Secret Sharing for mNP: Completeness Results

Mahabir Prasad Jhanwar[1(✉)] and Kannan Srinathan[2]

[1] Ashoka University, Sonepat, India
mahavir.jhawar@gmail.com
[2] IIIT Hyderabad, Hyderabad, India

Abstract. We show completeness results for secret sharing schemes realizing mNP access structures. We begin by proposing a new, Euclidean-type, division technique for access structures. Using this new technique we obtain several results in characterizing access structures for efficient (unconditionally secure) secret sharing schemes:

- We show a useful transformation that achieves efficient schemes for complex access structures using schemes realizing simple access structures.
- We show that, assuming every access structure in $\mathsf{P} \cap \mathsf{mono}$ admits efficient secret sharing, the existence of an efficient secret sharing for an access structure in mNP that is also complete for mNP under Karp/Levin *monotone-reductions* implies secret sharing schemes for all of mNP.
- We finally improve upon the above completeness result by obtaining the same under *ordinary* Karp/Levin reductions.

1 Introduction

Secret sharing schemes enable a dealer, holding a secret piece of information, to distribute this secret among a set $\mathcal{P}_n = \{P_1, \ldots, P_n\}$ of n players such that only some predefined authorized subsets of players can reconstruct the secret from their shares. The (monotone) collection $\Gamma_n \subseteq 2^{\mathcal{P}_n}$ of authorized sets that can reconstruct the secret is called an access structure. The security of a secret sharing scheme requires that any unauthorized set B of players, i.e., $B \notin \Gamma_n$, pulling its shares together and attempt to reconstruct the secret should fail with high probability. Consequently, the security is termed unconditional (computational) if the players are computationally unbounded (computationally bounded).

A secret sharing scheme realizing an access structure Γ_n over n players is termed size-efficient, if the total length of the n shares is polynomial in n; semi-efficient, if the share distribution is computable in $\mathsf{poly}(n)$ time; and efficient, if both share distribution and reconstruction are computable in $\mathsf{poly}(n)$ time. The notions of semi-efficiency and efficiency are stronger than size-efficiency.

A major problem in this field is the characterization of access structures in terms of secret sharing schemes that they admit, where the security and efficiency of the later is measured as a combination of the following:

- Unconditional/computational security, and
- size-efficiency/semi-efficiency/efficiency.

O. Dunkelman and S.K. Sanadhya (Eds.): INDOCRYPT 2016, LNCS 10095, pp. 380–390, 2016.
DOI: 10.1007/978-3-319-49890-4_21

For concrete characterization, now onwards, we use the term *access structure* for referring to an infinite family of access structures $\Gamma = \{\Gamma_n\}_{n \in \mathbb{N}}$ (for every n, Γ_n is an access structure over $\mathcal{P}_n$) and the term "scheme realizing Γ" for referring to an infinite family of secret sharing schemes $\{\Pi_n\}_{n \in \mathbb{N}}$ such that for every n, Π_n realizes Γ_n.

Associating sets $A \subseteq \mathcal{P}_n$ with there characteristic vectors $x_A \in \{0,1\}^n$, we can define a language $L_\Gamma \subseteq \{0,1\}^*$ associated with an access structure $\Gamma = \{\Gamma_n\}_{n \in \mathbb{N}}$. Namely, $L_\Gamma = \cup_{n=1}^{\infty} \{x_A \in \{0,1\}^n \mid A \in \Gamma_n\}$. An access structure $\Gamma = \{\Gamma_n\}_{n \in \mathbb{N}}$ is said to be in the complexity class $\mathsf{P} \cap \mathsf{mono}$ if the associated language $L_\Gamma \in \mathsf{P} \cap \mathsf{mono}$. The Γ is said to be in mNP if $L_\Gamma \in \mathsf{mNP}$.

The question of access structures characterization has been widely studied. The extensive work in this area can be divided under the following two category of security: unconditional and computational. The most general class of access structures with known characterization results under them are given below.

- **Unconditional Security**
  - **$\mathsf{P} \cap \mathsf{mono}$:** It has been extensively studied whether there exists efficient secret sharing schemes for every access structures in $\mathsf{P} \cap \mathsf{mono}$? In fact, it is wide open if the same is true for all of mP - the class of access structure strictly contained in $\mathsf{P} \cap \mathsf{mono}$. With several schemes realizing different classes of access structures [6–8,11,12,16], the most general class of access structures in $\mathsf{P} \cap \mathsf{mono}$ that admit efficient perfect secret sharing are those that can be described by a polynomial-size monotone span program [13].
  - **mNP:** The question of obtaining unconditionally secure efficient schemes for access structures in mNP was met with an impossibility result. Steven Rudich observed that if $\mathsf{NP} \neq \mathsf{coNP}$, then for Hamiltonian access structure in NP there exists no semi-efficient secret-sharing scheme (specifically, schemes with perfect privacy) [4].
- **Computational Security**
  - **$\mathsf{P} \cap \mathsf{mono}$:** It is known that the whole of mP admit efficient secret sharing schemes that are computationally secure - assuming that one-way functions exists [4,17].
  - **mNP:** Komargodski, Naor and Yogev [14] showed semi-secret sharing schemes for all of mNP (and therefore cover all of $\mathsf{P} \cap \mathsf{mono}$), where the reconstruction algorithm is polynomial-time if the NP-witnesses for the authorized sets are given. Their scheme assumes existence of witness encryption [9] for whole of NP and one-way functions.

1.1 Our Results

An important corollary of the main result of Komargodski, Naor and Yogev [14] is the following completeness theorem for secret sharing schemes realizing mNP access structures:

Theorem 1 [14]**.** *Assume that one-way functions exists. Then existence of an efficient computational secret sharing for an access structure in* mNP *that is also complete for* mNP *under Karp/Levin reductions implies efficient computational secret sharing scheme for every access structure in* mNP.

The above theorem was established using the following two results:

- A secret sharing scheme for an access structure $\Gamma = \{\Gamma_n\}_{n \in \mathbb{N}}$ implies witness encryption for the associated language L_Γ.
- *Completeness theorem of witness encryption*: Using standard Karp/Levin reductions between NP-complete languages, one can transform a witness encryption for a single NP-complete language to a witness encryption scheme for any other language in NP.

Beside one-way functions, the completeness result in Theorem 1, therefore, is obtained based on the existence of witness encryption which in turn relies on strong computational assumptions related to indistinguishability obfuscation [2,3].

In this paper we obtain such completeness results for mNP access structures assuming that efficient secret sharing schemes exists for access structures in $\mathsf{P} \cap \mathsf{mono}$. More importantly, *our completeness results hold under reductions with unconditional security.* As a corollary, our completeness results also partially resolve the following problem that was left open in [14]: Is there a way that can use secret sharing scheme for access structures in $\mathsf{P} \cap \mathsf{mono}$ to achieve secret sharing scheme for access structures in mNP?

In particular, this paper makes the following important contributions:

- Our foremost contribution lies in defining a new Euclidean-type division technique for access structures. Namely, for a given pair of access structures (more like a pair of *dividend* and *divisor*), this new technique distill a list of access structures, possibly simpler then dividend and divisor (more like a *remainder*). Unlike the ordinary Euclidean division for numbers, the remainder access structures are not fixed and choosing them carefully is of great importance as it allows for simplified reductions among schemes realizing these access structures.
- We next illustrate the usefulness of our proposed division property by describing a transformation that achieves efficient secret sharing scheme for a given access structure using secret sharing schemes for appropriately defined divisor and remainder access structures.
- The above transformation helps us to achieve our first completeness theorem: Namely we show that, assuming access structures in $\mathsf{P} \cap \mathsf{mono}$ admit efficient secret sharing, the existence of an efficient secret sharing for an access structure in mNP that is also complete for mNP under Karp/Levin *monotone-reductions* implies secret sharing schemes for all of mNP.
- The above completeness theorem is obtained for NP-completeness under monotone-reductions. Removing the later restriction proved to be an important achievement of our work. A clever construction of remainder access structures helped us to obtain our second completeness theorem: Namely we show, assuming access structures in $\mathsf{P} \cap \mathsf{mono}$ admit efficient secret sharing, the existence of an efficient secret sharing for an access structure in mNP implies efficient secret sharing for all of mNP.

2 Preliminaries

2.1 Access Structure and Its Complexity

Let $\mathcal{P}_n \stackrel{\mathsf{def}}{=} \{P_1, \ldots, P_n\}$ be a set of n players. A collection $\Gamma \subseteq 2^{\mathcal{P}_n}$ of subsets of $\mathcal{P}_n$ is called *monotone increasing* if, $A \in \Gamma$ and $A \subseteq B \subseteq \mathcal{P}_n$ implies $B \in \Gamma$. A collection $\Gamma' \subseteq 2^{\mathcal{P}_n}$ is called *monotone decreasing* if, $A \in \Gamma'$ and $B \subseteq A$ implies $B \in \Gamma'$.

Definition 1 (Access Structure). *An access structure on $\mathcal{P}_n$ is a tuple (Γ_n, Γ'_n), where $\Gamma_n, \Gamma'_n \subseteq 2^{\mathcal{P}_n}$, such that*

- *Γ_n is monotone increasing; Γ'_n is monotone decreasing, and*
- *$\Gamma_n \cap \Gamma'_n = \emptyset$.*

For an access structure (Γ_n, Γ'_n), the collection Γ'_n is often called an *adversary access structure*. We call an access structure complete if, the adversary access structure Γ'_n complements Γ_n in full. We consider only complete access structures in this paper and they are simply denoted by Γ_n.

Definition 2 (Complete Access Structure). *An access structure (Γ_n, Γ'_n) is called complete if, $\Gamma'_n = 2^{\mathcal{P}_n} \backslash \Gamma_n$, i.e., $\Gamma_n \cup \Gamma'_n = 2^{\mathcal{P}_n}$.*

An access structure Γ_n can be freely identified with its characteristic Boolean function $f_{\Gamma_n} : \{0,1\}^n \to \{0,1\}$. To each set $A \subseteq \mathcal{P}_n$ associate a unique (characteristic vector) $v^A = (v_1^A, \ldots, v_n^A) \in \{0,1\}^n$ as follows: for every j in $1 \le j \le n$, $v_j^A = 1$ iff $P_j \in A$. Define, $D_{\Gamma_n} = \{v^A \mid A \in \Gamma_n\} \subseteq \{0,1\}^n$.

Definition 3 (Associated Boolean function). *For access structure Γ_n, the corresponding boolean function $f_{\Gamma_n} : \{0,1\}^n \to \{0,1\}$ is defined as follows: for $x \in \{0,1\}^n$, $f_{\Gamma_n}(x) = 1$ iff $x \in D_{\Gamma_n}$.*

Clearly, the boolean function f_{Γ_n} is monotone. Associating access structures Γ_n with their boolean functions f_{Γ_n}, we can associate a language $L_\Gamma \subseteq \{0,1\}^*$ to a family of access structures $\Gamma = \{\Gamma_n\}_{n\in\mathbb{N}}$.

Definition 4 (Associated Language). *For an access structure $\Gamma = \{\Gamma_n\}_{n\in\mathbb{N}}$, the corresponding language $L_\Gamma \subseteq \{0,1\}^*$ is defined as follows: $L_\Gamma = \{x \in \{0,1\}^* \mid f_{\Gamma_{|x|}}(x) = 1\}$, where $|x|$ denotes the length of the binary string x.*

For any access structure $\Gamma = \{\Gamma_n\}_{n\in\mathbb{N}}$, the corresponding language L_Γ is clearly in the complexity class mono - the class of monotone languages.

Definition 5 (Access Structure Complexity). *An access structure $\Gamma = \{\Gamma_n\}_{n\in\mathbb{N}}$ is said to be*

1. *in $\mathsf{P} \cap \mathsf{mono}$ if $L_\Gamma \in \mathsf{P} \cap \mathsf{mono}$,*
2. *in $\mathsf{NP} \cap \mathsf{mono}$ if $L_\Gamma \in \mathsf{NP} \cap \mathsf{mono}$.*

It is a well known fact that, $\mathsf{P} \cap \mathsf{mono} \neq \mathsf{mP}$ [1,15], where the complexity class mP denotes languages that admit monotone circuits of polynomial-size; but $\mathsf{NP} \cap \mathsf{mono} = \mathsf{mNP}$ [10], where mNP denotes the class of languages accepted by polynomial-size monotone non-deterministic circuits. We will refer to access strutures in $\mathsf{NP} \cap \mathsf{mono}$ by mNP access structures.

2.2 Secret Sharing

An n-party secret sharing scheme involves $n + 1$ players: A dealer $\mathcal{D}$, a set $\mathcal{P}_n = \{P_1, \ldots, P_n\}$ of n participants, and an access structure Γ_n over $\mathcal{P}$. A secret sharing scheme for an arbitrary Γ_n allows the dealer to *distribute shares* of a *secret value* such that

- **Privacy**: any unauthorized set $B \subseteq \mathcal{P}$ of participants, i.e., $B \notin \Gamma_n$, must not obtain any information on the secret from their collective shares.
- **Reconstructability**: any authorized coalitions $A \subseteq \mathcal{P}$ of participants, i.e., $A \in \Gamma_n$, must always reconstruct the secret from their collective shares.

Definition 6 (Secret Sharing). *An n-party secret sharing for an access structure Γ_n over $\mathcal{P}_n = \{P_1, \ldots, P_n\}$ is a tuple $\Pi = \big(\mathsf{Share}, \mathsf{Rec}, \Sigma, \Sigma_1, \ldots, \Sigma_n\big)$ such that the following holds:*

- ***Algorithms***
  - $\mathsf{Share}.\Pi$: *The share distribution algorithm* $\mathsf{Share}.\Pi$ *is a probabilistic algorithm that, on input $s \in \Sigma$ returns* $(\mathsf{Sh}_1, \ldots, \mathsf{Sh}_n) \xleftarrow{\$} \mathsf{Share}.\Pi(s)$, *where* $\mathsf{Sh}_i \in \Sigma_i$, $1 \leq i \leq n$.
  - $\mathsf{Rec}.\Pi$: *The secret reconstruction algorithm* $\mathsf{Rec}.\Pi$ *is a deterministic algorithm that on input* $(\sigma_1, \ldots, \sigma_n) \in \prod_{i=1}^{n}(\Sigma_i \cup \{*\})$ *returns a value* $\sigma \leftarrow \mathsf{Rec}.\Pi(\sigma_1, \ldots, \sigma_n)$ *where $\sigma \in \Sigma \cup \{\perp\}$. The distinguished symbols $*$ and $\perp$ have the following meanings: $\sigma_i = *$ means the ith share is missing, and* $\perp \leftarrow \mathsf{Rec}.\Pi(\sigma_1, \ldots, \sigma_n)$ *indicates that the algorithm is unable to recover the underlying secret.*
- ***Property***
  - **Correctness:** *For every authorized set of players $A \subseteq \mathcal{P}_n$, i.e., $A \in \Gamma_n$, and for every $s \in \Sigma$, we have*

$$\mathsf{Rec}\big(\mathsf{Share}.\Pi(s)_A\big) = s \tag{1}$$

  where $\mathsf{Share}.\Pi(s)_A$ *restricts the n length vector* $(\mathsf{Sh}_1, \ldots, \mathsf{Sh}_n) \xleftarrow{\$} \mathsf{Share}.\Pi(s)$ *to its A-entries, i.e.,* $\mathsf{Share}.\Pi(s)_A = \{\mathsf{Sh}_i\}_{P_i \in A}$.
  - **Security:** *The security of a secret sharing scheme is measured by the maximum probability with which a adversary $\mathcal{A}$ can win the following privacy game* - PrivacySS.

The game is played between the dealer $\mathcal{D}$ and an adversary $\mathcal{A}$ as follows:

1. *$\mathcal{A}$ first picks a pair of secrets $s_0, s_1 \in S$, and gives them to $\mathcal{D}$.*
2. *$\mathcal{D}$ chooses a random bit $b \in \{0, 1\}$ and executes* $\mathsf{Share}.\Pi(s_b)$.
3. *$\mathcal{A}$ queries shares of a set of participants $B \subseteq \mathcal{P}$ such that $B \notin \Gamma_n$.*
4. *$\mathcal{A}$ outputs a guess b' for b using the shares* $\mathsf{Share}.\Pi(s_b)_B$.

The adversary is said to win the game if $b' = b$. We measure its success as

$$Adv^{\mathsf{PrivacySS}}(\mathcal{A}) = 2 \cdot \mathsf{Pr}[b' = b] - 1.$$

$$\boxed{\begin{array}{l} \Sigma \ni s_0, s_1 \leftarrow \mathcal{A}; \\ b \xleftarrow{\$} \{0,1\}; \\ (\mathsf{Sh}_1, \ldots, \mathsf{Sh}_n) \xleftarrow{\$} \mathsf{Share}.\Pi(s_b); \\ \Gamma_n \not\ni B \leftarrow \mathcal{A}; \\ \{0,1\} \ni b' \leftarrow \mathcal{A}\big(\mathsf{Share}.\Pi(s_b)_B\big) \end{array}}$$

Fig. 1. PrivacySS: The Privacy Game

Definition 7 (Privacy). *A secret sharing scheme is said to have:*

* Perfect-Privacy*, when $\mathcal{A}$ is unbounded and $Adv^{\mathsf{PrivacySS}}(\mathcal{A}) = 0$*
* ϵ-Statistical Privacy*, when $\mathcal{A}$ is unbounded and $Adv^{\mathsf{PrivacySS}}(\mathcal{A}) < \epsilon$, where $\epsilon > 0$.*
* Computational-Privacy*, when $\mathcal{A}$ is a probabilistic polynomial time (*PPT*) algorithm and $Adv^{\mathsf{PrivacySS}}(\mathcal{A}) < \eta(k)$, where $\eta(\cdot)$ is a negligible function, and k denotes the underlying security parameter of the scheme*[1]*.*

- **Efficiency:** *Different measure of efficiency is used in the secret sharing literature. A secret sharing scheme Π is termed*

* *Size Efficient, if the total length of the n shares is polynomial in n.*
* *Semi Efficient, if the share distribution algorithm* Share.Π *is computable in* poly(n) *time.*
* *Efficient, if both* Share.Π *and* Rec.Π *are computable in* poly(n) *time.*

Definition 8 (Secret Sharing for Languages). *A family of secret sharing schemes $\Pi = \{\Pi_n\}_{n \in \mathbb{N}}$ is said to realize $\Gamma = \{\Gamma_n\}_{n \in \mathbb{N}}$ if for every $n \in \mathbb{N}$, Π_n realizes Γ_n. Then Π is also called a secret sharing scheme for the corresponding language L_Γ (see Definition 4).*

Consequently, $\Pi = \{\Pi_n\}_{n \in \mathbb{N}}$ realizing $\Gamma = \{\Gamma_n\}_{n \in \mathbb{N}}$ is said to be (size/semi) efficient if for every $n \in \mathbb{N}$, Π_n realizing Γ_n is (size/semi) efficient.

In the following, all the secret sharing schemes that we will present are both efficient and have perfect privacy.

3 A Division Property for Access Structures

For $n, m \in \mathbb{N}$, consider the following access structures:

- Γ_n - an access structure over $\mathcal{P}_n = \{P_1, \ldots, P_n\}$
- Δ_m - an access structure over $\mathcal{Q}_m = \{Q_1, \ldots, Q_m\}$, and
- for every i in $1 \leq i \leq m$, $\Gamma_n^{(i)}$ - an access structure over $\mathcal{P}_n$.

[1] In this setting, the instantiations of n, $|\Sigma|$, Share.Π, Rec.Π and so on, admits an additional parameter k.

Definition 9. *We say* $\Gamma_n \bmod \Delta_m \stackrel{\mathsf{def}}{=} \{\Gamma_n^{(1)}, \ldots, \Gamma_n^{(m)}\}$ *if, for every* $A \subseteq \mathcal{P}_n$ *the set* $A \bmod \Delta_m \stackrel{\mathsf{def}}{=} \left\{Q_i \in \mathcal{Q}_m \mid A \in \Gamma_n^{(i)}\right\} \subseteq \mathcal{Q}_m$ *satisfies the following property:*

$$A \in \Gamma_n \iff A \bmod \Delta_m \in \Delta_m \tag{2}$$

The division property in Definition 9 closely resembles the ordinary Euclidean division for integers, where Γ_n is dividend, Δ_m is divisor, and remainder is formed by the list of access structures $\{\Gamma_n^{(1)}, \ldots, \Gamma_n^{(m)}\}$. Clearly, the size (the number of authorized sets) of each $\Gamma_n^{(i)}$ is at most that of Γ_n. We will later see the importance of obtaining smaller size (and therefore simpler) $\Gamma_n^{(i)}$'s.

4 A Transformation

Theorem 2. *Let* $\Gamma_n, \Gamma_n^{(1)}, \ldots, \Gamma_n^{(m)}$ *be access structures on* $\mathcal{P}_n$*, and* Δ_m *be an access structure on* $\mathcal{Q}_m$ *such that* $\Gamma_n \bmod \Delta_m = \{\Gamma_n^{(1)}, \ldots, \Gamma_n^{(m)}\}$*. Assume*

1. $\Pi_{\Delta_m} = (\mathsf{Share}.\Pi_{\Delta_m}, \mathsf{Rec}.\Pi_{\Delta_m})$ *is a perfect secret sharing scheme realizing* Δ_m*, and*
2. *for every* i *in* $1 \le i \le m$*,* $\Pi_{\Gamma_n^{(i)}} = (\mathsf{Share}.\Pi_{\Gamma_n^{(i)}}, \mathsf{Rec}.\Pi_{\Gamma_n^{(i)}})$ *is a perfect secret sharing realizing* $\Gamma_n^{(i)}$

then there exists Π_{Γ_n} *- a perfect secret sharing scheme realizing* Γ_n*.*

Proof: The secret sharing scheme Π_{Γ_n} can be described as follows:

- $\mathsf{Share}.\Pi_{\Gamma_n}$: The share distribution algorithm distributes a secret s among players in $\mathcal{P}_n = \{P_1, \ldots, P_n\}$ as follows:
  - Compute $(s_1, \ldots, s_m) \stackrel{\$}{\leftarrow} \mathsf{Share}.\Pi_{\Delta_m}(s)$
  - For every i in $1 \le i \le m$, compute $(s_{i1}, \ldots, s_{in}) \stackrel{\$}{\leftarrow} \mathsf{Share}.\Pi_{\Gamma_n^{(i)}}(s_i)$

  The player P_j, for every j in $1 \le j \le n$, gets the following share:

  $$P_j \leftarrow (s_{1j}, s_{2j}, \ldots, s_{mj})$$

- $\mathsf{Rec}.\Pi_{\Gamma_n}$: For every authorized set $A \in \Gamma_n$, the players in A pull together their respective shares and reconstruct the secret as follows. Let $A \bmod \Delta_m = \{Q_{i_1}, \ldots, Q_{i_r}\} \subseteq \mathcal{Q}_m$, for some r in $1 \le r \le m$. By the definition of $A \bmod \Delta_m$, $A \in \Gamma_n^{(i_j)}$, j in $1 \le j \le r$, and therefore players in A reconstruct intermediate shares s_{i_j}'s using reconstruction algorithm $\mathsf{Rec}.\Pi_{\Gamma_n^{(i_j)}}$'s respectively. As $A \bmod \Delta_m$ is in Δ_m, the secret is finally reconstructed by computing $s \leftarrow \mathsf{Rec}.\Pi_{\Delta_m}(s_{i_1}, \ldots, s_{i_r})$.
- $\mathsf{Privacy}$: Secret is perfectly hidden from the combined shares of any unauthorized set $A' \notin \Gamma_n$. Let $A' \bmod \Delta_m = \{Q_{i_1}, \ldots, Q_{i_u}\}$ and it does not belongs to Δ_m. The players in A' can compute intermediate shares s_{i_j}'s, $1 \le j \le u$, of the secret s. But these shares $\{s_{i_1}, \ldots, s_{i_u}\}$ will not reveal any information (perfectly hidden) about s as $\{Q_{i_1}, \ldots, Q_{i_u}\} \notin \Delta_m$.

5 Completeness Under Monotone-Reductions

Theorem 3. *Assume access structures in* $\mathsf{P} \cap \mathsf{mono}$ *admit efficient secret sharing. Then existence of an efficient secret sharing for an access structure in* mNP *that is also complete for* mNP *under Karp/Levin monotone-reductions implies secret sharing schemes for all of* mNP.

Proof: Let $\Delta = \{\Delta_m\}_{m\in\mathbb{N}}$ be an access structure in mNP that is also complete for mNP under monotone-reductions and suppose it admits an efficient secret sharing scheme. Consider an arbitrary access structure $\Gamma = \{\Gamma_n\}_{n\in\mathbb{N}}$ from mNP. We now show, for every $n \in \mathbb{N}$, Γ_n admits an efficient secret sharing scheme. For any fix n, there exists (completeness of Δ) an $m \in \mathbb{N}$ such that Γ_n is monotone-reducible to Δ_m, i.e., there exists a polynomial time computable *monotone* function $K_R : 2^{\mathcal{P}_n} \to 2^{\mathcal{Q}_m}$ such that the following holds:

$$\forall A \subseteq \mathcal{P}_n, A \in \Gamma_n \iff K_R(A) \in \Delta_m. \tag{3}$$

Define, for every i in $1 \le i \le m$, an access structure $\Gamma_n^{(i)}$ over $\mathcal{P}_n$ as follows:

$$\text{For } i \in [m], \Gamma_n^{(i)} = \big\{A \subseteq \mathcal{P}_n \mid Q_i \in K_R(A)\big\}. \tag{4}$$

The theorem follows by proving the following claims (see Theorem 2):

Claim 1: Each $\Gamma_n^{(i)}$ is in $\mathsf{P} \cap \mathsf{mono}$, $1 \le i \le m$
Claim 2: $\Gamma_n \bmod \Delta_m = \{\Gamma_n^{(1)}, \dots, \Gamma_n^{(m)}\}$.

Proof of Claim 1: We first show $\Gamma_n^{(i)}$ is monotone, i.e., for every $A, B \subseteq \mathcal{P}_n$ with $\Gamma_n^{(i)} \ni A \subseteq B$, we show $B \in \Gamma_n^{(i)}$. Firstly, $Q_i \in K_R(A)$ as $A \in \Gamma_n^{(i)}$. Secondly, the monotone property of K_R map implies $K_R(A) \subseteq K_R(B)$. These two mean that $Q_i \in K_R(B)$, implying B belongs to $\Gamma_n^{(i)}$.

We now show $\Gamma_n^{(i)}$ is in P. For any set $A \subseteq \mathcal{P}_n$, $A \in \Gamma_n^{(i)}$ iff $Q_i \in K_R(A)$. But, K_R is a polynomial time computable function and therefore computing $K_R(A)$ is efficient, implying $\Gamma_n^{(i)}$ is in P.
Proof of Claim 2: We now prove $\Gamma_n \bmod \Delta_m = \{\Gamma_n^{(1)}, \dots, \Gamma_n^{(m)}\}$, i.e., for every $A \subseteq \mathcal{P}_n$, $A \in \Gamma_n$ iff $A \bmod \Delta_m \in \Delta_m$. But

$$\begin{aligned} A \bmod \Delta_m &= \{Q_i \in \mathcal{Q}_m \mid A \in \Gamma_n^{(i)}\} \\ &= \{Q_i \in \mathcal{Q}_m \mid Q_i \in K_R(A)\} \\ &= K_R(A) \end{aligned}$$

Therefore, for every set $A \subseteq \mathcal{P}_n$

$$\begin{aligned} A \in \Gamma_n &\overset{eqn-3}{\iff} K_R(A) \in \Delta_m \\ &\iff A \bmod \Delta_m \in \Delta_m \end{aligned}$$

This completes the proof.

6 Completeness Without Monotone-Reductions

Theorem 4. *Assume access structures in* $\mathsf{P} \cap \mathsf{mono}$ *admit efficient secret sharing. Then existence of an efficient secret sharing for an access structure in* mNP *that is also complete for* mNP *under ordinary (not necessarily monotone) Karp/Levin reductions implies efficient secret sharing for all those* $\Gamma = \{\Gamma_n\}_{n\in\mathbb{N}} \in \mathsf{mNP}$ *that satisfy the following: for every* n *there exists a* $k_n \in \mathbb{N}$ *such that* $\Gamma_n = B_{k_n} \cup \{A \subseteq \mathcal{P}_n \mid |A| \geq k_n + 1\}$*, where* B_{k_n} *is a subset of* $A_{k_n} \stackrel{\mathsf{def}}{=} \{A \subseteq \mathcal{P}_n \mid |A| = k_n\}$*.*

Proof: Let $\Delta = \{\Delta_m\}_{m\in\mathbb{N}}$ be an access structure in mNP that is also complete and it admits an efficient secret sharing scheme. Consider an arbitrary access structure $\Gamma = \{\Gamma_n\}_{n\in\mathbb{N}}$ from mNP satisfying the following: for every n there exists a $k_n \in \mathbb{N}$ such that $\Gamma_n = B_{k_n} \cup \{A \subseteq \mathcal{P}_n \mid |A| \geq k_n + 1\}$, where B_{k_n} is a subset of A_{k_n}, the set of all k_n-size subsets of $\mathcal{P}_n$. We now show that Γ_n admits efficient secret sharing scheme for every $n \in \mathbb{N}$. For any fix n, there exists (completeness of Δ) $m \in \mathbb{N}$ such that Γ_n is Karp/Levin reducible to Δ_m, i.e., there exists a polynomial time computable function $K_R : 2^{\mathcal{P}_n} \to 2^{\mathcal{Q}_m}$ with the following property:

$$\forall A \subseteq \mathcal{P}_n, A \in \Gamma_n \iff K_R(A) \in \Delta_m. \tag{5}$$

We now define, for every i in $1 \leq i \leq m$, an access structure $\Gamma_n^{(i)}$ on $\mathcal{P}_n$ as follows:

$$\Gamma_n^{(i)} = \big\{A \subseteq \mathcal{P}_n \mid Q_i \in K_R(A) \wedge |A| = k_n\big\} \cup \{A \subseteq \mathcal{P}_n \mid |A| \geq k_n + 1\} \tag{6}$$

It is easy to see that, for every i in $1 \leq i \leq m$, $\Gamma_n^{(i)}$ is in $\mathsf{P}\cap\mathsf{mono}$. To prove the theorem, it suffices to show (by Theorem 2) that $\Gamma_n \bmod \Delta_m = \{\Gamma_n^{(1)}, \ldots, \Gamma_n^{(m)}\}$, i.e., for every $A \subseteq \mathcal{P}_n$, $A \in \Gamma_n$ iff $A \bmod \Delta_m \in \Delta_m$. We consider the following exhaustive cases.

- $|A| < k_n$: Clearly, $A \notin \Gamma_n$ and $A \bmod \Delta_m = \emptyset \notin \Delta_m$, and therefore $A \in \Gamma_n$ iff $A \bmod \Delta_m \in \Delta_m$ holds true.
- $|A| \geq k_n + 1$: In this case, $A \in \Gamma_n$ and $A \bmod \Delta_m = \mathcal{Q}_m \in \Delta_m$, and therefore $A \in \Gamma_n$ iff $A \bmod \Delta_m \in \Delta_m$ holds true.
- $|A| = k$: Finally, in this case

$$\begin{aligned} A \bmod \Delta_m &= \{Q_i \in \mathcal{Q}_m \mid A \in \Gamma_n^{(i)}\} \\ &= \{Q_i \in \mathcal{Q}_m \mid (Q_i \in K_R(A) \wedge |A| = k_n) \vee (|A| \geq k_n + 1)\} \\ &= \{Q_i \in \mathcal{Q}_m \mid Q_i \in K_R(A)\} \\ &= K_R(A) \end{aligned}$$

Hence, $A \in \Gamma_n \stackrel{eqn-5}{\iff} K_R(A) \in \Delta_m \iff A \bmod \Delta_m \in \Delta_m$.

Corollary 1. *Assume access structures in* $\mathsf{P}\cap\mathsf{mono}$ *admit efficient secret sharing. Then existence of an efficient secret sharing for an access structure in* mNP *implies efficient secret sharing for all of* mNP*.*

Proof: It suffices (by Theorem 4) to prove the following: the class of access structures $\Gamma = \{\Gamma_n\}_{n\in\mathbb{N}} \in \mathsf{mNP}$ as described in Theorem 4 cover whole of mNP. This follows by a technique developed in [5]. We now show access structures in mNP are in one-one correspondence with access structures of the type described in Theorem 4.

Let $\hat{\Gamma} = \{\hat{\Gamma}_n\}_{n\in\mathbb{N}}$ be an arbitrary access structure in mNP. For every $n \in \mathbb{N}$, we now define, based on $\hat{\Gamma}_n$, an access structure $\tilde{\Gamma}_{2n}$. First identify $\hat{\Gamma}_n$ with the set $L_{\hat{\Gamma}_n} \subseteq \{0,1\}^n$. Now define $\tilde{\Gamma}_{2n}$ over a set of $2n$ players $\tilde{\mathcal{P}}_{2n} = \{P_{i,b}\}_{1\le i\le n; b\in\{0,1\}}$:

$$\tilde{\Gamma}_{2n} = B_n \cup \{A \subseteq \tilde{\mathcal{P}}_{2n} \mid |A| \ge n+1\}$$

where the collection B_n consists of precisely the following n-size subsets of $\tilde{\mathcal{P}}_{2n}$: for every $x = (x_1,\ldots,x_n) \in L_{\hat{\Gamma}_n}$, the set $\{P_{1,x_1},\ldots,P_{n,x_n}\}$ is in B_n. Clearly, the complexity of checking whether a set $A \subseteq \tilde{\mathcal{P}}_{2n}$ is in $\tilde{\Gamma}_{2n}$ is exactly the complexity of deciding the membership in $L_{\hat{\Gamma}_n}$. However $L_{\hat{\Gamma}} = \{L_{\hat{\Gamma}_n}\}_{n\in\mathbb{N}}$ is in mNP (as $\hat{\Gamma} \in \mathsf{mNP}$) and so $\tilde{\Gamma} = \{\tilde{\Gamma}_{2n}\}_{n\in\mathbb{N}}$ is in mNP. Finally, $\tilde{\Gamma} = \{\tilde{\Gamma}_{2n}\}_{n\in\mathbb{N}}$ is clearly of the type described in Theorem 4. This proves the corollary.

References

1. Alon, N., Boppana, R.B.: The monotone circuit complexity of boolean functions. Combinatorica **7**(1), 1–22 (1987)
2. Barak, B., Goldreich, O., Impagliazzo, R., Rudich, S., Sahai, A., Vadhan, S., Yang, K.: On the (im)possibility of obfuscating programs. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 1–18. Springer, Heidelberg (2001). doi:10.1007/3-540-44647-8_1
3. Barak, B., Goldreich, O., Impagliazzo, R., Rudich, S., Sahai, A., Vadhan, S.P., Yang, K.: On the (im)possibility of obfuscating programs. J. ACM **59**(2), 6 (2012)
4. Beimel, A.: Secret-sharing schemes: a survey. In: Chee, Y.M., Guo, Z., Ling, S., Shao, F., Tang, Y., Wang, H., Xing, C. (eds.) IWCC 2011. LNCS, vol. 6639, pp. 11–46. Springer, Heidelberg (2011). doi:10.1007/978-3-642-20901-7_2
5. Beimel, A., Ishai, Y.: On the power of nonlinear secrect-sharing. In: IEEE Conference on Computational Complexity, pp. 188–202 (2001)
6. Benaloh, J., Leichter, J.: Generalized secret sharing and monotone functions. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 27–35. Springer, Heidelberg (1990). doi:10.1007/0-387-34799-2_3
7. Blakley, G.: Safeguarding cryptographic keys. In: AFIPS National Computer Conference, vol. 48, pp. 313–317 (1979)
8. Brickell, E.F.: Some ideal secret sharing schemes. In: Quisquater, J.-J., Vandewalle, J. (eds.) EUROCRYPT 1989. LNCS, vol. 434, pp. 468–475. Springer, Heidelberg (1990). doi:10.1007/3-540-46885-4_45
9. Garg, S., Gentry, C., Sahai, A., Waters, B.: Witness encryption and its applications. In: Boneh, D., Roughgarden, T., Feigenbaum, J. (eds.) STOC, pp. 467–476. ACM (2013)
10. Grigni, M., Sipser, M.: Monotone complexity. In: LMS Workshop on Boolean Function Complexity, vol. 169, pp. 57–75. Cambridge University Press (1992)

11. Ito, M., Saito, A., Nishizeki, T.: Secret sharing scheme realizing general access structure. Electron. Commun. Jpn. (Part III: Fundam. Electron. Sci.) **72**(9), 56–64 (1989)
12. Jackson, W.-A., Martin, K.M.: Cumulative arrays and geometric secret sharing schemes. In: Seberry, J., Zheng, Y. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 48–55. Springer, Heidelberg (1993). doi:10.1007/3-540-57220-1_51
13. Karchmer, M., Wigderson, A.: On span programs. In: Structure in Complexity Theory Conference, pp. 102–111 (1993)
14. Komargodski, I., Naor, M., Yogev, E.: Secret-sharing for NP. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8874, pp. 254–273. Springer, Heidelberg (2014). doi:10.1007/978-3-662-45608-8_14
15. Razborov, A.A.: Lower bounds on the monotone complexity of some Boolean functions. Dokl. Akad. Nauk SSSR **281**, 798–801 (1985). English translation in Sov. Math. Doklady **31**, 354–357 (1985)
16. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
17. Vinod, V., Narayanan, A., Srinathan, K., Rangan, C.P., Kim, K.: On the power of computational secret sharing. In: Johansson, T., Maitra, S. (eds.) INDOCRYPT 2003. LNCS, vol. 2904, pp. 162–176. Springer, Heidelberg (2003). doi:10.1007/978-3-540-24582-7_12