is based on [25, 8] and does not assume any probability distribution on the secrets.

Definition 2.3 (Secret-Sharing Schemes Realizing an Access Structure). *Let S be a finite set of secrets, where $|S| \geq 2$. A secret-sharing scheme Π with domain of secrets S realizes an access structure Γ if the following two requirements hold:*

Perfect Correctness. *The secret s can be reconstructed by any authorized set of parties. That is, for any set $B \in \Gamma$ (where $B = \{p_{i_1}, \ldots, p_{i_{|B|}}\}$), there exists a* reconstruction function *$\mathsf{Recon}_B : S_{i_1} \times \cdots \times S_{i_{|B|}} \to S$ such that for every $s \in S$,*

$$\Pr[\, \mathsf{Recon}_B(\Pi_B(s)) = s \,] \quad = \quad 1. \tag{1}$$

Perfect Security. *Every unauthorized set cannot learn anything about the secret (in the information theoretic sense) from their shares. Formally, for any set $T \notin \Gamma$, for every two secrets $s_1, s_2 \in S$, and for every possible vector of shares $\langle \mathsf{sh}_j \rangle_{p_j \in T}$:*

$$\Pr[\, \Pi_T(s_1) = \langle \mathsf{sh}_j \rangle_{p_j \in T} \,] \quad = \quad \Pr[\, \Pi_T(s_2) = \langle \mathsf{sh}_j \rangle_{p_j \in T} \,], \tag{2}$$

where the probabilities are over the randomness of Π.

The most important complexity measure that we study in secret-sharing schemes in the share size.

Definition 2.4 (Share Size)**.** *The size of the secret in a secret-sharing scheme* Π *with domain of secrets* S *and domains of shares* $S_1, \cdots, S_n$ *is* $\log(|S|)$*, the share size of party* p_i *is* $\log(|S_i|)$*, the* max *share size is* $\max_{1 \leq j \leq n} \log(|S_j|)$*, and the* total *share size is* $\sum_{1 \leq j \leq n} \log(|S_j|)$*.*

Definition 2.5. *An access structure* Γ *is a* k*-hypergraph access structure (also called* k*-homogeneous access structure) if the size of every minimal authorized set in* $A \in \Gamma$ *is* exactly k*. An access structure* Γ *is a* k*-partite hypergraph access structure if there exists a partition of the set of parties to* k *sets* $D_1, \ldots, D_k$ *such that every minimal authorized set* $A \in \Gamma$ *contains exactly one party from each* D_i*, that is* $|A \cap D_i| = 1$ *for every* $1 \leq i \leq k$*.*

Note that that the size of unauthorized sets in a k-hypergraph access structure can be much larger that k. For example, in a graph access structure (i.e., in a 2-hypergraph access strucure), the minimal authorized sets are the edges of the graph and the unauthorized sets are independent sets.

Remark 2.6. Erdös and Pyber [39] have proved that every graph can be partitioned into complete bipartite graphs such that each vertex is contained in at most $O(n/\log(n))$ complete bipartite graphs. Blundo et al. [19] observed that this implies that for every n-vertex graph there is a secret-sharing realizing the graph with 1-bit secret, max share size $O(n/\log(n))$, and, in particular, total share size $O(n^2/\log(n))$.

This secret-sharing scheme can be used to construct a secret-sharing scheme for k-hypergraphs as follows. Given a k-hypergraph Γ with a set of parties P, define for every set of parties A of size exactly $k-2$ an access structure $\Gamma_A = \{B \subseteq P \setminus A : A \cup B \in \Gamma\}$. Notice that Γ_A is a graph access structure. We independently share the secret s for each access structure Γ_A, that is, we independently choose $k-2$ random bits $r_1, \ldots, r_{k-2}$, give each bit to a party in A, and share $s \oplus r_1 \oplus \cdots \oplus r_{k-2}$ using a graph secret-sharing for the graph access structure Γ_A. The total share in this scheme is $O\left(\binom{n}{k-2}\frac{n^2}{\log(n)}\right)$; this expression is equal to $O\left(\binom{n}{k}\frac{k^2}{\log(n)}\right)$ for $k \leq n/2$. Observe that each minimal authorized set (of size k) is an authorized set in $\binom{k}{2}$ access structures Γ_A. Thus, we can use Stinson's decomposition [59] to construct a secret-sharing scheme realizing Γ with ℓ-bit secrets, where $\ell > k^4 \log(n)$, and total share size $O\left(\binom{n}{k}\frac{1}{\log(n)} \cdot \ell\right)$.

3 Lower Bounds on the Size of the Shares in k-Partite Hypergraph Access Structures

Lower bounds for secret-sharing schemes have been proved in, e.g., [46, 23, 19, 38, 28, 29, 18]. The best lower bound was proved by Csirmaz [28, 29], who proved that for every n there exists an explicit n-party access structure such that every secret-sharing scheme realizing it with an ℓ-bit secret requires total share size $\Omega(n^2/\log(n) \cdot \ell)$. We use this lower bound to prove lower bounds for k-partite hypergraphs. We do this in two stages, we first define in Definition 3.3 a k-partite access structure in which the max share size is $\Omega\left(n^{1-1/(k-1)}\ell/k\right)$ and then define in Definition 3.7 a k-partite access structure in which the total share size is $\Omega\left(n^{2-1/(k-1)}\ell/k\right)$.

3.1 A Lower Bound on the Max Share Size

We first define a family of access structures $\texttt{CSI}$; access structures from this family were used by Csirmaz [28] to prove his lower bound. Each access structure in the family is defined by a given sequence of subsets satisfying the following condition: we say that a sequence of subsets $A_1, A_1, \dots, A_m$ is valid if $A_i \not\subseteq A_j$ for every $i < j$ (e.g., $|A_i| \geq |A_{i+1}|$ for $1 \leq i \leq m$).

Definition 3.1 ([28]). *Let A be a set and $A_1, A_2, \dots, A_m$ be a valid sequence of subsets of A. Furthermore, let $B = \{b_1, \dots, b_m\}$ and define $B_i = \{b_1, \dots, b_i\}$ for $1 \leq i \leq m$. We assume that $A \cap B = \emptyset$. Define the access structure $\texttt{CSI}^{A_1,\dots,A_m}$, whose parties are $A \cup B$ and the minimal authorized sets of $\texttt{CSI}^{A_1,\dots,A_m}$ are $A_1 \cup B_1, A_2 \cup B_2, \dots, A_m \cup B_m$.*

Theorem 3.2 ([28]). *For every valid sequence of subsets $A_1, A_2, \dots, A_m$ and every integer $\ell \in \mathbb{N}$, in every secret-sharing scheme realizing $\texttt{CSI}^{A_1,A_1,\dots,A_m}$ with domain of secrets $\{0,1\}^\ell$, the total share size of the parties A (i.e., $\sum_{p \in A} |\mathsf{sh}_p|$) is at least $(m-1) \cdot \ell$.*

Csirmaz considered the case in which $A = \{p_1, \dots, p_k\}$, $m = 2^k$, and $A_1 \dots, A_m$ is some valid ordering of all subsets of A. In this case the number of parties in the access structure is $n = O(2^k)$ and Theorem 3.2 implies that there is at least one party whose share size is $\Omega(2^k/|A|) = \Omega(n/\log(n))$. However, Csirmaz's proof applies to any access structure defined for a valid sequence. We will use larger sets A.

The main contribution of this paper is a construction of a k-hypergraph access structure k-$\texttt{CSI}^n$ from $\texttt{CSI}$; this access structure requires long shares. An illustration of the 3-$\texttt{CSI}^8$ access structure appears in Figure 1.

Definition 3.3 (The Access Structure k-$\texttt{CSI}^n$). *Fix k, n and let t be the maximal number such that $(k-1) \cdot t + t^{k-1} \leq n$. Let $D_i = \{a_{i,1}, \dots, a_{i,t}\}$ for $1 \leq i \leq k-1$, $A = \cup_{i=1}^{k-1} D_i$, $m = t^{k-1}$, and $A_1, \dots, A_m$ be any ordering of the subsets of A of size $k-1$ that contain exactly one element from each D_i (that is, $|A_j \cap D_i| = 1$ for every $1 \leq j \leq m, 1 \leq i \leq k-1$). Finally, let $C = \left\{c_1, \dots, c_{n-(k-1)\cdot t}\right\}$. Define the access structure k-$\texttt{CSI}^n$, whose parties are $A \cup C$ and the minimal sets of k-$\texttt{CSI}^n$ are $A_1 \cup \{c_1\}, A_2 \cup \{c_2\}, \dots, A_m \cup \{c_m\}$.*

Every minimal authorized set in k-$\texttt{CSI}^n$ contains exactly one party from each part $D_1, \dots, D_{k-1}, C$, i.e., there is a minimal authorized set $\left\{a_{1,j_1}, a_{2,j_2}, \dots, a_{k-1,j_{k-1}}, c_j\right\}$ for every sequence $(j_1, j_2, \dots, j_{k-1}) \in [t]^{k-1}$ and the appropriate j.

Remark 3.4. To define an access structure with exactly n parties, we added the redundant parties $c_{m+1}, \dots, c_{n-(k-1)\cdot t}$. These parties do not belong to any minimal authorized set and they can be ignored.

Theorem 3.5. *For every n, every $k \leq \log(n)$, every $\ell \in \mathbb{N}$, in every secret-sharing scheme realizing the n-party k-hypergraph access structure k-$\texttt{CSI}^n$ with domain of secrets $\{0,1\}^\ell$, the total share size of the parties in A is $\Omega(n \cdot \ell)$, in particular, there is at least one party with share size $\Omega\left(\frac{n^{1-1/(k-1)}}{k} \cdot \ell\right)$.*

Proof. Consider any secret-sharing scheme Π realizing k-$\texttt{CSI}^n$ with domain of secrets $\{0,1\}^\ell$. We construct from it a secret-sharing Π' realizing $\texttt{CSI}^{A_1,\dots,A_m}$ (where $A_1, \dots, A_m$ are all the subsets of A that contain exactly one party from each D_i) such that the share of each $a_{i,j}$ is the same in both schemes.

The construction of Π' is as follows:

- Share the secret using the scheme Π. Let $\mathsf{sh}^a_{i,j}$ be the share of $a_{i,j}$ for $1 \leq i \leq k-1, 1 \leq j \leq t$ and sh^c_i be the share of c_i for $1 \leq i \leq m$.
- For $1 \leq i \leq m$, share sh^c_i using an i-out-of-i secret-sharing scheme. Denote the shares by $\mathsf{sh}^c_{i,j}$ for $1 \leq j \leq i$.
- The share of $a_{i,j}$ is $\mathsf{sh}^a_{i,j}$ and the share of b_j is $\mathsf{sh}^c_{i,j}$ for $j \leq i \leq m$.

Any authorized set $A_i \cup B_i \in \mathtt{CSI}^{A_1,\dots,A_m}$ holds in Π' the shares of A_i and can reconstruct the share sh^c_i, hence the parties in $A_i \cup B_i$ can reconstruct the secret. Next we argue that the scheme Π' is secure. Consider an unauthorized set $T' \notin \mathtt{CSI}^{A_1,\dots,A_m}$ and let $j \leq m$ be the minimal index such that $b_j \notin T'$; if such index does not exist set $j = m+1$. Define $T = (T' \cap A) \cup \{c_1, \dots, c_{j-1}\}$. Since $T' \notin \mathtt{CSI}^{A_1,\dots,A_m}$ and $\{b_1, \dots, b_{j-1}\} \subseteq T'$, it must be that $A_i \not\subseteq T'$ for every $i \leq j-1$. This implies that $T \notin k\text{-}\mathtt{CSI}^n$. By the properties of the i-out-of-i secret-sharing scheme, the parties in T' have no information on sh^c_i for $i \geq j$. I.e., the parties in T' only have the shares of the unauthorized set T in Π and get no information on the secret.

We next analyze the lower bound on the share size that we get. By the choice of the parameters in $k\text{-}\mathtt{CSI}^n$, we get that $t^{k-1} = m = \Theta(n)$ and $|A| = (k-1) \cdot t = (k-1)\Omega(n^{1/(k-1)})$. By Theorem 3.2, the total share size of the parties in A in Π', hence also in Π, is $\Omega(m \cdot \ell) = \Omega(n \cdot \ell)$, in particular, there exists a party $p \in A$ whose share size in Π is

$$\Omega\left(\frac{n}{|A|} \cdot \ell\right) = \Omega\left(\frac{n}{(k-1)n^{1/(k-1)}} \cdot \ell\right).$$

□

Remark 3.6. We proved the lower bound by using Theorem 3.2 as a black-box. An alternative proof for Theorem 3.5 can directly apply the information inequalities as in the proof of [28].

3.2 A Lower Bound on the Total Share Size

We next construct a k-partite hypergraph access structure $k\text{-}\mathtt{TotCSI}^n$ that requires large *total* share size. The construction is similar to the construction of Csirmaz [29], who showed how to construct an access structure requiring total share size $\Omega(n^2/\log(n) \cdot \ell)$; to show a small monotone circuit for this access structure, we use a variant of [4] of this construction. Recall that in the access structure $k\text{-}\mathtt{CSI}^n$ there is a small set A, whose total share size is large. To construct $k\text{-}\mathtt{TotCSI}^n$, we will take many copies of the access structure $k\text{-}\mathtt{CSI}^n$ using the same set C, i.e., we only use many copies of the set A. Since the set A is small, the number of parties in $k\text{-}\mathtt{TotCSI}^n$ will be small. On the other hand, we have many copies of the set A, each copy requires large share size, hence the *total* share size is large. Specifically, we take $\alpha = O(n/(k \cdot t))$ copies of each party in A and for each minimal authorized set $A_j \cup \{c_j\}$ in $k\text{-}\mathtt{CSI}^n$ we take α^{k-1} minimal authorized sets in $k\text{-}\mathtt{TotCSI}^n$ by replacing each party a^1_{i,j_i} in A_j by each a^h_{i,j_i}.

Definition 3.7 (The Access Structure $k\text{-}\mathtt{TotCSI}^n$)**.** *Fix k, n, take t as the maximal integer such that $t^{k-1} \leq n/2$, and let $m = t^{k-1}$ and $\alpha = \lfloor n/(2(k-1) \cdot t) \rfloor$. For every $1 \leq h \leq \alpha$, let $D^h_i = \left\{a^h_{i,1}, \dots, a^h_{i,t}\right\}$ for $1 \leq i \leq k-1$, $A^h = \cup_{i=1}^{k-1} D^h_i$, and $A_1, \dots, A_m$ be any ordering of the subsets of A^1 of size $k-1$ that contain exactly one element from each D^1_i (that is, $|A_j \cap D^1_i| = 1$ for every $1 \leq j \leq m, 1 \leq i \leq k-1$). Furthermore, let $A = \cup_{1 \leq h \leq \alpha} A^h$ and let $C = \left\{c_1, \dots, c_{n-|A|}\right\}$.*

Define the access structure k-$\texttt{TotCSI}^n$, whose parties are $A \cup C$ and for every $1 \le j \le m$ we have the following α^{k-1} minimal authorized sets in k-$\texttt{TotCSI}^n$: Let $A_j = \left\{a^1_{1,j_1}, \dots, a^1_{k-1,j_{k-1}}\right\}$ for a sequence $(j_1, \dots, j_{k-1}) \in [t]^{k-1}$; for every sequence $h_1, \dots, h_{k-1} \in [\alpha]^{k-1}$ the set $\left\{a^{h_1}_{1,j_1}, \dots, a^{h_{k-1}}_{k-1,j_{k-1}}, c_j\right\}$ is a minimal authorized set in k-$\texttt{TotCSI}^n$.

Note that k-$\texttt{TotCSI}^n$ is a k-partite hypergraph access structure, where the parts are $\cup_{h=1}^{\alpha} D_1^h$, $\dots$, $\cup_{h=1}^{\alpha} D_{k-1}^h, C$. The access structure has $(t \cdot \alpha)^{k-1}$ minimal authorized sets.

Theorem 3.8. *For every n, every $k \le \log(n)$, every integer $\ell \in \mathbb{N}$, in every secret-sharing scheme realizing the n-party k-hypergraph access structure k-$\texttt{TotCSI}^n$ with domain of secrets $\{0,1\}^{\ell}$, the total share size is at least $\Omega\left(\frac{n^{2-1/(k-1)}}{k} \cdot \ell\right)$.*

Proof. For every $1 \le h \le \alpha$, the access structure k-$\texttt{TotCSI}^n$ restricted to the parties in $A^h \cup \{c_1, \dots, c_{t^{k-1}}\}$ is isomorphic to k-$\texttt{CSI}^{n'}$, where $n' = (k-1)t + t^{k-1} = \Theta(n)$. Thus, by Theorem 3.5, in any secret-sharing scheme realizing k-$\texttt{TotCSI}^n$ the total share size of the parties in A^h is $\Omega(n \cdot \ell)$, hence the total share size of the parties in A is

$$\Omega(\alpha n \cdot \ell) = \Omega\left(\frac{n^2}{k \cdot t} \cdot \ell\right) = \Omega\left(\frac{n^2}{k \cdot n^{1/(k-1)}} \cdot \ell\right).$$

□

3.3 Secret Sharing vs. Monotone Circuits

We next observe that the access structure $\log(n)$-$\texttt{TotCSI}^n$ can be described by a shallow monotone circuit of size $O(n \log(n))$; that is, we derive an almost quadratic separation between the total share size required in any secret-sharing scheme realizing k-$\texttt{TotCSI}^n$ and the size of the monotone circuit for it.

Theorem 3.9. *The access structure* $\log(n)$-$\texttt{TotCSI}^n$ *can be described by a monotone circuit of size $O(n \log(n))$ and depth 3.*

Proof. The access structure $\log(n)$-$\texttt{CSI}^{n'}$, where $t = 2$ and $n' = (\log(n) - 1)2 + 2^{\log(n)-1} = \Theta(n)$ has $2^{\log(n)-1} = n/2$ minimal authorized sets of size $\log(n)$, thus it can be described by a monotone CNF formula F of size $O(n \log(n))$;[2] denote the variables of this formula by $\{a_{i,j_i}\}_{i \in [\log(n)-1], j_i \in [t]} \cup \left\{c_1, \dots, c_{n/2}\right\}$. For every $i \in [\log(n) - 1], j_i \in [t]$, we compute $\wedge_{h \in [\alpha]} a^h_{i,j_i}$ and connect this AND gate to each leaf in F labeled by a_{i,j_i}. The resulting monotone circuit describes the access structure $\log(n)$-$\texttt{TotCSI}^n$. The size of the circuit is $O(n \log(n) + \alpha(\log(n) - 1)2) = O(n \log(n))$ and its depth is 3. □

Acknowledgment. I would like to thank Noam Mazor for telling me about his result [50]; this result inspired this work. I would also like to thank Eran Omri and Oriol Farràs for helpful discussions.

[2] It can also be described by a monotone formula of size $O(n)$ and depth $O(\log(n))$.

References

[1] Benny Applebaum and Barak Arkis. On the power of amortization in secret sharing: d-uniform secret sharing and CDS with constant information rate. In *TCC 2018*, volume 11239 of *LNCS*, pages 317–344, 2018.

[2] Benny Applebaum, Barak Arkis, Pavel Raykov, and Prashant Nalini Vasudevan. Conditional disclosure of secrets: Amplification, closure, amortization, lower-bounds, and separations. In *CRYPTO 2017*, volume 10401 of *LNCS*, pages 727–757, 2017.

[3] Benny Applebaum, Amos Beimel, Oriol Farràs, Oded Nir, and Naty Peter. Secret-sharing schemes for general and uniform access structures. In *EUROCRYPT 2019*, volume 11478 of *LNCS*, pages 441–471, 2019.

[4] Benny Applebaum, Amos Beimel, Yuval Ishai, Eyal Kushilevitz, Tianren Liu, and Vinod Vaikuntanathan. Succinct computational secret sharing. In *55th STOC*, pages 1553–1566, 2023.

[5] Benny Applebaum, Amos Beimel, Oded Nir, and Naty Peter. Better secret sharing via robust conditional disclosure of secrets. In *52nd STOC*, pages 280–293, 2020.

[6] Benny Applebaum, Amos Beimel, Oded Nir, Naty Peter, and Toniann Pitassi. Secret sharing, slice formulas, and monotone real circuits. In *ITCS 2022*, volume 215 of *LIPIcs*, pages 8:1–8:23, 2022.

[7] Benny Applebaum and Oded Nir. Upslices, downslices, and secret-sharing with complexity of 1.5^n. In *CRYPTO 2021*, volume 12827 of *LNCS*, pages 627–655, 2021.

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

[9] Amos Beimel and Oriol Farràs. The share size of secret-sharing schemes for almost all access structures and graphs. *IACR Cryptol. ePrint Arch.*, 2020:664, 2020. Conference version in TCC 2020, volume 12552 of LNCS, pages 499–529, 2020.

[10] Amos Beimel, Oriol Farràs, and Yuval Mintz. Secret-sharing schemes for very dense graphs. *J. of Cryptology*, 29(2):336–362, 2016.

[11] Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. In *TCC 2014*, volume 8349 of *LNCS*, pages 317–342, 2014.

[12] Amos Beimel and Naty Peter. Optimal linear multiparty conditional disclosure of secrets protocols. In *ASIACRYPT 2018*, volume 11274 of *LNCS*, pages 332–362, 2018.

[13] Michael Ben-Or, Shaffi Goldwasser, and Avi Wigderson. Completeness theorems for noncryptographic fault-tolerant distributed computations. In *20th STOC*, pages 1–10, 1988.

[14] Josh Cohen Benaloh and Jerry Leichter. Generalized secret sharing and monotone functions. In *CRYPTO '88*, volume 403 of *LNCS*, pages 27–35, 1988.

[15] Michael Bertilsson and Ingemar Ingemarsson. A construction of practical secret sharing schemes using linear block codes. In *AUSCRYPT '92*, volume 718 of *LNCS*, pages 67–79, 1992.

[16] George Robert Blakley. Safeguarding cryptographic keys. In *Proc. of the 1979 AFIPS National Computer Conference*, volume 48, pages 313–317, 1979.

[17] George Robert Blakley and Grigory A. Kabatianskii. Linear algebra approach to secret sharing schemes. In *Error Control, Cryptology, and Speech Compression*, volume 829 of *LNCS*, pages 33–40. Springer, 1994.

[18] Carlo Blundo, Alfredo De Santis, Roberto De Simone, and Ugo Vaccaro. Tight bounds on the information rate of secret sharing schemes. *Des. Codes Cryptography*, 11(2):107–122, 1997.

[19] Carlo Blundo, Alfredo De Santis, Luisa Gargano, and Ugo Vaccaro. On the information rate of secret sharing schemes. *Theoretical Computer Science*, 154(2):283–306, 1996.

[20] Ernest F. Brickell. Some ideal secret sharing schemes. *Journal of Combin. Math. and Combin. Comput.*, 6:105–113, 1989.

[21] Ernest F. Brickell and Daniel M. Davenport. On the classification of ideal secret sharing schemes. *J. of Cryptology*, 4(73):123–134, 1991.

[22] Ernest F. Brickell and Douglas R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *J. of Cryptology*, 5(3):153–166, 1992.

[23] Renato M. Capocelli, Alfredo De Santis, Luisa Gargano, and Ugo Vaccaro. On the size of shares for secret sharing schemes. *J. of Cryptology*, 6(3):157–168, 1993.

[24] David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols. In *20th STOC*, pages 11–19, 1988.

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

[26] Ronald Cramer, Ivan Damgård, and Ueli Maurer. General secure multi-party computation from any linear secret-sharing scheme. In *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 316–334, 2000.

[27] Giovanni Di Crescenzo and Clemente Galdi. Hypergraph decomposition and secret sharing. In *14th ISAAC*, volume 2906 of *LNCS*, pages 645–654, 2003.

[28] László Csirmaz. The size of a share must be large. In *EUROCRYPT '94*, volume 950 of *LNCS*, pages 13–22, 1994.

[29] László Csirmaz. The dealer's random bits in perfect secret sharing schemes. *Studia Sci. Math. Hungar.*, 32(3–4):429–437, 1996.

[30] László Csirmaz. Secret sharing schemes on graphs. Technical Report 2005/059, Cryptology ePrint Archive, 2005.

[31] László Csirmaz. An impossibility result on graph secret sharing. *Des. Codes Cryptography*, 53(3):195–209, 2009.

[32] László Csirmaz. Secret sharing on the d-dimensional cube. *Des. Codes Cryptography*, 74(3):719–729, 2015.

[33] László Csirmaz and Péter Ligeti. Secret sharing on large girth graphs. *Cryptogr. Commun.*, 11(3):399–410, 2019.

[34] László Csirmaz, Péter Ligeti, and Gábor Tardos. Erdös-pyber theorem for hypergraphs and secret sharing. *Graphs and Combinatorics*, 31(5):1335–1346, 2014.

[35] László Csirmaz and Gábor Tardos. Optimal information rate of secret sharing schemes on trees. *IEEE Trans. Inf. Theory*, 59(4):2527–2530, 2013.

[36] Yvo Desmedt and Yair Frankel. Shared generation of authenticators and signatures. In *CRYPTO '91*, volume 576 of *LNCS*, pages 457–469, 1991.

[37] Marten van Dijk. A linear construction of perfect secret sharing schemes. In *EUROCRYPT '94*, volume 950 of *LNCS*, pages 23–34, 1995.

[38] Marten van Dijk. On the information rate of perfect secret sharing schemes. *Des. Codes Cryptography*, 6(2):143–169, 1995.

[39] Paul Erdös and László Pyber. Covering a graph by complete bipartite graphs. *Discrete Mathematics*, 170(1–3):249–251, 1997.

[40] Oriol Farràs, Tarik Kaced, Sebastià Martín, and Carles Padró. Improving the linear programming technique in the search for lower bounds in secret sharing. In *EUROCRYPT 2018*, LNCS, pages 597–621, 2018.

[41] Romain Gay, Iordanis Kerenidis, and Hoeteck Wee. Communication complexity of conditional disclosure of secrets and attribute-based encryption. In *CRYPTO 2015*, volume 9216 of *LNCS*, pages 485–502, 2015.

[42] Viput Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *13th CCS*, pages 89–98, 2006.

[43] Shuichi Hirahara. NP-hardness of learning programs and partial MCSP. In *63rd FOCS*, pages 968–979, 2022.

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

[45] Mauricio Karchmer and Avi Wigderson. On span programs. In *8th Structure in Complexity Theory*, pages 102–111, 1993.

[46] Ehud D. Karnin, Jonathan W. Greene, and Martin E. Hellman. On secret sharing systems. *IEEE Trans. on Information Theory*, 29(1):35–41, 1983.

[47] Tianren Liu and Vinod Vaikuntanathan. Breaking the circuit-size barrier in secret sharing. In *50th STOC*, pages 699–708, 2018.

[48] Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Conditional disclosure of secrets via non-linear reconstruction. In *CRYPTO 2017*, volume 10401 of *LNCS*, pages 758–790, 2017.

[49] Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Towards breaking the exponential barrier for general secret sharing. In *EUROCRYPT 2018*, volume 10820 of *LNCS*, pages 567–596, 2018.

[50] Noam Mazor. A lower bound on the share size in evolving secret sharing. *Electron. Colloquium Comput. Complex.*, TR23-013, 2023. `arXiv:TR23-013`.

[51] Moni Naor and Avishai Wool. Access control and signatures via quorum secret sharing. *IEEE Transactions on Parallel and Distributed Systems*, 9(1):909–922, 1998.

[52] Carles Padró and Germán Sáez. Lower bounds on the information rate of secret sharing schemes with homogeneous access structure. *Inform. Process. Lett.*, 83(6):345–351, 2002.

[53] Naty Peter. *Secret-Sharing Schemes and Conditional Disclosure of Secrets Protocols*. PhD thesis, Ben-Gurion University of the Negev, 2020. `https://primo.bgu.ac.il/permalink/972BGU_INST/23v028/alma9926575584104361`.

[54] Michael O. Rabin. Randomized Byzantine generals. In *24th FOCS*, pages 403–409, 1983.

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

[56] Bhavani Shankar, Kannan Srinathan, and C. Pandu Rangan. Alternative protocols for generalized oblivious transfer. In *9th ICDCN*, volume 4904 of *LNCS*, pages 304–309, 2008.

[57] Gustavus J. Simmons, Wen-Ai Jackson, and Keith M. Martin. The geometry of shared secret schemes. *Bulletin of the ICA*, 1:71–88, 1991.

[58] Douglas R. Stinson. New general lower bounds on the information rate of secret sharing schemes. In *CRYPTO '92*, volume 740 of *LNCS*, pages 168–182, 1993.

[59] Douglas R. Stinson. Decomposition construction for secret sharing schemes. *IEEE Trans. on Information Theory*, 40(1):118–125, 1994.

[60] Hung-Min Sun and Shiuh-Pyng Shieh. Constructing perfect secret sharing schemes for general and uniform access structures. *J. Inf. Sci. Eng.*, 15(5):679–689, 1999.

[61] Tamir Tassa. Generalized oblivious transfer by secret sharing. *Des. Codes Cryptography*, 58(1):11–21, 2011.

[62] Brent Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *PKC 2011*, volume 6571 of *LNCS*, pages 53–70, 2011.

[63] Andrew Chi-Chih Yao. Unpublished manuscript, 1989. Presented at Oberwolfach and DIMACS workshops.

A A Secret-Sharing Scheme for an Arbitrary Access Structure from a Secret-Sharing Scheme for k-Hypergraph

We next describe a simple reduction from realizing an arbitrary access structure to realizing k-hypergraphs. Given an access structure Γ with parties $p_1, \ldots, p_n$ we define the following k-hypergraph access structure Γ_k with $k \cdot N$ vertices, where $N = 2^{n/k}$ (for simplicity assume that n/k is an integer):

- Let $P_i = \left\{p_{(i-1)\cdot n/k+1}, \ldots, p_{i\cdot n/k}\right\}$ for $1 \le i \le k$, $D_i = 2^{P_i}$, and $D = \cup_{i=1}^{k} D_i$. The parties in Γ_k are D, i.e., each party in Γ_k is a subset of the parties in Γ.[3]
- For every minimal authorized set A in Γ, the set
$$\{A \cap P_1, \ldots, A \cap P_k\}$$
is a minimal authorized set in Γ_k.

An illustration of a construction of such access structure for $k = 2$ appears in Figure 2.

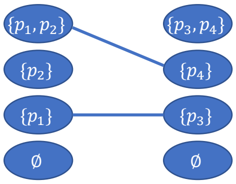

Figure 2: The access structure Γ_2 constructed from the access structure with two minimal authorized sets $\{p_1, p_3\}$ and $\{p_1, p_2, p_4\}$. The minimal authorized sets of Γ_2 are described by an edge.

The secret-sharing Π for Γ is as follows:

- Construct the above hypergraph access structure Γ_k from the access structure Γ.
- Share the secret s using any secret-sharing scheme Π_k for Γ_k. Let sh_C be the share in this scheme of the vertex $C \in D$.
- For every non-empty set $C \in D$, independently share sh_C using a $|C|$-out-of-$|C|$ secret-sharing scheme among the parties of C. In addition, give the shares of $\emptyset \in D_i$ for each $1 \le i \le k$ to all parties in Γ.

We next argue the correctness and security of the scheme. First, let $A = A_1 \cup \cdots \cup A_k$ be a minimal authorized set in Γ, where $A_i \subseteq P_i$ for every $1 \le i \le k$. By the construction of Γ_k, the set $\{A_1, \ldots, A_k\}$ is an authorized set in Γ_k, thus $\mathsf{sh}_{A_1}, \ldots, \mathsf{sh}_{A_k}$ determine the secret. Furthermore, the parties in A can reconstruct $\mathsf{sh}_{A_1}, \ldots, \mathsf{sh}_{A_k}$, hence, can reconstruct the secret.

For the security of the scheme, consider an unauthorized set $T = T_1 \cup \cdots \cup T_k \notin \Gamma$, where $T_i \subseteq P_i$ for every $1 \le i \le k$. Clearly, the parties in T can reconstruct sh_{T_i} for every $1 \le i \le k$; however they can also reconstruct the shares of every subset of T_i. On the other hand, for any

[3] There is party for the empty set in each D_i. These are k distinct parties.

other set $B \in D$, the parties in T miss at least one party in B. Hence, the parties in T have no information of the shares of these sets.

Since T is unauthorized, every subset of T is unauthorized and for every $T'_1 \subseteq T_1, \dots, T'_k \subseteq T_k$, the set $\{T'_1, \dots, T'_k\}$ is unauthorized in Γ_k. Thus, the shares in Π_k that the parties in T can reconstruct are shares of an unauthorized set in Γ_k and these shares do not reveal any information on the secret s.

The total share size of the scheme Π is at most n times the total share size of the scheme Π', i.e., n times the share size required to realize a $(k \cdot 2^{n/k})$-party k-hypergraph.