A Lower Bound on the Share Size in Evolving Secret Sharing

Noam Mazor*

Abstract

Secret sharing schemes allow sharing a secret between a set of parties in a way that ensures that only authorized subsets of the parties learn the secret. *Evolving secret sharing* schemes (Komargodski, Naor, and Yogev [TCC '16]) allow achieving this end in a scenario where the parties arrive in an online fashion, and there is no a-priory bound on the number of parties.

An important complexity measure of a secret sharing scheme is the share size, which is the maximum number of bits that a party may receive as a share. While there has been a significant progress in recent years, the best constructions for both secret sharing and evolving secret sharing schemes have a share size that is exponential in the number of parties. On the other hand, the best lower bound, by Csirmaz [Eurocrypt '95], is sub-linear.

In this work, we give a tight lower bound on the share size of evolving secret sharing schemes. Specifically, we show that the sub-linear lower bound of Csirmaz implies an exponential lower bound on evolving secret sharing.

Keywords: Secret sharing, Evolving secret sharing

*The Blavatnik School of Computer Science at Tel-Aviv University. E-mail:{noammaz@gmail.com. Research supported by Israel Science Foundation grant 666/19.

1 Introduction

Secret sharing is a fundamental concept in cryptography, that allows a dealer to distribute a secret among a set of parties in a way that ensures that only *authorized* subsets of parties learn the secret. Such schemes are used in secure multi-party computation, amplification schemes for cryptographic primitives, Byzantine agreement protocols, and more (see [Bei11]). *Evolving secret sharing* (Komargodski, Naor, and Yogev [KNY17]) is a variant of secret sharing, that can be used in evolving systems, for which there is no a-priory bound on the number of parties. In such schemes, the dealer distributes the secret to an infinite number of parties in an online fashion: the parties arrive one by one, and each party receives its share of the secret as it arrives. The correctness guarantee promises that by the time the n-th party receives their share, all the authorized subsets among the first n parties can reconstruct the secret. Such a scheme is *adaptive* if the dealer does not need to know the entire access structure to give a share to a party. Rather, it is sufficient to know the list of authorized sets containing only parties that already arrived.

The main complexity measure of a secret sharing scheme is its share size: the maximal number of bits a party might receive as a share. While there have been significant advancements in the area in recent years ([LVW18; LV18; ABFNP19; ABNP20]), the best known constructions for (classical) secret sharing have exponential share size in the number of parties (Applebaum and Nir [AN21]). For the harder task of evolving secret sharing, the best construction for arbitrary access structure gives the i-th party share of size 2^{i-1} ([KNY17]).

Somewhat surprisingly, we do not know if exponential share size is the best possible, or even if the share size must be *super linear* in the number of parties. Indeed, the best known lower bound on (classical) secret sharing is due to Csirmaz [Csi97], which showed a specific access structure for which every scheme must give some party a share of size $\Omega(n/\log n)$. Thus, the optimal share size for arbitrary access structures is an important open question. Prior to this paper, this question was open also for the case of evolving secret sharing.

1.1 Our Result

In this work, we resolve the above question for the case of evolving secret sharing. We show that the linear lower bound of Csirmaz [Csi97] implies a tight exponential lower bound on evolving secret sharing. This is stated in the following two theorems. The first is for adaptive evolving secret sharing schemes.

Theorem 1.1 (Lower bound for adaptive schemes, informal)**.** *There exists an access structure $\mathcal{A}$ such that for every adaptive evolving secret sharing scheme and for every n, the total share size of the first n parties in $\mathcal{A}$ is at least 2^n. In particular, the share size of the i-th party is at least 2^{i-1} for infinitely many i's.*

As stated before, this lower bound is tight with the scheme of [KNY17] which gives the i-th party share of size 2^{i-1}. Interestingly, the access structure for which we prove this lower bound does not contain a single authorized set. We also prove the following slightly weaker lower bound, for a larger class of schemes, namely, non-adaptive schemes.

Theorem 1.2 (Lower bound for non-adaptive schemes, informal)**.** *There exists an access structure $\mathcal{A}$ such that the following holds. For every evolving secret sharing scheme for $\mathcal{A}$ and for every n, the total share size of the first n parties is at least $2^{n-o(n)}$. Moreover, the share size of the i-th party is at least $2^{i-o(i)}$ for infinitely many i's.*

The formal bound we prove (Theorem 3.2) is somewhat stronger, as we can choose the $o(n)$ term to be any super-constant. For example, Theorem 3.2 implies that the total share size of the first n parties is at least $2^{n-\log n}$. The proof of both theorems follows from an observation on [Csi97]'s lower bound. In his work, Csirmaz [Csi97] shows that in some access structure over n parties, there is a specific set of $t = \log n$ parties that must hold together at least n bits. We observe that if these t parties are the first to arrive, by [Csi97]'s lower bound they must hold exponential (in t) share size. See more details in Section 3.[1]

1.2 Additional Related Work

Lower bounds on secret sharing schemes. Besides the aforementioned lower bound of [Csi97], Csirmaz [Csi96] showed an access structure for which, the *total share size* must be quadratic. The construction is simply duplicating the parties with large shares in [Csi97]'s construction. Csirmaz [Csi97] also shows that a better lower bound on the share size cannot be proven using Shannon information inequalities. Beimel and Orlov [BO11] showed the same result for a larger set of information inequalities. Recently, Applebaum, Beimel, Nir, Peter, and Pitassi [ABNPP22] showed a connection between the known constructions of secret sharing and monotone real circuits, and used this connection to give a lower bound on a family of constructions. For evolving schemes, [KNY17] gave a tight lower bound for the special case of the 2-threshold access structure.

Constructions of evolving secret sharing schemes. Following Komargodski et al. [KNY17], Paskin-Cherniavsky [PC16] showed a more efficient construction for some classes of access structures. In this scheme, the dealer needs to know the access structure in advance. More efficient schemes are known for specific types of access structures ([CT12],[KNY17; KPC17]).

Paper Organization

Basic definitions and notations are given in Section 2, and the proofs of the lower bounds are given in Section 3.

2 Preliminaries

2.1 Notations

All logarithms are taken in base 2. We use calligraphic letters to denote sets and distributions, uppercase for random variables, and lowercase for values and functions. We use $[n]$ to denote the set $\{1, \ldots, n\}$. Given a vector $v \in \Sigma^n$, let v_i denote its i^{th} entry, let $v_{<i} = (v_1, \ldots, v_{i-1})$ and $v_{\leq i} = (v_1, \ldots, v_i)$. Similarly, for a set $\mathcal{I} \subseteq [n]$, let $v_{\mathcal{I}}$ be the ordered sequence $(v_i)_{i \in \mathcal{I}}$.

When unambiguous, we will naturally view a random variable as its marginal distribution. For a (discrete) distribution $\mathcal{D}$, let $x \leftarrow \mathcal{D}$ denote that x was sampled according to $\mathcal{D}$. Let $\text{Supp}(\mathcal{D}) = \{p \colon \Pr_{\mathcal{D}}[p] > 0\}$, and define $|\mathcal{D}| = \log(|\text{Supp}(\mathcal{D})|)$.

[1] We remark that, as in [Csi97], both of our bounds generalize to the *information-ratio* of the scheme. That is, the ratio between the total share size of the first n parties to the length of the secret must be exponential in n.

2.1.1 Entropy and Mutual Information

The *Shannon entropy* of a distribution $\mathcal{P}$ is defined by $H(\mathcal{P}) = \sum_{p \in \mathrm{Supp}(\mathcal{P})} \Pr_{\mathcal{P}}[p] \cdot \log \frac{1}{\Pr_{\mathcal{P}}[p]}$. The conditional entropy of a random variable A given B, is defined as $H(A \mid B) = \mathrm{E}_{b \leftarrow B}[H(A|_{B=b})]$. The mutual information between two random variables A and B is defined by

$$I(A;B) = H(A) - H(A \mid B) = H(B) - H(B \mid A)$$

and the conditional mutual information given a random variable C is defined similarly

$$I(A;B \mid C) = H(A \mid C) - H(A \mid B,C).$$

We will use the following well known facts:

Fact 2.1 (Chain rule for mutual information)**.** *For two random variables A and $B = (B_1, \ldots, B_n)$, it holds that $I(A;B) = \sum_{i=1}^{n} I(A;B_i \mid B_{<i})$.*

Fact 2.2 (Upper bound on mutual information)**.** *For two random variables A and B, it holds that $I(A;B) \leq |A|$.*

2.2 Secret Sharing Schemes.

We now formally define secret sharing schemes. Let $\mathcal{P}$ be a set of parties. An *access structure* is a monotone collection of subsets of $\mathcal{P}$.

Definition 2.3 (Access structure)**.** *A collection of sets $\mathcal{A} \subseteq 2^{\mathcal{P}}$ is an* access structure *if it is monotone: for every set $\mathcal{B} \in \mathcal{A}$ and for every $\mathcal{B}'$ such that $\mathcal{B} \subseteq \mathcal{B}' \subseteq \mathcal{P}$, it holds that $\mathcal{B}' \in \mathcal{A}$. A set $\mathcal{B}$ is* authorized *if $\mathcal{B} \in \mathcal{A}$, and* unauthorized *otherwise.*

An access structure can be defined by a set of minimal authorized sets. Given a (non-monotone) set $\mathcal{M}$ of subsets of parties, the induced access structure $\mathcal{A}_{\mathcal{M}}$ is received by adding to $\mathcal{A}_{\mathcal{M}}$ all the subsets contained a set in $\mathcal{M}$. That is, $\mathcal{A}_{\mathcal{M}} := \{\mathcal{B} \subseteq \mathcal{P} \colon \exists \mathcal{C} \in \mathcal{M} \ s.t. \ \mathcal{C} \subseteq \mathcal{B}\}$. We now ready to define secret sharing schemes.

Definition 2.4 (Secret sharing scheme)**.** *A* secret sharing scheme *for an access structure $\mathcal{A}$ is a pair of algorithms* $(\mathsf{SHARE}, \mathsf{RECON})$ *such that the following holds:*

1. *Given a secret $s \in \{0,1\}$, $\mathsf{SHARE}(s)$ returns shares $\pi = \{\pi_p\}_{p \in \mathcal{P}}$. π_p is called the share of party p.*
2. *Correctness: For every secret $s \in \{0,1\}$, $\pi \leftarrow \mathsf{SHARE}(s)$ and an authorized set $\mathcal{B} \in \mathcal{A}$, $\mathsf{RECON}(\mathcal{B}, \pi_{\mathcal{B}}) = s$.*
3. *Perfect Privacy: For every unauthorized set $\mathcal{B} \notin \mathcal{A}$, it holds that $\mathsf{SHARE}(0)_{\mathcal{B}} \equiv \mathsf{SHARE}(1)_{\mathcal{B}}$.*

2.3 Evolving Secret Sharing

We now formally define evolving secret sharing schemes, introduces by Komargodski et al. [KNY17].

Definition 2.5 (Restriction)**.** *Given an access structure $\mathcal{A}$ over $\mathcal{P}$, and a subset of parties $\mathcal{P}' \subseteq \mathcal{P}$, let $\mathcal{A}|_{\mathcal{P}'} := \{\mathcal{B} \in \mathcal{A} \colon \mathcal{B} \subseteq \mathcal{P}'\}$.*

[KNY17] showed that $\mathcal{A}|_{\mathcal{P}'}$ is an access structure for every $\mathcal{A}$ and $\mathcal{P}'$.

Definition 2.6 (Evolving access structure)**.** *Let $\mathcal{P} = \mathbb{N}$ be an infinite set of parties. An* evolving access structure over $\mathcal{P}$ *is a set of access structures $\{\mathcal{A}_n\}_{n\in\mathbb{N}}$ such that for every n, $\mathcal{A}_n$ is an access structure over $[n]$ and $\mathcal{A}_{n+1}|_{[n]} = \mathcal{A}_n$.*

For an evolving access structure $\mathcal{A}$ and a finite set of parties $\mathcal{I} \subseteq \mathcal{P}$, we use $\mathcal{A}|_{\mathcal{I}}$ to denote the access structure $\mathcal{A}_n|_{\mathcal{I}}$ for some n with $\mathcal{I} \subseteq [n]$. Notice that the set $\mathcal{A}_n|_{\mathcal{I}}$ is independent from the choice of such n (That is, $\mathcal{A}_n|_{\mathcal{I}} = \mathcal{A}_{n'}|_{\mathcal{I}}$ for every n and n' such that $\mathcal{I} \subseteq [n]$ and $\mathcal{I} \subseteq [n']$).

Definition 2.7 (Evolving secret sharing scheme)**.** *An* evolving secret sharing scheme *for an evolving access structure $\{\mathcal{A}_n\}_{n\in N}$ is a pair of algorithms* $(\mathsf{SHARE}, \mathsf{RECON})$ *such that the following holds for every n:*

1. *Given a secret $s \in \{0,1\}$ and sequence of shares $\pi_1, \ldots, \pi_{n-1}$, $\mathsf{SHARE}(s, \pi_1, \ldots, \pi_{n-1})$ returns a share π_n for party n. Denote by $\Pi^s = (\Pi^s_1, \Pi^s_2, \ldots)$ the distribution of the shares of the parties on secret s. That is, $\Pi^s_i = \mathsf{SHARE}(s, \Pi^s_1, \ldots, \Pi^s_{i-1})$.*
2. *Correctness: For every secret $s \in \{0,1\}$, shares $\pi = (\pi_1, \ldots, \pi_n) \leftarrow \Pi^s_{\leq n}$ and an authorized set $\mathcal{B} \in \mathcal{A}_n$, $\mathsf{RECON}(\mathcal{B}, \pi_{\mathcal{B}}) = s$.*
3. *Perfect Privacy: For every set $\mathcal{B} \subseteq [n]$ of parties with $\mathcal{B} \notin \mathcal{A}_n$, it holds that $\Pi^0_{\mathcal{B}} \equiv \Pi^1_{\mathcal{B}}$.*

Note that for every set $\mathcal{B} \subseteq [n]$ of parties with $\mathcal{B} \notin \mathcal{A}_n$, it holds that $\mathcal{B} \notin \mathcal{A}_k$ for every $k \in \mathbb{N}$.

An adaptive evolving secret sharing scheme is a secret sharing scheme that doesn't know the access structure in advance. In this definition, the algorithms SHARE and RECON get a description of the access structure.

Definition 2.8 (Adaptive evolving secret sharing scheme)**.** *An* adaptive evolving secret sharing scheme *is a pair of algorithms* $(\mathsf{SHARE}, \mathsf{RECON})$ *such that the following hold for every evolving access structure $\{\mathcal{A}_n\}_{n\in N}$ and for every n:*

1. *Given a secret $s \in \{0,1\}$, $\mathcal{A}_n$ and sequence of shares $\pi_1, \ldots, \pi_{n-1}$, $\mathsf{SHARE}(s, \mathcal{A}_n, \pi_1, \ldots, \pi_{n-1})$ returns a share π_n for party n. Denote by $\Pi^s = (\Pi^s_1, \Pi^s_2, \ldots)$ the distribution of the shares of the first n parties on secret s. That is, $\Pi^s_i = \mathsf{SHARE}(s, \mathcal{A}_i, \Pi^s_1, \ldots, \Pi^s_{i-1})$.*
2. *Correctness: For every secret $s \in \{0,1\}$, shares $\pi = (\pi_1, \ldots, \pi_n) \leftarrow \Pi^s_{\leq n}$ and an authorized set $\mathcal{B} \in \mathcal{A}_n$, $\mathsf{RECON}(\mathcal{B}, \mathcal{A}_n, \pi_B) = s$.*
3. *Perfect Privacy: For every set $\mathcal{B} \subseteq [n]$ of parties with $\mathcal{B} \notin \mathcal{A}_n$, it holds that $\Pi^0_{\mathcal{B}} \equiv \Pi^1_{\mathcal{B}}$.*

We now formally define the share size of a set of parties.

Definition 2.9 (Share size)**.** *For an evolving access structure $\mathcal{A} = \{\mathcal{A}_n\}_{n\in N}$, an adaptive scheme* $(\mathsf{SHARE}, \mathsf{RECON})$*, and $S \leftarrow \{0,1\}$, let $\Pi_i := \mathsf{SHARE}(S, \mathcal{A}_i, \Pi_1, \ldots, \Pi_{i-1})$ for every $i \in \mathbb{N}$. Then the* share size for $\mathcal{A}$ *of a party $p \in \mathbb{N}$ is simply $|\Pi_p|$. The* total share size *of a set of parties $\mathcal{B}$ is $|\Pi_{\mathcal{B}}| \leq \sum_{p\in\mathcal{B}} |\Pi_p|$.* [2]

We define share size and total share size for non-adaptive/non-evolving secret sharing schemes similarly.

[2] Recall that $|\Pi_b| := \log(|\mathrm{Supp}(\Pi_p)|)$ is a lower bound on the maximal representation size of a sample from Π_p.

2.4 Csirmaz's lower bound [Csi97]

Csirmaz proved a lower bound on the share size of a (classic) secret sharing scheme for a specific access structure. We exploit the properties of this access structure in our proof. The following is the formal statement we need.

Theorem 2.10 ([Csi97])**.** *For every $t \in \mathbb{N}$, there exists an access structure $\mathcal{Z}_t$ over $t + 2^t$ parties, such that the following holds: The set of players is composed of two disjoint sets, $\mathcal{B}$ and $\mathcal{C}$, such that $|\mathcal{C}| = t$, $|\mathcal{B}| = 2^t$, and:*

1. *$\mathcal{C}$ is an unauthorized set, and,*
2. *the total share size of players in $\mathcal{C}$ is at least $2^t - 1$.*

For completeness, we give here the proof.

Proof. Fix $t \in \mathbb{N}$ and let $n = 2^t$. We start with describing the access structure $\mathcal{Z}_t$. Let $\mathcal{B} = \{P_1, \ldots, P_n\}$ be a set of n parties, and let $\mathcal{C}$ be a disjoint set of parties of size t. Let $\mathcal{C}_1, \ldots, \mathcal{C}_n$ be an ordering of all the subsets of $\mathcal{C}$, such that for every $i < j$ it holds that $\mathcal{C}_i \nsubseteq \mathcal{C}_j$.[3] Define the set of minimal authorized sets of $\mathcal{Z}_t$ to be the set

$$\mathcal{M} = \{\mathcal{C}_i \cup \{P_1, \ldots, P_i\} \colon i \in [n]\},$$

and let $\mathcal{Z}_t = \mathcal{A}_{\mathcal{M}}$ be the induced access structure. Item 1 holds by construction. Moreover, by the definition of $\mathcal{C}_1, \ldots, \mathcal{C}_n$ and $\mathcal{M}$, for every i the set $\mathcal{C}_i \cup \{P_1, \ldots, P_{i-1}\}$ is unauthorized. We now use this to prove the lower bound on the share size. Let $S \leftarrow \{0,1\}$ be a uniformly chosen secret, and Π be a random sharing of S. We want to lower bound the size of $\Pi_{\mathcal{C}}$. It holds that,

$$\begin{aligned}
|\Pi_{\mathcal{C}}| + |S| &\geq I(\Pi_{\mathcal{C}}, S; \Pi_{\mathcal{B}}) \\
&= \sum_i I(\Pi_{\mathcal{C}}, S; \Pi_{P_i} \mid \Pi_{P_{<i}}) \\
&\leq \sum_i I(\Pi_{\mathcal{C}_i}, S; \Pi_{P_i} \mid \Pi_{P_{<i}}) \\
&\leq \sum_i I(S; \Pi_{P_i} \mid \Pi_{\mathcal{C}_i}, \Pi_{P_{<i}}) \\
&= \sum_i H(S \mid \Pi_{\mathcal{C}_i}, \Pi_{P_{<i}}) - H(S \mid \Pi_{P_i}, \Pi_{\mathcal{C}_i}, \Pi_{P_{<i}}) \\
&= \sum_i 1 - 0 \\
&= n
\end{aligned}$$

where the first inequality holds by Fact 2.2. The first equality, the second inequality, and the third inequality hold by the chain rule of mutual information. The last inequality holds since $\mathcal{C}_i \cup P_{<i}$ is an unauthorized set, but $\mathcal{C}_i \cup P_{\leq i}$ is authorized. Item 2 now follows from the above since $n = 2^t$ and $|S| = 1$. □

[3] For example, order the sets according to there size in reverse order, with arbitrary order between sets of equal size.

3 The Lower Bound on the Share Size

In this section, we formally prove our lower bound. We start with a lower bound on adaptive evolving secret sharing, and then show how to generalize the bound to hold for non-adaptive schemes.

3.1 The Adaptive Case

We start by formally stating our main result.

Theorem 3.1. *Let $\mathcal{A} = \{\mathcal{A}_n\}_{n\in\mathbb{N}}$ be the access structure for which $\mathcal{A}_n = \emptyset$ for every n. Then for every adaptive evolving secret sharing scheme and every t, the total share size for $\mathcal{A}$ of the first t parties is at least $2^t - 1$. In particular, there are infinite many parties i with share size at least $2^{i-1} - 1$.*

The proof of the lower bound is by showing that for every t, after the first t parties arrived, it is possible to add 2^t parties such that the resulting access structure will be Csirmaz's structure. Thus, by Csirmaz's lower bound, the t parties must hold long shares.

Proof. Let $(\mathsf{SHARE}, \mathsf{RECON})$ be an adaptive secret sharing scheme, and fix $t \in \mathbb{N}$. We start by defining an evolving access structure $\mathcal{A}'$, and bounding its share size. Later, we relate the share size of $\mathcal{A}$ and $\mathcal{A}'$.

Let $\mathcal{C} = [t]$, and let $n = 2^t$. Let $\mathcal{B} = \{P_1, \ldots, P_n\}$ for $P_i = i + t$. Define the evolving access structure $\mathcal{A}' = \{\mathcal{A}'_n\}_{n\in\mathbb{N}}$ as follows: for every $i \in [t]$, let $\mathcal{A}'_i = \mathcal{A}_i = \emptyset$. Let $\mathcal{A}'_{t+n} = \mathcal{Z}_t$ be the access structure over the set $\mathcal{B}\cup\mathcal{C}$ promised by Theorem 2.10. For every $j \in [n]$, define $\mathcal{A}'_{t+j} = \mathcal{A}'_{t+n}|_{[t+j]}$. Finally, for every $i > t + n$, let $\mathcal{A}'_i = \mathcal{A}'_{t+n}$. Notice that $\mathcal{A}'$ is indeed an evolving access structure as $\mathcal{A}'_{t+n}|_{[t]} = \mathcal{A}_t$.

Let $S \leftarrow \{0, 1\}$ be an uniformly random secret, and let $\Pi = (\Pi_1, \ldots, \Pi_{t+n})$ be the distribution of the shares of the first $t + n$ parties on $\mathcal{A}$. That is, $\Pi_i = \mathsf{SHARE}(S, \mathcal{A}_i, \Pi_1, \ldots, \Pi_{i-1})$. Similarly, let $\Pi' = (\Pi'_1, \ldots, \Pi'_{t+n})$ be the distribution of the shares of the first $t + n$ parties on $\mathcal{A}'$ (using SHARE and the secret S).

Notice that by definition of evolving secret sharing scheme, the pair $(\widehat{\mathsf{SHARE}}, \mathsf{RECON})$ is a secret sharing scheme for the access structure $\mathcal{A}'_{t+n}$, for $\widehat{\mathsf{SHARE}}(s) := \Pi'|_{S=s}$. Thus, it must hold by Theorem 2.10 that $|\Pi'_{\mathcal{C}}| = \left|\Pi'_{\leq t}\right| \geq 2^t - 1$. However, since $\mathcal{A}'_i = \mathcal{A}_i$ for every $i \leq t$, it holds that $\Pi'_{\leq t} = \Pi_{\leq t}$. Therefore, $|\Pi_{\leq t}| \geq 2^t - 1$, and the first part of the theorem follows.

To see the second part, assume towards a contradiction that there is only a finite number of parties i for which the share size is at least $2^{i-1} - 1$, and let i^* be the maximal such (or $i^* = 1$ if no such exists). Let ℓ be the total share size of the first i^* parties. Consider the first $i^* + \ell$ first parties of $\mathcal{A}$. By the assumption, their total share size is at most

$$\ell + \sum_{j=i^*+1}^{i^*+\ell} (2^{j-1} - 1) = \sum_{j=i^*+1}^{i^*+\ell} 2^{j-1} < \sum_{j=1}^{i^*+\ell} 2^{j-1} = 2^{i^*+\ell} - 1.$$

On the other hand, by the first part of the theorem, the total share size of the first $i^* + \ell$ parties is at least $2^{i^*+\ell} - 1$ which is a contradiction to the above. □

3.2 The Non-Adaptive Case

We now prove our main result for non-adaptive schemes. We start with formally stating the result.

Theorem 3.2. *For every function $f\colon \mathbb{N} \to \mathbb{N}$ with $f \in \omega(1)$, there exists an access structure $\mathcal{A} = \{\mathcal{A}_n\}_{n\in\mathbb{N}}$ such that the following holds for any evolving secret sharing scheme for $\mathcal{A}$. For every t, the total share size of the first t parties is at least $2^{t-f(t)} - 1$. Moreover, there are infinite many parties i with share size at least $2^{i-f(i)-1} - 1$.*

The proof of the above theorem is similar to the proof of Theorem 3.1. However, since the access structure is fixed, we cannot argue that the security and correctness hold if we change the access structure on parties that did not arrive yet. To overcome this, we need to embed inside $\mathcal{A}$ all the access structures $\mathcal{Z}_t$ for every value of $t \in \mathbb{N}$. Recall that Csirmaz's structure $\mathcal{Z}_t$ is over two sets of parties, $\mathcal{C}$ and $\mathcal{B}$, such that the set $\mathcal{C}$ is of size t and has total share size 2^t. To get the stated lower bound, we need to embed in $\mathcal{A}$ the structure $\mathcal{Z}_t$ in such a way that the parties that hold long shares (that is, the parties in the set $\mathcal{C}$) will arrive early enough. This is done by associating only a sparse fraction of the parties to the set $\mathcal{B}$, using the function f.

Proof. Fix a function $f \in \omega(1)$. We start by describing the access structure $\mathcal{A}$. Assume without loss of generality that $f(0) = 0$ and $0 \leq f(n+1) - f(n) \leq 1/2$,[4] and for every n let x_n be a number such that $f(x_n) \geq n$ and $f(x_n - 1) < n$. Let $\mathcal{X} = \{x_1, x_2, \dots\}$. We divide $\mathcal{X}$ into disjoint segments $\{\mathcal{I}_j\}_{j\in\mathbb{N}}$ as follows, such that the size of the j-th segment is 2^j. Namely, for every $j \in \mathbb{N}$ let $\mathcal{I}_j = \{x_{2^j}, \dots, x_{2^{j+1}-1}\}$. For every $t \in \mathbb{N}$, let $[t]_{\overline{\mathcal{X}}} = [t] \setminus \mathcal{X}$, and let $t' = \left|[t]_{\overline{\mathcal{X}}}\right|$ be the size of $[t]_{\overline{\mathcal{X}}}$. Observe that $t' \geq t - f(t)$.

We next define the evolving access structure $\mathcal{A}$ such that $\mathcal{A}|_{[t]_{\overline{\mathcal{X}}}\cup\mathcal{I}_{t'}} = \mathcal{Z}_{t'}$ where $\mathcal{Z}_{t'}$ is the access structure promised by Theorem 2.10. Moreover, $[t]_{\overline{\mathcal{X}}}$ will match the set $\mathcal{C}$ in Theorem 2.10. This concludes the proof of the theorem similarly to the proof of Theorem 3.1, as it follows that the total share size of the parties in $[t]_{\overline{\mathcal{X}}}$ (and therefore also in $[t]$) is at least $2^{t'} - 1 \geq 2^{t-f(t)} - 1$.

To define $\mathcal{A}$ as stated above, for every $t' \in \mathbb{N}$ let $\mathcal{Z}_{t'}$ be the access structure promised by Theorem 2.10, over the sets of parties $\mathcal{C} = [t]_{\overline{\mathcal{X}}}$ and $\mathcal{B} = \mathcal{I}_{t'}$. For every $n \in \mathbb{N}$ define

$$\mathcal{A}_n := \bigcup_{t'=1}^{\infty} \{\mathcal{D} \in \mathcal{Z}_{t'} \colon \mathcal{D} \subseteq [n]\}.$$

By definition the sequence $\mathcal{A} = \{\mathcal{A}_n\}_{n\in\mathbb{N}}$ is an evolving access structure. Moreover, by construction it holds that for every t' and for every large enough n (with $f(n) > 2^{t'+1}$), it holds that $\mathcal{A}_n|_{[t]_{\overline{\mathcal{X}}}\cup\mathcal{I}_{t'}}$ is equal to $\mathcal{Z}_{t'}$, as stated above. Indeed, to make sure that we didn't add additional authorized subsets, observe that every authorized set of any structure $\mathcal{Z}_j$ for $j \neq t'$ contains at least one party from $\mathcal{I}_j$. Since $[t]_{\overline{\mathcal{X}}} \cup \mathcal{I}_{t'}$ and $\mathcal{I}_j$ are disjoint, all the authorized sets in $\mathcal{A}_n|_{[t]_{\overline{\mathcal{X}}}\cup\mathcal{I}_{t'}}$ are authorized in $\mathcal{Z}_{t'}$. □

3.3 Evolving Secret Sharing Over a Fixed Number of Parties

Our technique also implies a (weaker) lower bound on the share size of adaptive evolving secret sharing, when the number of parties is known from advanced (but the access structure is unknown).

[4] Otherwise, define $f'(n) = \min\{f'(n-1) + 1/2, \min_{n'>n}\{f(n')\}\}$. Clearly f' has the assumed property, and for every n, $f'(n) \leq f(n)$.

For example, one can prove that for the empty access structure, every scheme that supports an arbitrary structure over $2n$ parties, must give a share of length $n/\log n$ to at least $n - \log n$ of the first n parties. Otherwise, there are $\log n$ such parties with total share size less than n. We thus can use the remaining n parties to complete Csirmaz's structure, with these $\log n$ parties being the set $\mathcal{C}$. This is of course a contradiction to Theorem 2.10.

Acknowledgments

We thank Iftach Haitner and Ilan Komargodski for useful discussions.

References

[ABFNP19] Benny Applebaum, Amos Beimel, Oriol Farràs, Oded Nir, and Naty Peter. "Secret-sharing schemes for general and uniform access structures". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2019, pp. 441–471 (cit. on p. 2).

[ABNP20] Benny Applebaum, Amos Beimel, Oded Nir, and Naty Peter. "Better secret sharing via robust conditional disclosure of secrets". In: *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*. 2020, pp. 280–293 (cit. on p. 2).

[ABNPP22] Benny Applebaum, Amos Beimel, Oded Nir, Naty Peter, and Toniann Pitassi. "Secret sharing, slice formulas, and monotone real circuits". In: *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik. 2022 (cit. on p. 3).

[AN21] Benny Applebaum and Oded Nir. "Upslices, Downslices, and Secret-Sharing with Complexity of 1. 5 n". In: *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part III*. 2021, pp. 627–655 (cit. on p. 2).

[Bei11] Amos Beimel. "Secret-sharing schemes: A survey". In: *International conference on coding and cryptology*. Springer. 2011, pp. 11–46 (cit. on p. 2).

[BO11] Amos Beimel and Ilan Orlov. "Secret sharing and non-Shannon information inequalities". In: *IEEE Transactions on Information Theory* 57.9 (2011), pp. 5634–5649 (cit. on p. 3).

[Csi96] László Csirmaz. "The dealer's random bits in perfect secret sharing schemes". In: *Studia Scientiarum Mathematicarum Hungarica* 32.3 (1996), pp. 429–438 (cit. on p. 3).

[Csi97] László Csirmaz. "The size of a share must be large". In: *Journal of cryptology* 10.4 (1997), pp. 223–231 (cit. on pp. 2, 3, 6).

[CT12] László Csirmaz and Gábor Tardos. "On-line secret sharing". In: *Designs, Codes and Cryptography* 63.1 (2012), pp. 127–147 (cit. on p. 3).

[KNY17] Ilan Komargodski, Moni Naor, and Eylon Yogev. "How to share a secret, infinitely". In: *IEEE Transactions on Information Theory* 64.6 (2017), pp. 4179–4190 (cit. on pp. 2–5).

[KPC17] Ilan Komargodski and Anat Paskin-Cherniavsky. "Evolving secret sharing: dynamic thresholds and robustness". In: *Theory of Cryptography Conference*. Springer. 2017, pp. 379–393 (cit. on p. 3).

[LV18] Tianren Liu and Vinod Vaikuntanathan. "Breaking the circuit-size barrier in secret sharing". In: *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*. 2018, pp. 699–708 (cit. on p. 2).

[LVW18] Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. "Towards breaking the exponential barrier for general secret sharing". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2018, pp. 567–596 (cit. on p. 2).

[PC16] Anat Paskin-Cherniavsky. "How to infinitely share a secret more efficiently". In: *Cryptology ePrint Archive* (2016) (cit. on p. 3).