New Results in Share Conversion, with Applications to Evolving Access Structures

Tamar Ben David
Ariel University, Israel

Varun Narayanan
University of California, Los Angeles, CA, USA

Olga Nissenbaum
Ariel University, Israel

Anat Paskin-Cherniavsky
Ariel University, Israel

Abstract

We say there is a share conversion from a secret-sharing scheme Π to another scheme Π' implementing the same access structure if each party can locally apply a deterministic function to their share to transform any valid secret-sharing under Π to a valid (but not necessarily random) secret-sharing under Π' of the same secret. If such a conversion exists, we say that $\Pi \geq \Pi'$. This notion was introduced by Cramer et al. (TCC'05), where they particularly proved that for any access structure, any linear secret-sharing scheme over a given field $\mathbb{F}$, has a conversion from a CNF scheme, and is convertible to a DNF scheme.

In this work, we initiate a systematic study of convertability between secret-sharing schemes, and present a number of results with implications to the understanding of the convertibility landscape.

- In the context of linear schemes, we present two key theorems providing necessary conditions for convertibility, proved using linear-algebraic tools. It has several implications, such as the fact that Shamir secret-sharing scheme can be neither maximal or minimal. Another implication of it is that a scheme may be minimal if its share complexity is at least as high as that of DNF.
- Our second key result is a necessary condition for convertibility to CNF from a broad class of (not necessarily linear) schemes. This result is proved via information-theoretic techniques and implies non-maximality for schemes with share complexity smaller than that of CNF.

We also provide a condition which is both necessary and sufficient for the existence of a share conversion to some linear scheme. The condition is stated as a system of linear equations, such that a conversion exists if and only if a solution to the linear system exists. We note that the impossibility results for linear schemes may be viewed as identifying a subset of contradicting equations in the system.

Another contribution of our paper, is in defining and studying share conversion for evolving secret-sharing schemes. In such a schemes, recently introduced by Komargodski et al. (IEEE ToIT'18), the number of parties is not bounded apriori, and every party receives a share as it arrives, which never changes in the sequel. Our impossibility results have implications to the evolving setting as well. Interestingly, unlike in the standard setting, there is no maximum or minimum in a broad class of evolving schemes, even without any restriction on the share size.

Finally, we show that, generally, there is no conversion between additive schemes over different fields, even from CNF to DNF! However by relaxing from perfect to statistical security, it may be possible to convert, and exemplify this for (n, n)-threshold access structures.

2012 ACM Subject Classification Security and privacy → Information-theoretic techniques; Security and privacy → Mathematical foundations of cryptography

Keywords and phrases secret sharing, linear secret sharing, evolving access structures, share conversion, feasibility

Digital Object Identifier 10.4230/LIPIcs.ITC.2025.11

Related Version *Full Version*: `https://eprint.iacr.org/2024/1781` [11]

6th Conference on Information-Theoretic Cryptography (ITC 2025).
Editor: Niv Gilboa; Article No. 11; pp. 11:1–11:23
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Introduction

Secret-sharing is a fundamental notion in cryptography. A secret-sharing scheme enables a dealer to distribute a secret among a set of parties so that any pre-specified subset of qualified parties can recover the secret while any other subset of parties remains oblivious to the secret. The monotone class of subsets of qualified parties constitutes the *access structure* realized by the secret-sharing scheme.

Secret-sharing is a building block for realizing several complex cryptographic tasks. Certain such tasks may require additional properties in the secret-sharing scheme – for instance, succinctness of the shares, or homomorphism and other algebraic properties. This suggests use cases where a protocol requires secret-sharing according to one scheme during one stage, and according to another scheme during another. This motivated non-interactive conversion between secret-sharing schemes, which was formalized in [9] by Cramer, Damgard, and Ishai as *share conversion*.

We say there is a share conversion from a secret-sharing scheme Π to another scheme Π' implementing the same access structure Γ if each party can locally apply a deterministic function to their share to transform any valid secret-sharing under Π to a valid (but not necessarily random) secret-sharing of the same secret under Π'. In full generality, share conversion may be defined from Π to Π' which implement different access structures $\Gamma \supseteq \Gamma'$, respectively. Moreover the secret under Π' after the transformation can be a pre-specified function of the secret under Π before transformation. In this work, we focus on the natural case where $\Gamma = \Gamma'$ and the above-mentioned function is identity.

In the sequel, we will say $\Pi \geq \Pi'$ if there is a share conversion from Π to Π'. This induces a partial ordering over secret-sharing schemes realizing any access structure Γ. Many important insights into the partial order $\geq$ of convertability for *linear secret-sharing schemes* over a finite field were provided in [9]. Among other results, they proved that, for any access structure Γ and finite filed $\mathbb{F}$, CNF-based secret-sharing scheme $CNF_{\Gamma,\mathbb{F}}$ is maximal, and DNF-based secret-sharing scheme $DNF_{\Gamma,\mathbb{F}}$ is minimal among the set of all linear secret-sharing schemes for Γ over $\mathbb{F}$. I.e., $CNF_{\Gamma,\mathbb{F}} \geq \Pi \geq DNF_{\Gamma,\mathbb{F}}$ for any linear secret-sharing scheme Π. Note, however, that the existence of additional minimal and maximal schemes is not ruled out in [9]. For certain access structures, specifically (2,3)-threshold, they demonstrated that certain linear schemes like Shamir secret-sharing scheme in not maximal, as it is not convertible to CNF. They also show that a limited class of linear secret-sharing schemes – the so called *replicated schemes*, that are similar in structure to CNF in the sense that the secret is defined as the sum of random elements, and every party gets a subset of them as it's share, are not maximal for (k, n)-threshold access structures unless they have share complexity as high as that of CNF (see Section 3.3 in [9]).

In this paper, we initiate a systematic study of convertibility between secret-sharing schemes, and obtain new results in several directions:

- We develop new and easily checkable necessary conditions for share conversion between linear schemes implementing a given access structure. These necessary conditions are in the form of linear algebraic constraints on the *monotone span program (MSP)* corresponding to the linear schemes. Using these conditions, we are able to get a clearer view of the partial order induced by convertibility over the linear schemes.
- We develop a necessary and sufficient condition for a conversion between the linear schemes Π, Π' in form of a linear system decided by the MSP of Π and Π' which has a solution if and only if $\Pi \geq \Pi'$.

- Next, we address the broader problem of share conversions involving potentially non-linear secret-sharing schemes. To this end, we introduce the notion of *non-degenerate* secret-sharing schemes and establish a necessary condition for converting shares from general (potentially non-linear) schemes to non-degenerate ones. This condition has implications for share conversion to CNF and Shamir secret-sharing schemes, which are both non-degenerate.
- We apply our results to develop necessary conditions for conversion to the well-studied schemes, such as CNF, DNF, and Shamir secret-sharing schemes.
- The necessary conditions we develop also bear consequences for secret-sharing schemes for evolving setting, i.e. where the number of parties is not bounded, and the party gets it's share when appears. We show that, for several interesting evolving access structures, there is no maximal or minimal scheme.
- We also initiate the study of share conversion between different fields. We show that, in a general case, there is no conversion between linear schemes over two different fields. To circumvent this, we propose a general approach of bounding the randomness domain in a source scheme. We build a leaky additive scheme over $\mathbb{Z}_p$ allowing conversion into $\mathbb{Z}_q$. As it's possible to see from our example, the proposed approach could result in a privacy leakage, which is often tolerable if small.

1.1 Overview of Our Results

In this section, we provide a brief exposition of our results, which we formally describe and prove in the subsequent sections.

Necessary conditions for conversion between linear schemes. A linear secret-sharing scheme Π over a field $\mathbb{F}$ implementing access structure Γ over n parties is characterized by a monotone span program described as a triple $(\mathbb{F}, M, \rho)$, where M is a matrix over $\mathbb{F}$ of dimension $m \times k$ and $\rho : [m] \to [n]$ defines the set of M's rows corresponding to a certain party [16].

To share a secret $s \in \mathbb{F}$, the dealer samples a vector $\mathbf{r} \in \mathbb{F}^k$ such that its first coordinate is s, and computes $\mathbf{v} = M \cdot \mathbf{r}$. Then, the i'th share in Π is $\mathsf{sh}_i = \mathbf{v}[\rho^{(-1)}(i)]$, which is the sub-vector containing entries in the coordinates $\rho^{-1}(i)$. A qualified set of parties T can recover the secret using a reconstruction function $\alpha \in \mathbb{F}^{|\rho^{-1}(T)|}$ such that

$$(\alpha)^{\mathsf{T}} \cdot \mathbf{v}_T = (\alpha)^{\mathsf{T}} \cdot M_T \cdot \mathbf{r} = \mathbf{r}[1] = s.$$

Here, $\mathbf{v}_T = \mathbf{v}[\rho^{-1}(T)]$ and $M_T = M[\rho^{-1}(T), \cdot]$, i.e., the rows of M corresponding to the coordinates $\rho^{-1}(T)$ (under some pre-specified ordering).

One of the key tools in our paper is a necessary condition for conversion between a pair of linear schemes. Informally, it states that conversion is impossible, if the schemes satisfy certain linear-algebraic conditions.

▶ **Theorem 1** (Necessary condition for conversion between linear schemes – Informal). *There is no share conversion from a linear secret-sharing scheme described by MSP $(\mathbb{F}, M \in \mathbb{F}^{m \times k}, \rho)$ to another linear scheme $(\mathbb{F}, M' \in \mathbb{F}^{m' \times k'}, \rho')$ both realizing Γ, if there are sets of parties T, T^* and party $h \notin T \cup T^*$ such that $T \cup h \in \Gamma$, and no strict subsets of $T \cup h$ is qualified, and, when α and α' are reconstruction functions for $T \cup h$ in M and M', respectively,*

1. $(\alpha'_h)^{\mathsf{T}} \cdot M'_h \in \mathrm{Rowspan}(M'_{T^*})$.
2. $(\alpha_h)^{\mathsf{T}} \cdot M_h \notin (\mathrm{Rowspan}(M_T) \cap \mathrm{Rowspan}(M_h)) + (\mathrm{Rowspan}(M_{T^*}) \cap \mathrm{Rowspan}(M_h))$.

This theorem is formally stated as Theorem 27 in the technical section. We demonstrate the power of this seemingly abstract necessary condition by providing a concrete application to well studied secret-sharing schemes, and its application to share conversions for evolving access structures.

We exploit the fact that the share conversion function is local and the secret is preserved during the share conversion. We can reach a contradiction if it is possible to produce a pair of fooling instances of sharing under the source scheme that result in shares after conversion that do not respect the dependencies present among the shares in the target distribution. This proof is a vast generalization of the proof of a result in [9] that showed that in $(2,3)$-Shamir is not convertible to CNF, so that it applies to conversion between any pair of linear schemes. Specifically, it follows that any Shamir secret-sharing scheme is not convertible to CNF.

In Theorem 30 we prove a different type of necessary condition for convertibility between linear schemes. As a corollary from Theorem 1 and Theorem 30, we prove that DNF is not convertible to any linear scheme with lower share complexity. In particular, it is not convertible to Shamir, which proves the non-minimality of the latter.

Both Theorem 30 and Theorem 1 are based on a key technical result – Lemma 25, which involves a single minterm T, while the theorems refer to at least 2 minterms to establish a conversion does not exist. We believe it is a useful conceptual simplification towards understanding convertability.

Convertibility characterization for linear schemes. We devise a characterization of convertibility between linear schemes by solvability of a certain system of linear equations $\mathcal{L}_{\Pi,\Pi'}$ which we provide in Section 5.

▶ **Theorem 2** (Theorem 35, informal). *There is a conversion from a linear scheme* Π *to a linear scheme* Π' *realizing the same access structure over the same field if and only if the linear system* $\mathcal{L}_{\Pi,\Pi'}$ *has a solution.*

A solution of the system encodes a conversion in a straightforward (although redundant) way. The high level idea is to solve for variables $X_{\mathbf{r},i,j}$, where $X_{\mathbf{r},i,j}$ represents the j'th share of p_i, when converting from a sharing based on randomness $\mathbf{r}$ in Π (as is sometimes useful, here $\mathbf{r}$ is assumed to include s). We note that the impossibility in Theorem 1 may be viewed as identifying a subset of contradicting equations, so that a solution does not exist.

Share conversion from non-linear schemes. In a prior work [9], CNF was proved to be maximal among linear schemes over the same field. In this work, we prove new necessary conditions for share conversion from general (potentially non-linear) schemes to CNF secret-sharing.

For this, we introduce the notion of *non-degenerate* secret-sharing schemes. A secret-sharing scheme Π is non-degenerate if any sub-scheme of Π is equivalent to Π. Here, a secret-sharing scheme Π' is a sub-scheme of Π if the secret domains of both schemes are identical, and every valid secret-sharing under Π' is also a valid secret-sharing under Π. A formal definition of non-degenerate secret-sharing schemes is provided in Definition 36.

To drive down this subtle notion, we will demonstrate that a 2-out-of-3 DNF secret-sharing scheme for secret domain $\{0,1\}$ is *not* non-degenerate. In 2-out-of-3 DNF secret-sharing of a secret $s \in \{0,1\}$, the shares of the 3 parties are $(r_{1,2}, s \oplus r_{3,1})$, $(s \oplus r_{1,2}, r_{2,3})$ and $(s \oplus r_{2,3}, r_{3,1})$, respectively, where $r_{1,2}, r_{2,3}$ and $r_{3,1}$ are uniform and independent bits. Consider a modified secret-sharing scheme in which the secret s is shared among the three parties exactly as in 2-out-of-3 DNF secret-sharing except that $r_{1,2}, r_{2,3}$ and $r_{3,1}$ are uniform and only pairwise independent bits. It is easy to see that the latter is a 2-out-of-3 secret-sharing which is also a sub-scheme of the former. However, they are not clearly not equivalent: the former uses more randomness; hence, 2-out-of-3 DNF is not non-degenerate.

On the other hand, CNF secret-sharing scheme for arbitrary access structures over a group $\mathbb{G}$ for secret domain $\mathbb{G}$, and Shamir secret-sharing scheme are non-degenerate as established in Lemma 38 and Lemma 39, respectively. Lemma 38 is proved by considering the correlation of the shares induced by picking a secret $s \in \mathbb{G}$ at random and secret-sharing it using any secret-sharing scheme Π that is a sub-scheme of the given CNF scheme. Appealing to correctness and privacy of Π, an information theoretic argument is used to show that the entropy of each share in this correlation is the same as that in the correlation obtained by secret-sharing a random secret s using the CNF scheme. Since the secret domain is the same as the group over which CNF is defined, this further implies in a straightforward way that Π coincides with the CNF scheme, establishing its non-degeneracy.

By appealing to non-degeneracy of CNF, and using standard entropy lower bounds, we show that share conversion to CNF scheme is possible only if the share size under the source scheme is at least as large as that in the CNF scheme. The following result is formally stated in Theorem 40.

▶ **Theorem 3** (Extended maximality of CNF). *Let Π be a secret-sharing scheme realizing an n-party access structure Γ with secret domain $\mathbb{G}$ – a finite group. There is a share conversion from Π to CNF over $\mathbb{G}$ realizing Γ only if, for each $i \in [n]$, size of the share i in Π is at least $\log|\mathbb{G}| \cdot |\{F \in \mathcal{F} \text{ s.t. } i \notin F\}|$, where $\mathcal{F}$ is the set of all maximal forbidden sets associated with Γ.*

We note that Theorem 1 also implies results of non-maximality by impossibility of conversion to CNF for certain linear schemes Π with low share complexity. These results are mostly subsumed by Theorem 3, both because it does not restrict Π to be linear, and in terms of share size.

Share conversion for evolving secret-sharing. Komargodski et al. [17] defined evolving secret-sharing schemes where the unbounded number of parties arriving one after another, obtain their shares of secret. The previously qualified sets remain qualified, and shares of parties are not refreshed as new parties come, but each newcomer is provided a (potentially) progressively larger share. An evolving access structure is an infinite monotone class of qualified subsets of $\mathbb{N}$.

We initiate a study of share conversion for evolving secret-sharing, starting with formal extension of the notion of share conversion, MSP and linearity to the evolving setting. Then, we apply the theory we develop for proving impossibility of share conversion in the standard setting to the evolving setting. In particular, some of our results apply to *evolving linear secret-sharing schemes*, which have been previously considered in the literature, but never explicitly defined.

We address the problem of maximal and minimal secret-sharing schemes for evolving access structures, and show that for several broad classes of evolving schemes there is no maximal and minimal scheme. In Theorem 46 we formally state and prove the following result.

▶ **Theorem 4** (No evolving maximal scheme – Informal). *For any non-trivial evolving access structure, there exists no maximal secret-sharing scheme for one-bit secrets.*

By a non-trivial evolving access structure (See Definition 45), we mean one that does not devolve into a finite secret-sharing scheme among the first n parties (for some n) with the remaining parties either being not part of the qualified set or are required to simply receive the secret.

In the other direction, we obtain a slightly weaker result, showing there is no minimal linear scheme for certain access structures. This is formally stated and proved as Theorem 44.

▶ **Theorem 5** (No evolving minimal scheme – Informal). *For a certain broad class of evolving access structures Γ, and for the finite field $\mathbb{F}_2$, there is no minimal linear evolving scheme for any Γ in the class.*

Conversion between different fields. The bit simultaneously shared in two different fields, is called *dBit*, and is an important primitive for many applications, such as [2, 6, 8, 12, 13, 19, 20, 24]. There exist bit share conversion protocols, here we point out only few of them, such as proposed in [6, 7, 10]. It is natural to raise the question if such a conversion can be done locally.

Generalizing our impossibility result for linear schemes over the same field, we prove the inconvertibility of the maximal CNF scheme over $\mathbb{Z}_p$ to any other linear scheme over $\mathbb{Z}_q$ for primes $p \neq q$ with the same secret domain $\{0, 1\}$.

We complement this result with a relaxed form of conversion between additive schemes for certain pairs of distinct primes for 1-bit shares. The relaxation allows for a privacy leakage (over the scheme randomness). It may be interesting to further explore share conversions with a small correctness errors. These may suffice for many applications, while potentially extending the set of convertible secret sharing scheme pairs (denote $\Pi \geq_\epsilon \Pi'$).

1.2 Future work

Our work leaves several fascinating questions open. The main question is to obtain a simpler characterization of convertibility between linear schemes. As a first step, identify pairs of linear schemes Π, Π' over the same field where Π is not convertible to Π', which is not implied by Theorem 27 or Theorem 30. It may be particularly interesting to find a different type of conflicting requirements in the linear system in Section 5, thereby better understanding the easier linear case, which was also studied in the original paper on share conversion [9]. Another concrete question is to characterize the minimal and maximal schemes for various access structures (in other words, those convertible to CNF, or from DNF). As the linear systems introduced in Section 5 work also for non-linear source schemes, it could be also interesting to explore convertibility from such schemes to linear ones. This would require new techniques not based on theorems as above, that both rely on linearity of Π as well.

In evolving setting, proving impossibility results is potentially easier. In our context, it could be interesting to understand whether minimal and/or maximal schemes exist for access structures for which we have not resolved this question.

Finally, it is interesting to find new non-trivial examples of conversions which *are* possible. As an extension, it is interesting to study the direction of converting from a modified subset of a scheme Π where part of the randomness is removed, as we do for a modified version of additive over $\mathbb{Z}_p$ to $\mathbb{Z}_q$, and the incurred privacy losses. The motivation here is that some properties of the original Π may be preserved by such a transformation, which may suffice for certain applications.

2 Prior Work

Share conversion. Cramer et al. [9] first defined share conversion for secret-sharing schemes as a way for converting shares of a secret in one scheme into shares of the same secret in a different scheme using only local computation and no communication between parties. Referring to a conversion between schemes realizing the same access structure and defined over the same field, they showed that CNF can be converted to any linear scheme, and any linear scheme can be converted to DNF. Furthermore, they put forward an application of share conversion to improving efficiency of multiparty computation (MPC). Beimel et al. [5] use generalized share conversion including non-identity relation between secrets from $(2,3)$ CNF to $(3,3)$ additive secret-sharing over different groups to 3-party private information retrieval (PIR). In fact, they observe that certain share conversions are implicit in state-of-the-art 3-party PIR constructions from the literature, and devise another conversions along these lines that induces an improved PIR construction. They also put forward certain impossibility results for certain PIR induced conversions. The following papers [21, 22] show additional positive results for potential conversions for 3-party schemes from the PIR-induced family.

Evolving secret-sharing. Komargodski et al. [17] defined evolving secret-sharing schemes for a case that the number of parties is unbounded, parties are only added as they arrive one after the other, and previously qualified sets remain qualified. They constructed the following evolving linear secret-sharing schemes: (1) a scheme for every evolving access structure, such that, the share size of the t^{th} party is 2^{t-1}; (2) a k-threshold schemes in which the size of the share of party p_t is $O(k \log t)$; (3) an undirected st-connectivity schemes in which the share of each party is a bit.

A natural generalization of an evolving threshold access structure is to allow the threshold to depend on the index of the arriving party. Komargodski and Paskin-Cherniavsky [18] showed that any dynamic-threshold access can be realized with an evolving linear secret-sharing scheme in which the size of the share of party p_t is $O(t^4 \cdot \log t)$. Infinite decision trees were used in [17, 18] to construct evolving secret-sharing schemes. Alon et al. [1] define formally this model. They showed how to construct evolving secret-sharing schemes for generalized infinite decision trees. We use this construction in our work.

Peter in [23] defined evolving conditional disclosure of secrets (CDS), where the number of parties is unbounded, and parties arrive sequentially. Each party holds a private input, and when arrives, it sends a random message to a referee. In turn, at any stage of the protocol, the referee should be able to reconstruct a secret string, held by all the parties, from the messages it gets, if and only if the inputs of the parties that arrived satisfy some condition.

3 Preliminaries

In this section, we present the necessary notation and formal definitions of secret-sharing schemes and evolving secret-sharing schemes.

Notation. For $n \in \mathbb{N}$ by $[n]$ we denote the set $\{1, 2, \ldots, n\}$. We denote by log the logarithmic function with base 2. Vectors are denoted by bold letters (e.g., $\mathbf{r}$). For matrices M, M' with the same number of columns we denote by $[M; M']$ the concatenation of matrix M' below M. For matrices M, M' with the same number of rows, $[M|M']$ is the concatenation of M' to the right for M. By $\text{Rowspan}(M)$ we denote the set of all vectors spanned by rows of M.

For a set of parties $\mathcal{P} = \{p_1, \ldots, p_n\}$, when it is clear from the context, we often abuse notation replacing parties by their indexes from $[n]$. When we refer to a subset of parties $\{p_{i_1}, p_{i_2}, \ldots, p_{i_t}\}$, we assume that $i_1 < i_2 < \cdots < i_t$.

We will need the following well known fact in linear algebra.

▶ **Fact 6.** *Let $\mathbb{F}$ be a field, and $A \in \mathbb{F}^{n\times k}$, $\mathbf{v} \in \mathbb{F}^{1\times k}$ such that $\mathbf{v} \notin \mathrm{Rowspan}(A)$. Then there exists a solution $\mathbf{r}$ to the linear system $[\mathbf{v}|A]\mathbf{r} = (1, 0, \dots, 0)$.*

Finally, we sometimes abuse notation, and use a linear subspace $L = \mathbb{F}^k$ as a matrix consisting of some basis of L as its rows, without explicitly stating so.

3.1 Secret-Sharing

We start by defining (perfect) secret-sharing schemes for a finite set of parties.

▶ **Definition 7** (Access Structures). *Let $\mathcal{P} = \{p_1, \dots, p_n\}$ be a set of parties. A collection $\Gamma \subseteq 2^{\{p_1,\dots,p_n\}}$ is monotone if $B \in \Gamma$ and $B \subseteq C$ imply that $C \in \Gamma$. An access structure $\Gamma \subseteq 2^{\{p_1,\dots,p_n\}}$ is a monotone collection of non-empty sets. Sets in Γ are called authorized, and sets not in Γ are called unauthorized. We will represent an n-party access structure by a function $f : \{0,1\}^n \to \{0,1\}$, where an input (i.e., a string) $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n) \in \{0,1\}^n$ represents the set $A_\sigma = \{p_i : i \in [n], \sigma_i = 1\}$, and $f(\sigma) = 1$ if and only if $A \in \Gamma$. We will also call f an access structure.*

In a monotone access structure, the set $A \in \Gamma$ is called a minterm *if there is no $B \subset A$ such that $B \in \Gamma$. The set $A \notin \Gamma$ is called* a maxterm *if for all $p_i \notin A$ it holds that $A \cup \{p_i\} \in \Gamma$.*

The most basic and well-known access structure is the threshold access structure:

▶ **Definition 8** (Threshold Access Structures). *Let $1 \le k \le n$. A* k-out-of-n threshold access structure Γ *over a set of parties $\mathcal{P} = \{p_1, \dots, p_n\}$ is the access structure containing all subsets of size at least k, that is, $\Gamma = \{A \subseteq P : |A| \ge k\}$.*

A secret-sharing scheme defines a way to distribute shares to parties. Such a scheme is said to realize an access structure Γ if the shares held by any authorized set of parties (i.e., a set in the access structure) can be used to reconstruct the secret, and the shares held by any unauthorized set of parties reveal nothing about the secret. The formal definition follows.

▶ **Definition 9** (Secret-Sharing Schemes). *A secret-sharing scheme Π over a set of parties $\mathcal{P} = \{p_1, \dots, p_n\}$ with domain of secrets S and domain of random strings R is a mapping from $S \times R$ to a set of n-tuples $S_1 \times S_2 \times \cdots \times S_n$ (the set S_j is called the domain of shares of p_j). A dealer distributes a secret $s \in S$ according to Π by first sampling a random string $r \in R$ with uniform distribution, computing a vector of shares $\Pi(s; r) = (\mathsf{sh}_1, \dots, \mathsf{sh}_n)$, and privately communicating each share sh_j to party p_j. For a set $A \subseteq \{p_1, \dots, p_n\}$, we denote $\Pi_A(s; r)$ as the restriction of $\Pi(s; r)$ to its A-entries (i.e., the shares of the parties in A).*

A secret-sharing scheme Π with domain of secrets S realizes an access structure Γ if the following two requirements hold:

Correctness. *The secret s can be reconstructed by any authorized set of parties. That is, for any authorized set $B = \{p_{i_1}, \dots, p_{i_{|B|}}\} \in \Gamma$, there exists a reconstruction function $\mathrm{Recon}_B : S_{i_1} \times \cdots \times S_{i_{|B|}} \to S$ such that for every secret $s \in S$ and every random string $r \in R$, it holds that $\mathrm{Recon}_B(\Pi_B(s; r)) = s$.*

Security. *Every unauthorized set cannot learn anything about the secret from its shares. Formally, for any set $T \notin \Gamma$, every two secrets $s_1, s_2 \in S$, and every possible vector of shares $\langle \mathsf{sh}_j \rangle_{p_j \in T}$, $\Pr\left[\Pi_T(s_1; r) = \langle \mathsf{sh}_j \rangle_{p_j \in T}\right] = \Pr\left[\Pi_T(s_2; r) = \langle \mathsf{sh}_j \rangle_{p_j \in T}\right]$, where the probability is over the choice of r from R with uniform distribution.*

The size of the share of party p_j is defined as $\log |S_j|$ and the size of the shares of Π as $\max_{1 \le j \le n} \log |S_j|$. The total share size of Π is defined as $\sum_{j=1}^{n} \log |S_j|$.

Next we give some widely known secret-sharing schemes.

▶ **Definition 10** (Additive Secret-Sharing Scheme [15]). *In the* additive secret-sharing scheme $ADD_{\mathbb{F},n}$ *over* $\mathbb{F}$*, shares* $\mathsf{sh}_1, ..., \mathsf{sh}_n$ *are sampled uniformly at random from* $\mathbb{F}$ *on the condition that* $s = \sum_{i=1}^{n} \mathsf{sh}_i$*, and* $\Gamma = \{\mathcal{P}\}$*.*

▶ **Definition 11** (Shamir Secret-Sharing Scheme [25]). *In the* (n, k)-Shamir secret-sharing scheme *over* $\mathbb{F}$ *realizing* k*-out-of-*n *threshold access structure* Γ*, the dealer sets a polynomial* $p(x) = s + r_1 x + \cdots + r_{k-1}x^{k-1}$ *by uniformly random sampling of* $r_j \leftarrow \mathbb{F}$ *for* $j \in [k-1]$*. The share of* p_i *for* $i \in [n]$ *is set as* $\mathsf{sh}_i = p(i)$*.*

The properties of Shamir's scheme over $\mathbb{F}_{2^m}$ for an appropriate $m \in \mathbb{N}$ are summarized in the next theorem.

▶ **Theorem 12** (Shamir [25]). *For every* $n \in \mathbb{N}$*, and* $k \in [n]$*, there is a secret-sharing scheme for secrets of size* ℓ *(i.e., the domain of secrets is* $S = \{0,1\}^\ell$*) realizing the* k*-out-of-*n *threshold access structure, in which the share size is* $\max\{\ell, \lceil \log(n+1) \rceil\}$*. Moreover, the shares of the scheme are elements of the field* $\mathbb{F}_{2^{\ell+\log n}}$*.*

Next two schemes realize any monotone access structure. A replicated secret-sharing scheme [14] is also known as a CNF secret-sharing scheme [15].

▶ **Definition 13** (Replicated Secret-Sharing Schemes [14]). *Let* $\Gamma \subseteq 2^{[n]}$ *be a (monotone) access structure, and let* $\mathcal{T}$ *is the set of all maxterms of* Γ*. The CNF secret-sharing schemes for* Γ *over* $\mathbb{F}$*, denoted* $CNF_{\Gamma,\mathbb{F}}$*, proceeds as follows. A secret* $s \in S$ *is shared in* $ADD_{\mathbb{F},|\mathcal{T}|}$*, where each share* r_T *is labelled by a different set* $T \in \mathcal{T}$*. Then, the dealer distributes to each party* p_j *all shares* r_T *such that* $j \notin T$*, that is,* $\mathsf{sh}_j = (r_T)_{j \notin T}$*. For correctness, since* Γ *is monotone, a qualified set* $Q \in \Gamma$ *cannot be contained in any unqualified set, hence, members of* Q *jointly view all shares* r_T *and can thus reconstruct the secret* s*. For privacy, the parties of every maxterm* $T \in \mathcal{T}$ *jointly miss exactly one additive share* r_T*, hence parties of any unqualified set miss at least one share.*

▶ **Definition 14** (DNF Secret-Sharing Scheme [15]). *In DNF secret-sharing schemes, denoted* $DNF_{\Gamma,\mathbb{F}}$*, the secret* s *is additively shared between the parties of each minterm, where each additive sharing uses independent randomness.*

More secret-sharing schemes can be defined using the notion of a monotone span program (MSP). We bring the definition of MSP below.

▶ **Definition 15** (Monotone Span Program [16]). *A* monotone span program *is a triple* $\mathcal{M} = (\mathbb{F}, M, \rho)$*, where* $\mathbb{F}$ *is a field,* M *is an* $m \times k$ *matrix over* $\mathbb{F}$*, and a mapping* $\rho : [m] \to [n]$ *labels each row of* M *by a party's index. The size of* $\mathcal{M}$ *is the number of rows of* M *(i.e.,* m*).*

Next we give some notation which simplifies addressing to sets and operations of MSP. Let $M \in \mathbb{F}^{m \times k}$ be a matrix, and $A \subseteq [m]$. We denote by $M[A, \cdot]$ the $|A| \times k$ dimensional submatrix that restricts M to the rows labeled by $i \in A$. Hence, for an MSP $(\mathbb{F}, M \in \mathbb{F}^{m \times k}, \rho)$ describing an n-party linear secret-sharing scheme, and $h \in [n]$, $M[\rho^{-1}(h), \cdot]$ denotes the submatrix induced by rows of M corresponding to shares of party h. For any $S \subseteq [n]$, for brevity, we will refer to $M[\rho^{-1}(S), \cdot]$ by M_S, and when $S = \{h\}$ for some $h \in [n]$, we will further simplify the notation by referring to $M_{\{h\}}$ as M_h. Similarly, for a column vector $\alpha \in \mathbb{F}^m$, and set $A \subseteq [m]$, we denote by $\alpha[A]$ the sub-vector of α labeled by $i \in A$, and for the subset of parties $S \subseteq [n]$ we let $\alpha_S = \alpha[\rho^{-1}(S)]$, and $\alpha_{\{h\}} = \alpha_h$.

▶ **Definition 16** (Access structure accepted by MSP [16]). *We say that MSP $\mathcal{M}$* accepts *$B \subseteq [n]$ if the rows of M_B span the vector $\mathbf{e_1} = (1, 0, \ldots, 0)$, called* a target vector.[1] *We say that $\mathcal{M}$* accepts an access structure *Γ if $\mathcal{M}$ accepts a set B if and only if $B \in \Gamma$.*

A monotone span program implies a so called *linear secret-sharing scheme* for an access structure containing all the sets accepted by the program. Essentially, a dealer gives each party the rows of matrix M assigned to it, multiplied by the randomness vector.

▷ Claim 17 ([4]). Let $\mathcal{M} = (\mathbb{F}, M, \rho)$ be a MSP accepting an access structure Γ, where $\mathbb{F}$ is a finite field and for every $j \in [n]$ there are a_j rows of M labeled by p_j. Then, there is a linear secret-sharing scheme realizing Γ for $S = \mathbb{F}$ such that the share of party p_j is a vector in $\mathbb{F}^{a_j}$ with the information equal to $\max_{1 \leq j \leq n} a_j$.

3.2 Evolving Secret-Sharing Schemes

In an evolving secret-sharing scheme, defined by [17], the number of parties is unbounded. Parties arrive one after the other; when a party p_t arrives the dealer gives it a share. The dealer cannot update the share later and does not know how many parties will arrive after party p_t. Thus, we measure the share size of p_t as a function of t. We start by defining an evolving access structure, which specifies the authorized sets. The number of parties in an evolving access structure is infinite, however every authorized set is finite.

▶ **Definition 18** (Evolving Access Structures). *Let $\mathcal{P} = \{p_i\}_{i \in \mathbb{N}}$ be an infinite set of parties. A collection of finite sets $\Gamma \subseteq 2^{\mathcal{P}}$ is an* evolving access structure *if for every $t \in \mathbb{N}$ the collections $\Gamma^t \triangleq \Gamma \cap 2^{\{p_1, \ldots, p_t\}}$ is an access structure as defined in Definition 7. We will represent an access structure by a function $f : \{0,1\}^* \to \{0,1\}$, where an input (i.e., a string) $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n) \in \{0,1\}^n$ represents the set $A_\sigma = \{p_i : i \in [n], \sigma_i = 1\}$,[2] and $f(\sigma) = 1$ if and only if $A_\sigma \in \Gamma$. We will also call f an evolving access structure.*

▶ **Definition 19** (Evolving Secret-Sharing Schemes). *Let S be a domain of secrets, where $|S| \geq 2$, and $\{R_t\}_{t \in \mathbb{N}}, \{S_t\}_{t \in \mathbb{N}}$ be two sequences of finite sets. An* evolving secret-sharing scheme *with domain of secrets S is a sequence of mappings $\Pi = \{\Pi^t\}_{t \in \mathbb{N}}$, where for every $t \in \mathbb{N}$, Π^t is a mapping $\Pi^t : S \times R_1 \times \cdots \times R_t \to S_t$ (which returns the share sh_t of p_t).*

An evolving secret-sharing scheme $\Pi = \{\Pi^t\}_{t \in \mathbb{N}}$ realizes an evolving access structure Γ if for every $t \in \mathbb{N}$ the secret-sharing scheme $\Pi_t(s; r_1, \ldots, r_t) \triangleq \left\langle \Pi^1(s; r_1), \ldots, \Pi^t(s; r_1, \ldots, r_t) \right\rangle$ (i.e., the shares of the first t parties) is a secret-sharing scheme realizing Γ^t according to Def. 9.

By default, the domain of secrets of an evolving scheme is $\{0,1\}$. Known results show that every evolving access structure can be realized by an evolving secret-sharing scheme.

▶ **Definition 20** (Evolving Threshold Access Structures). *Let $k \in \mathbb{N}$. The* evolving k-threshold access structure *is the evolving access structure Γ, where Γ^t is the k-out-of-t threshold access structure.*

Komargodski et al. [17] showed that any evolving threshold access structure can be realized by an efficient evolving secret-sharing scheme.

[1] In [16] it is proven that one could define MPS's with any target vector $\epsilon \neq \mathbf{0}$, rather than $\mathbf{e}_1$, resulting in the same matrix size and labeling.

[2] In particular, the same set has infinitely many representations by inputs of various lengths, using sufficiently many trailing zeros.

▶ **Theorem 21** ([17]). *For every $k \in \mathbb{N}$, there is a secret-sharing scheme realizing the evolving k-threshold access structure such that the share size of party p_t is $(k-1)\cdot\log t + \mathrm{poly}(k)\cdot o(\log t)$.*

More evolving asses structures are defined by such structures as *undirected st-connectivity graphs (st-connectivity),* infinite decision trees (IDT), and *generalized infinite decision trees (GIDT)* [1]. Komargodski et al. [17] showed that every undirected st-connectivity access structure can be realized by an evolving secret-sharing scheme in which the share of each party is a bit. Infinite decision trees were used in [17, 18] to construct evolving secret-sharing schemes. Alon et al. [1] showed how to construct secret-sharing schemes for IDT and GIDT. For definitions and constructions we refer to the full version [11].

3.3 Share Conversion

Cramer et al. [9] defined the notion of a share conversion as a local mapping from the shares a secret over one scheme into shares over another scheme, maintaining the secret value. We next include a formal definition of share conversion.[3]

▶ **Definition 22** (Share Conversion). *Let Π, Π' be two secret-sharing schemes over the same secret-domain S for n parties realizing the same access structure. We say that Π is* locally convertible *to Π' if there exist functions $g_1, \ldots, g_n$ such that the following holds. If $(\mathsf{sh}_1, \ldots, \mathsf{sh}_n)$ are valid shares of a secret s in Π (i.e., $\Pr[\Pi(s; \mathbf{r}) = (\mathsf{sh}_1, \ldots, \mathsf{sh}_n)] > 0$), then $(g_1(\mathsf{sh}_1), \ldots, g_n(\mathsf{sh}_n))$ are valid shares of the same secret s in Π'. We denote by g the concatenation of all g_i, namely $g(\mathsf{sh}_1, \ldots, \mathsf{sh}_n) = (g_1(\mathsf{sh}_1), \ldots, g_n(\mathsf{sh}_n))$, and refer to g as a* conversion function*.*

We next extend the definition of share conversion to the evolving setting.

▶ **Definition 23** (Evolving Share Conversion). *Let Π, Π' be two evolving secret-sharing schemes over the same secret-domain S realizing an access structure Γ. We say that Π is* locally convertible *to Π' if there exists a sequence of functions $g_1, g_2, g_3, \ldots$ such that the following holds. For every $t \geq 1$, if $(\mathsf{sh}_1, \ldots, \mathsf{sh}_t)$ are valid shares of a secret s in Π (i.e., $\exists \mathbf{r} \in R_1 \times \ldots \times R_t$ such that $\Pi(s; \mathbf{r}) = (\mathsf{sh}_1, \ldots, \mathsf{sh}_t)$), then $(g_1(\mathsf{sh}_1), \ldots, g_t(\mathsf{sh}_t))$ are valid shares of the same secret s in Π'. We denote by g the concatenation of all g_i, namely $g(\mathsf{sh}_1, \mathsf{sh}_2, \ldots) = (g_1(\mathsf{sh}_1), g_2(\mathsf{sh}_2), \ldots)$, and refer to g as* a conversion function*.*

If the secret-sharing scheme Π is convertible to Π', we say that $\Pi \geq \Pi'$. This defines a partial ordering over secret-sharing schemes. Next, we show that changing a target vector preserves much of the MSP structure, while being convertible to the original scheme.

▷ Claim 24. Let $\Pi = (\mathbb{F}, M \in \mathbb{F}^{m\times k}, \rho)$ is a linear scheme for an access structure Γ with the target vector $\epsilon \in \mathbb{F}^m \setminus \mathbf{0}$. Then for any target vector $\epsilon' \in \mathbb{F}^m \setminus \mathbf{0}$, there exists a linear scheme $\Pi' = (\mathbb{F}, M' \in \mathbb{F}^{m\times k}, \rho)$ for Γ, convertible to Π.

The proof is simply by observing the identity conversion works. See [11] for a full proof.

In linear (MSP-based) schemes, it is convenient to consider a secret s as part of the randomness vector $\mathbf{r}$, being its first coordinate. Sometimes, s is defined by $\mathbf{r}$ in a different manner, which results in a different than $\mathbf{e}_1$ target vector in MSP. For example, in CNF with $\mathbf{1}$ target, as used in [9], the secret is the sum of all elements in $\mathbf{r}$. Thus, we will sometimes consider conversions to a scheme Π' with a certain target vector, and implicitly rely on the implied conversion to Π' with a different target vector.

[3] In [9], they in fact give a slightly more general definition.

4 Impossibility results for linear Share Conversion

Our impossibility results for linear schemes presented in this section follow from the lemma stated below.

▶ **Lemma 25.** *Let* Π, Π' *denote linear secret-sharing schemes realizing* Γ *and specified by MSPs* $(\mathbb{F}, M \in \mathbb{F}^{m\times k}, \rho)$, $(\mathbb{F}, M' \in \mathbb{F}^{m'\times k'}, \rho')$*. Let* $T \cup \{h\}$ *denote a minterm in* Γ *for* $T \subseteq [n], h \in [n]$*, and let* $\alpha_{T\cup h}$, $\alpha'_{T\cup h}$ *be its reconstruction functions for* Π *and* Π'*, respectively. Let* $L = \mathrm{Rowspan}(M_T) \cap \mathrm{Rowspan}(M_h)$*, and* B *denote a basis for* L*. Suppose* g *is some share conversion from* Π *to* Π'*. Then* $(\alpha'_h)^{\mathsf{T}} g_h(M_h\mathbf{r}) = (\alpha_h)^{\mathsf{T}} M_h\mathbf{r} + c(B\mathbf{r})$ *for some function* c*, where* $\mathbf{r}$ *is a randomness vector for* Π*.* [4]

▶ Remark 26. The lemma gives us a high level clue as to why CNF is high up in the convertibility (partial) order for linear schemes of a given access structure, while DNF is so low. In DNF, for every party h, and every minterm $T \cup \{h\}$, it is easy to see that the resulting $L = \{\mathbf{0}\}$. This way, there is "little freedom" in converting determining the converted (sub)share for h (this is formally proved in Theorem 31). On the other hand, in CNF, for a given h and minterm $T \cup \{h\}$, $dim(L)$ is typically large – equal to the number of maxterms H where $H \cap (T \cup \{h\}) \subset T$. This allows for more freedom at choosing the conversion function.

Proof of Lemma 25. First observe that since $T \cup \{h\}$ is a minterm, $(\alpha_h)^{\mathsf{T}} M_h \notin \mathrm{Rowspan}(M_T)$, and hence$(\alpha_h)^{\mathsf{T}} M_h \notin L$. Also, by definition, $B \subseteq \mathrm{Rowspan}(M_h)$. Note that $\{(\alpha_h)^{\mathsf{T}} M_h\} \cup B$ may not constitute a basis of the rows of M_h, it which case, it is complemented by adding a set of appropriate linear combinations of an appropriate set X of rows in M_h. Let M_T^- denote a subset of M_T's rows constituting a basis of $\mathrm{Rowspan}(M_T)$. By choice of B, for any scalar a and vector $\mathbf{v}$ (of the right dimension) there exists randomness $\mathbf{r}$ (one or more) such that $M_T^-\mathbf{r} = \mathbf{v}$, $(\alpha_h)^{\mathsf{T}} M_h\mathbf{r} = a$. Note that $B\mathbf{r}$ is determined by $\mathbf{v}$ (and is otherwise independent of $\mathbf{r}$). In the sequel, for (an implicit or explicit) randomness vector $\mathbf{r}$, we let $\mathbf{v}$, a denote the share portions as above induced by it. As α' is a reconstruction function, and by locality of g and linearity of Π', $\forall\mathbf{r}$ it holds that

$$(\alpha'_{T\cup h})^{\mathsf{T}} g_{T\cup h}(M_{T\cup h}\mathbf{r}) = (\alpha'_h)^{\mathsf{T}} g_h(M_h\mathbf{r}) + (\alpha'_T)^{\mathsf{T}} g_T(\mathbf{v}) = s \tag{1}$$

By Equation (1), and the definition of α we have that

$$(\alpha'_h)^{\mathsf{T}} g_h(M_h\mathbf{r}) = s - (\alpha'_T)^{\mathsf{T}} g_T(M_T\mathbf{r}) = (\alpha_h)^{\mathsf{T}} M_h\mathbf{r} + (\alpha_T)^{\mathsf{T}} M_T\mathbf{r} - (\alpha'_T)^{\mathsf{T}} g_T(M_T\mathbf{r}), \tag{2}$$

where the first term equals to a by definition, and the rest is some function of only $\mathbf{v}$. We denote $(\alpha_T)^{\mathsf{T}} M_T\mathbf{r} - (\alpha'_T)^{\mathsf{T}} g_T(M_T\mathbf{r})$ by $f(\mathbf{v})$. From locality of g, $f(\mathbf{v})$ in fact depends only on $B\mathbf{r}$. To see this, denote $span(M_T^-) = span(B) \oplus span(B_T^-)$ (direct sum of linear subspaces) for an independent set of vectors $B_T^- \subseteq \mathrm{Rowspan}(M_T)$ complementing B into a basis. Using the fact that B is a basis of $\mathrm{Rowspan}(M_h) \cap \mathrm{Rowspan}(M_T)$, it is easy to show that B_T^- with $span(B_T^-) \cap \mathrm{Rowspan}(M_h) = \{\mathbf{0}\}$ indeed exists.

The observation follows by locality, since g_h has no information on $span(B_T^-)\mathbf{r}$ (given $B\mathbf{r}$ that it knows). Also, $(\alpha'_h)^{\mathsf{T}} g_h(M_h\mathbf{r})$ may not depend on $X\mathbf{r}$, as $span(X) \cap \mathrm{Rowspan}(M_T) = \{\mathbf{0}\}$, as then it would not be a (deterministic) function of $\mathbf{v}$.[5] Thus, we have

$$(\alpha'_h)^{\mathsf{T}} g_h(M_h\mathbf{r}) = a + c(B\mathbf{r}) \tag{3}$$

for some function c, as required. ◀

[4] Note that even if $L = \{\mathbf{0}\}$, we are free to pick the constant $c(\mathbf{0})$, which depends only on α in this case.

[5] Note that the above does not imply that $g_h(M_h\mathbf{r})$ does not depend on $X\mathbf{r}$, but rather that it is of the form $g'_h(B\mathbf{r}, a) + g''_h(X\mathbf{r})$, where $g''_h(X\mathbf{r}) = (g''_{h,1}(X\mathbf{r}), \ldots, g''_{h,\ell}(X\mathbf{r}))$ is a vector of functions in the formal variables $X[1]\mathbf{r}, \ldots, X[\ell]\mathbf{r}$, such that $\left(\alpha'_h\right)^{\mathsf{T}} g''_h(X\mathbf{r}) = 0$. Similarly, it implicitly follows that the vector

Next we state two corollaries defining necessary conditions for convertability between linear schemes Π, Π' (as sufficient conditions for non-convertability).

The following theorem is in a sense a generalization of the Claim in Section 3.3 in [9] of non-convertability from Shamir to CNF for $(2,3)$-threshold access structures.

▶ **Theorem 27.** *Let Γ be an access structure on n parties. Let Π and Π' be linear secret-sharing schemes realizing Γ and specified by MSP $(\mathbb{F}, M \in \mathbb{F}^{m\times k}, \rho)$ and $(\mathbb{F}, M' \in \mathbb{F}^{m'\times k'}, \rho')$, respectively. Then, Π has no share conversion to Π' if there exist $h \in [n]$, $\emptyset \neq T \subseteq [n] \setminus \{h\}$ such that $T \cup \{h\}$ is a minterm of Γ with the reconstruction functions α and α' in Π and Π' resp., and $\emptyset \neq T^* \subseteq [n] \setminus \{h\}$ that satisfy the following conditions:*

1. $(\alpha'_h)^\intercal \cdot M'_h \in \mathrm{Rowspan}(M'_{T^*})$.
2. $(\alpha_h)^\intercal \cdot M_h \notin (\mathrm{Rowspan}(M_T) \cap \mathrm{Rowspan}(M_h)) + (\mathrm{Rowspan}(M_{T^*}) \cap \mathrm{Rowspan}(M_h))$.[6]

Proof. Let us assume for contradiction a conversion g exists, and denote $L = \mathrm{Rowspan}(M_T) \cap \mathrm{Rowspan}(M_h)$ and $L^* = \mathrm{Rowspan}(M_{T^*}) \cap \mathrm{Rowspan}(M_h)$. We first show that there exist randomness vectors $\mathbf{r}_1$, $\mathbf{r}_2$ such that:

1. $(L + \mathrm{Rowspan}(M_{T^*}))\mathbf{r}_1 = (L + \mathrm{Rowspan}(M_{T^*}))\mathbf{r}_2 = \mathbf{0}$.
2. $(\alpha_h)^\intercal M_h \mathbf{r}_1 \neq (\alpha_h)^\intercal M_h \mathbf{r}_2$.

Fix $\mathbf{r}_1 = \mathbf{0}$. Then, $(L+\mathrm{Rowspan}(M_{T^*}))\mathbf{r}_1 = \mathbf{0}$ and $(\alpha_h)^\intercal M_h \mathbf{r}_1 = 0$. Next, let us show that $\mathbf{r}_2$ as required exists. We claim $\mathrm{Rowspan}(M_h) \cap (L+L^*) = \mathrm{Rowspan}(M_h) \cap (L+\mathrm{Rowspan}(M_{T^*}))$.

Clearly, former is contained in the latter. For the other direction, consider $x \in \mathrm{Rowspan}(M_h) \cap (L + \mathrm{Rowspan}(M_{T^*}))$. Since L is a subspace of M_h, it suffices to show that if $x \in L + y$ such that $y \in \mathrm{Rowspan}(M_{T^*})$, then $y \in \mathrm{Rowspan}(M_{T^*}) \cap \mathrm{Rowspan}(M_h) = L^*$. Indeed, if $y \in \mathrm{Rowspan}(M_{T^*}) \setminus \mathrm{Rowspan}(M_h)$, then $y + z \notin \mathrm{Rowspan}(M_h)$ for all $z \in L$, which contradicts the fact $x \in \mathrm{Rowspan}(M_h)$; the claim follows.

By this claim and condition 2 of the Theorem, $(\alpha_h)^\intercal M_h \notin L + \mathrm{Rowspan}(M_{T^*})$ since $(\alpha_h)^\intercal M_h \in \mathrm{Rowspan}(M_h)$. Therefore, there exists $\mathbf{r}_2$ such that $(L + \mathrm{Rowspan}(M_{T^*}))\mathbf{r}_2 = \mathbf{0}$ and $(\alpha_h)^\intercal M_h \mathbf{r}_2 = 1 (\neq 0)$, by Fact 6.

By Lemma 25 applied to h, T, when B is the basis for L, we have

$$(\alpha'_h)^\intercal g_h(M_h \mathbf{r}_1) \neq (\alpha'_h)^\intercal g_h(M_h \mathbf{r}_2), \tag{4}$$

since $B\mathbf{r}_1 = B\mathbf{r}_2 (= \mathbf{0})$ and $(\alpha_h)^\intercal M_h \mathbf{r}_1 \neq (\alpha_h)^\intercal M_h \mathbf{r}_2$. On the other hand, by locality, $g_{T^*}(M_{T^*}\mathbf{r}_1) = g_{T^*}(M_{T^*}\mathbf{r}_2) = g_{T^*}(\mathbf{0})$, and thus

$$g_{T^*}(M_{T^*}\mathbf{r}_1) = g_{T^*}(M_{T^*}\mathbf{r}_2). \tag{5}$$

By condition 1 of the theorem, there exists $\mathbf{u}$ such that $(\alpha'_h)^\intercal M'_h = (\mathbf{u})^\intercal M'_{T^*}$. Further, by definition of g, there exists randomness vectors $\mathbf{r}'_1, \mathbf{r}'_2$ for Π' such that $g(M\mathbf{r}_i) = M'\mathbf{r}'_i$ for $i = 1, 2$. Hence,

$$\begin{aligned}(\alpha'_h)^\intercal g_h(M_h\mathbf{r}_1) &= (\alpha'_h)^\intercal M'_h\mathbf{r}'_1 = (\mathbf{u})^\intercal M'_{T^*}\mathbf{r}'_1 = (\mathbf{u})^\intercal g_{T^*}(M_{T^*}\mathbf{r}_1)\\ &= (\mathbf{u})^\intercal g_{T^*}(M_{T^*}\mathbf{r}_2) = (\mathbf{u})^\intercal M'_{T^*}\mathbf{r}'_2 = (\alpha'_h)^\intercal M'_h\mathbf{r}'_2 = (\alpha'_h)^\intercal g_h(M_h\mathbf{r}_2).\end{aligned}$$

The first equality in the second line uses Equation (5). We conclude our proof since the above sequence of equations contradicts Equation (4). ◀

$g_T(M_T\mathbf{r}) = g_T(B\mathbf{r}, B_T^-\mathbf{r})$, of functions is such that $\left(\alpha'_T\right)^\intercal g''_T(B_T^-\mathbf{r})$ is a formal function of $B\mathbf{r}$ only. That is in Fourier basis in the variables $y_1 = B[1]\mathbf{r}, \ldots, y_{|B|} = B[|B|]\mathbf{r}, \ldots, y_i = B_T^-[i - |B|]\mathbf{r}, \ldots, y_k$, it does not contain minterms of the form $\prod_{j\in A} y_j$ where $A \setminus [|B|]$ is not empty. This also poses a certain restriction of g_T which can possibly exploited by future work.

[6] Recall that $U + V = \{u + v | u \in U, v \in V\}$.

The following corollary from Theorem 27 provides necessary conditions for $\Pi_\Gamma \leq CNF_\Gamma$ that are easy to check. These conditions involve only Γ, and the share size of a single party.

▶ **Corollary 28.** *Let Γ denote an access structure on n parties, such that there exists a party h and two minterms T_1, T_2 of size ≥ 2 each, such that $h \in T_1$, $h \in T_2$, $(T_1 \cup T_2) \setminus \{h\}$ is qualified. Let $\Pi = (\mathbb{F}, M \in \mathbb{F}^{m \times k}, \rho)$ be a linear scheme for Γ, and M_h consists of a single row. Then Π is not convertible to $\Pi' = CNF_{\Gamma,\mathbb{F}}$.*

In the proof we apply Theorem 27 to Π, Π', with $T = T_1 \setminus \{h\}$, $T^* = T_2 \setminus \{h\}$. See [11] for details.

▶ Remark 29. From Corollary 28 it follows directly that Shamir secret-sharing scheme is not convertible to CNF, and hence is not maximal. Indeed, any party can be viewed as h, as it obtains a single field element as its share. The condition on the access structure automatically holds for threshold structures.

The following theorem exploits a different property implied by convertability than the previous theorem.

▶ **Theorem 30.** *Let Γ be an access structure on n parties. Let Π, Π' be linear secret-sharing schemes specified for Γ by MSP $(\mathbb{F}, M \in \mathbb{F}^{m \times k}, \rho)$ and $(\mathbb{F}, M' \in \mathbb{F}^{m' \times k'}, \rho')$, respectively. Let $h \in [n]$ denote a party, and let $\mathcal{T}^h = \{T_1, \ldots, T_{v_h}\}$ denote minterms each of which is of size ≥ 2, and contains h. Let $\{\alpha^{T_i}\}_{i \in [v_h]}$ denote a set of reconstruction functions for sets $T_1, \ldots, T_{v_h}$ in Π respectively. Similarly, $\{\alpha'^{T_i}\}_{i \in [v_h]}$ denotes a set of reconstruction functions for $T_1, \ldots, T_{v_h}$ in Π'. Assume the following conditions hold:*

1. *$A = \{\alpha_h^{T_i}\}_{i \in [v_h]}$ constitutes a set of v_h linearly independent vectors.*
2. *$A' = \{\alpha_h'^{T_i}\}_{i \in [v_h]}$ constitutes a (multi)set of vectors with $rank(span(A')) < v_h$.*
3. *$span(\{\alpha^\intercal M_h | \alpha \in A\}) \cap \sum_{i \in [v_h]}(\mathrm{Rowspan}(M_{T_i \setminus h}) \cap \mathrm{Rowspan}(M_h)) = \{\mathbf{0}\}$.*

Then Π has no share conversion to Π'.

Proof. Assume for contradiction that a conversion g exists. Fix some party $h \in [n]$ as guaranteed to exist by the theorem. Consider the matrix $Rec^h = [\left(\alpha_h^{T_1}\right)^\intercal M_h; \ldots; \left(\alpha_h^{T_{v_h}}\right)^\intercal M_h]$. For each $i \in [v_h]$, let $L_i = \mathrm{Rowspan}(M_{T_i \setminus h}) \cap \mathrm{Rowspan}(M_h)$. By condition 1, it is of rank v_h. Therefore, there exists a set $R^h = \{\mathbf{r}^1, \ldots, \mathbf{r}^{|\mathbb{F}|^{v_h}}\}$ of randomness values such that

1. $\{Rec^h \mathbf{r}^j\}_{j \in [|\mathbb{F}|^{v_h}]}$ goes over all distinct vectors in $\mathbb{F}^{v_h}$.
2. For every $j \in |\mathbb{F}|^{v_h}, i \in [v_h]$, $L_i \mathbf{r}^j = \mathbf{0}$.

Such a set R^h exists, by combining conditions 1 and 3 in the Theorem. Now, let us consider the matrix $Rec'^h = [\left(\alpha'^{T_1}_h\right)^\intercal M_h; \ldots; \left(\alpha'^{T_{v_h}}_h\right)^\intercal M_h]$, and let $R'^h = \{\mathbf{r}'^1, \ldots, \mathbf{r}'^{|\mathbb{F}|^{v_h}}\}$ denote the set of effective randomness vectors induced by the conversion g (that is $M'\mathbf{r}'^j = g(M\mathbf{r}^j)$). By condition 2 in the Theorem, $rank(Rec'^h) < v_h$. Therefore, $span(\{Rec'^h \mathbf{r}'^j\}_{j \in |\mathbb{F}|^{v_h}})$ is of dimension at most $v_h - 1$, and thus contains at most $|\mathbb{F}|^{v_h - 1}$ distinct values. However, by Lemma 25, for every $i \in [v_h], j \in [|\mathbb{F}|^{v_h}]$ we have

$$Rec'^h[i]\mathbf{r}'^j = Rec^h[i]\mathbf{r}^j + c^i(\mathbf{0})$$

That is, $c^j(\mathbf{0})$ is some constant, independent of $\mathbf{r}^j$. Therefore,

$$R'^h \mathbf{r}'^j = R^h[j]\mathbf{r}^j + \mathbf{c}$$

where $\mathbf{c}$ is a constant vector. Going over all values of j, on the RHS we obtain a permutation of the set $\mathbb{F}^{v_h}$, but on the LHS, we only get a subset of at most $|\mathbb{F}|^{v_h - 1}$ (constituting a linear subspace) – a contradiction. ◀

The above theorem implies that DNF can only be converted to linear schemes of size at least that of the DNF. More precisely:

▶ **Theorem 31.** *Let Γ be an access structure over $n > 1$ parties, and $\mathbb{F}$ be a finite field. For simplicity, assume Γ has no redundant parties. Let Π' be a linear secret-sharing scheme specified by MSP $\mathcal{M}' = (\mathbb{F}, M' \in \mathbb{F}^{m' \times k'}, \rho')$ for Γ. If $\mathcal{M} = DNF_{\Gamma,\mathbb{F}} = (\mathbb{F}, M \in \mathbb{F}^{m \times k}, \rho)$ is convertible to Π', then* [7]

$$m' \geq \sum_{T:T \text{ is a minterm of } \Gamma} |T|.$$

Proof. Consider some $h \in [n]$ that belongs to some minterm T of size at least 2. Let $\mathcal{T}^h = \{T_i \text{ is a minterm} | |T_i| \geq 2, h \in T_i\}$, and denote $v_h = |\mathcal{T}^h|$. The (unique, in case of DNF) reconstruction function projection set $A = \{\alpha_h^{T_i}\}$ are all linearly independent by construction of DNF. Namely, each selects a single row in M_h, and $\left(\alpha_h^{T_i}\right)^\intercal M_h$ is either of the form $r_{i,h}$ or of the form $s - \sum_{k \in T_i \setminus h} r_{i,k}$, where $r_{i,j}$ is a random element used by the DNF in the additive sub-scheme for minterm T_i and party j.

For a fixed $k \in [v_h]$, by structure of DNF, we have $\text{Rowspan}(M_{T_k \setminus h}) \cap \text{Rowspan}(M_h) = \mathbf{0}$. Therefore, $\sum_{k \in [v_h]} \left(\text{Rowspan}(M_{T_k \setminus h}) \cap \text{Rowspan}(M_h)\right) = \{\mathbf{0}\}$. Thus, A satisfies conditions 1 and 3 of Theorem 30 relative to $\mathcal{T}^h$.

It follows from Theorem 30 that A' is of dimension $\geq v_h$. Thus, the matrix $A'M'_h$ (where A' is treated as a matrix constructed from the vectors of A' as rows) also has dimension at least v_h. This implies M'_h itself is of rank at least v_h, which in turn lower bounds its number of rows.

Parties that constitute a singleton minterm, contribute at least 1 to $rank(M'_h)$, as the party contained in the minterm is not redundant. Going over all parties h, the result follows by changing the order of summation, obtaining.

$$m' \geq \sum_h \sum_{T:T \text{ is a minterm}, h \in T} 1 = \sum_{T:T \text{ is a minterm}} |T| \tag{6}$$

◀

▶ Remark 32. Theorem 31, in fact, states that DNF is not convertible to any linear scheme with lower share complexity, in particular, in the Shamir secret sharing scheme. The non-minimality of Shamir follows.

▶ Remark 33. In fact, the above theorem can be fairly easily generalized to Π where $span(\{\alpha^\intercal M_h | \alpha \in A\}) \cap \sum_{i \in [v_h]} (\text{Rowspan}(M_{T_i \setminus h}) \cap \text{Rowspan}(M_h)) = U$ for some h has a "relatively small" dimension u. Then, we can prove $dim(span(A)) - u$ lower bounds $rank(M'_h)$ if $\Pi \leq \Pi'$. That is, the smaller u relatively to $dim(span(A))$ is, the higher the share complexity of party h in Π' must be.

5 A characterization of convertability between linear schemes

Let Γ be an access structure on n parties. Let Π, Π' be linear secret-sharing schemes specified by MSPs $(\mathbb{F}, M \in \mathbb{F}^{m \times k}, \rho)$ and $(\mathbb{F}, M' \in \mathbb{F}^{m' \times k'}, \rho')$, respectively, realizing Γ. We devise a characterization of convertibility from Π to Π' by solvability of a certain system of linear equations. Essentially, every solution of the system represents a conversion function g. Namely, for every randomness vector from Π, it defines converted shares for Π'.

[7] In fact, the number of rows assigned to each party is at least as large as in DNF.

The linear system $\mathcal{L}_{\Pi,\Pi'}$. For each randomness vector $\mathbf{r} \in \mathbb{F}^m$ we define a variable $X^{(\mathbf{r})} \in \mathbb{F}^{m'}$, that assumes a value for the purported sharing under M' induced by the share conversion of $M \cdot \mathbf{r}$. The constraints we define are as follows.

- **Locality.** For every $i \in [n]$ and $\mathbf{r}, \mathbf{r}' \in \mathbb{F}^m$ such that $M_i \cdot \mathbf{r} = M_i \cdot \mathbf{r}'$, add the constraint:
  $$X_i^{(\mathbf{r})} = X_i^{(\mathbf{r}')}.$$
- **Consistency.** Let $A \subseteq [m']$ be a subset of rows of M' which form a basis of Rowspan(M'). Since $M'[A, \cdot]$ is a basis of Rowspan(M'), there exists a (unique) matrix $H \in \mathbb{F}^{m', |A|}$ such that $H \cdot M'[A, \cdot] = M'$. For every $\mathbf{r} \in \mathbb{F}^m$, we add the constraint
  $$H \cdot X^{(\mathbf{r})}[A] = X^{(\mathbf{r})}.$$
- **Correctness.** For each minterm $T \subset [n]$ of Γ do the following: let $\alpha'^T \in \mathbb{F}^{|(\rho')^{-1}(T)|}$ be a smallest reconstruction vector for T under some arbitrary ordering of $\mathbb{F}^{|(\rho')^{-1}(T)|}$). For every $s \in \mathbb{F}$, and every $\mathbf{r}$ such that $\mathbf{r}[1] = s$, add the constraint
  $$\left(\alpha'^T\right)^{\mathsf{T}} \cdot X_T^{(\mathbf{r})} = s.$$

▶ Remark 34. The characterization may be easily extended to non-linear Π with $S = \mathbb{F}$, keeping the system linear.

▶ **Theorem 35.** *Let Γ be an access structure on n parties. Let Π, Π' be linear secret-sharing schemes specified by MSPs $(\mathbb{F}, M \in \mathbb{F}^{m \times k}, \rho)$ and $(\mathbb{F}, M' \in \mathbb{F}^{m' \times k'}, \rho')$, respectively, realizing Γ. Then, Π is convertible to Π' if and only if the linear system $\mathcal{L}_{\Pi,\Pi'}$ is solvable.*

Proof. Both directions essentially follow from the fact that the solution set to $\mathcal{L}_{\Pi,\Pi'}$ exactly corresponds to the set of conversions from Π to Π'. See [11] for a formal proof. ◀

Theorems 27 and 30 may be viewed as a result of an inconsistency in the characterization equations. In Theorem 27, the inconsistent subset of equations supported only on $X^{(\mathbf{r}^1)}, X^{(\mathbf{r}^2)}$ for a pair $\mathbf{r}_1, \mathbf{r}_2$ as chosen in the proof, and the inconsistency involves a potentially large set of $\mathbf{r}^j$'s, already. Lemma 25 relies on equations of all three types to derive its conclusion.

Future work. We believe that there exist additional types of "inconsistencies" in the linear equations in the characterization that may result in proving non-existence of a conversion from between pairs of linear schemes Π to Π', and it is an interesting open question to list all possible types of inconsistencies, and thereby make the above characterization easier to apply. Most importantly, we wish to understand when conversions between linear schemes *do* exist. Another interesting open question on convertability between pairs of linear schemes is understanding whether it is helpful to have non-linear conversion functions g.

6 Impossibility of conversion to CNF for general schemes

In this section, we introduce the class of non-degenerate secret-sharing schemes, which includes CNF and Shamir schemes, and, using properties of non-degenerate schemes, we prove a necessary condition of convertibility to CNF from any (not necessarily linear) scheme.

▶ **Definition 36.** *Let Π be a secret-sharing scheme with secret domain S and randomness domain R realizing an access structure Γ. Π is* non-degenerate *if the following holds: If Π' is a secret-sharing scheme with secret domain S and randomness domain R' realizing Γ such that, for all $s \in S, r' \in R'$, there exists $r \in R$ such that $\Pi'(s; r') = \Pi(s; r)$, then*

$$(\Pi'(s; r')|r' \leftarrow R') \equiv (\Pi(s; r)|r \leftarrow R), \forall s \in S. \tag{7}$$

Suppose Π is a non-degenerate secret-sharing scheme. If a secret-sharing scheme Π' is locally convertible to Π, then the secret-sharing scheme induced by the applying the share conversion function to Π' coincides with Π.

▶ **Proposition 37.** *Let Π be a non-degenerate secret-sharing scheme with secret domain S and randomness domain R realizing access structure Γ over n parties. Suppose Π' be a secret-sharing scheme with the same secret domain and access structure and randomness domain R' that admits share conversion to Π using a share conversion function $g = (g_1, \dots, g_n)$. Then, for all $s \in S$,*

$$(g(\Pi'(s; r'))|r' \leftarrow R') \equiv (\Pi(s; r)|r \leftarrow R)\,. \tag{8}$$

Proof. Consider the secret-sharing scheme in which $s \in S$ is secret shared as $(\mathsf{sh}_1, \dots, \mathsf{sh}_n) = g(\Pi'(s, r'))$ where $r' \leftarrow R'$. Since g is a share conversion function that converts Π' to Π, this induces secret-sharing scheme with secret domain S realizing the access structure Γ. Further, for each $s \in S$ and $r' \in R'$, $g(\Pi'(s; r')) = \Pi(s; r)$ for some $r \in R$. The proposition now follows from the fact that Π is a non-degenerate secret-sharing scheme (See Definition 36). ◀

We establish that CNF and Shamir secret sharing schemes are non-degenerate. The proofs of these claims follow the outline sketched in Section 1.1; their formal proofs are deferred to the full version.

▶ **Lemma 38.** *For any finite group $\mathbb{G}$, and access structure Γ over n parties, the CNF secret-sharing scheme for secrets in $\mathbb{G}$ realizing Γ is non-degenerate.*

▶ **Lemma 39.** *For any finite field $\mathbb{F}$ such that $|\mathbb{F}| > n$, and $1 \le t \le n$, a t-private n-party Shamir secret-sharing scheme over $\mathbb{F}$ is non-degenerate.*

We exploit the non-degeneracy of CNF secret sharing to establish lower bound on share size in any (potentially non-linear) secret sharing schemes that admit share conversion to CNF secret sharing.

▶ **Theorem 40.** *Let Π be a secret-sharing scheme with secret domain $\mathbb{G}$ and randomness domain R realizing an n-party access structure Γ. There is a share conversion from Π to CNF secret-sharing over $\mathbb{G}$ realizing Γ only if, for each $i \in [n]$, size of the share i in Π is at least $\log |\mathbb{G}| \cdot |\{F \in \mathcal{F}$ s.t. $i \notin F\}|$, where $\mathcal{F}$ is the set of all maximal forbidden sets associated with Γ.*

Proof. By Lemma 38, the CNF secret-sharing scheme is non-degenerate. Let $g = (g_1, \dots, g_n)$ be the share conversion function that induces the share conversion from Π to the CNF secret-sharing scheme. By Proposition 37, for any $s \in \mathbb{G}$, when $r \leftarrow R$, $g(\Pi(s; r))$ is identically distributed as CNF secret-sharing of s. Hence, $g_i(\Pi(s; r))$ corresponds to the share of party i in CNF secret-sharing: $\{\gamma_F : F \in \mathcal{F}, i \notin F\}$ where γ_F is uniformly chosen from $\mathbb{G}$ for each $F \in \mathcal{F}$ subject to $\sum_F \gamma_F = s$. Theorem follows immediately from this observation. ◀

7 Results for Evolving Linear Secret-Sharing Schemes

In this section, we extend the notion of Monotone Span Programs and the induced notion of a linear secret-sharing scheme to the evolving setting. We then apply our impossibility results obtained is Sections 4 and 6 for the finite case to study the convertibility hierarchy in this setting.

Monotone span programs [16] were used to construct linear secret-sharing schemes in [4]. In this section, we extend Definition 15 to define infinite monotone span programs and cast a few constructions from the literature as instances of this notion. We define the product of an infinite matrix $K \in \mathbb{F}^{[n]\times\mathbb{N}^+}$ by a finite vector $\mathbf{r} \in \mathbb{F}^{[m]}$ as $K'\mathbf{r}$, where K' is obtained by keeping the first m columns of K. We will typically use such products for matrices where all but the first m columns are 0. Generalizing this notion to the evolving setting, we dub IMSP, requires some care. Roughly, in an IMSP $M(\mathbb{F}, M, \rho)$ $|\rho^{-1}(i)|$ is finite for all i, every row, as well as the target vector (typically $\mathbf{e}_1 = (1, 0, \dots, 0)$) have finitely many non-0 elements. See [11] for a formal definition. [8]

In the following theorem, we generalize the MSP-based linear secret-sharing schemes to the evolving setting, essentially giving each party the linear combinations of a randomness vector (that also defines the secret s), as specified by the IMSP. As in the finite case, every finite subset $A \subseteq \mathbb{N}^+$ either reconstructs the secret, or learns nothing about it.

▶ **Theorem 41.** *Let $\mathcal{M} = (\mathbb{F}, M, \rho)$ be an IMSP accepting an access structure Γ. Then, Construction 42 instantiated with $\mathcal{M}$ implements Γ.*

▶ **Construction 42.** *Consider an IMSP $\mathcal{M}(\mathbb{F}, M, \rho)$.*

- *INPUT: a secret $s \in \mathbb{F}$.*
  We determine $r_0 = s$ and define $\mathbf{r} = (s, r_1, r_2 \dots)$.
- *SHARE: To generate sh_i the dealer does the following:*
  1. *Gets as input $(s, \mathsf{sh}_1, \dots, \mathsf{sh}_{i-1})$, that is, a secret s and the shares of parties $p_1, \dots, p_{i-1}$. For convenience, we assume it in fact receives the set of $r_1, \dots, r_j$'s sampled so far, for $j = max(C_{[i-1]})$. It samples random independent elements $r_{j+1}, \dots, r_{j+d} \in \mathbb{F}$ for $j + d = max(C_{[i]})$.*
  2. *Set $\mathsf{sh}_i = M_i\mathbf{r}$, where $\mathbf{r}$ is the prefix of $\mathbf{r}$ sampled so far.*
- *RECON: Let α denote the (finite) reconstruction vector such that $\alpha^T M_B = \mathbf{e_1}$. Return $< \alpha, \Pi(B) >$.*

The proof of this theorem is deferred to the main version [11] and re-interprets the construction of [1] as an IMSP based scheme. We define *evolving linear secret-sharing schemes* as the set of schemes so specified by an IMSP.

For constructions for the evolving threshold, and for the evolving undirected *st*-connectivity access structures families as instances of IMSP, we refer the reader to the full version [11].

▶ **Theorem 43.** *Let Γ denote an evolving access structure. Then GIDT [1, Construction 3.9] for $S = \mathbb{F}_2$ and Γ instantiated so that edge predicates are implemented by linear schemes over $\mathbb{F}_2$ is (evolving) linear.*

The proof immediately follows from observing the GIDT [1] given as Construction 3.9.

The following theorem states that for a large class of evolving access structures there is no minimal linear evolving secret-sharing scheme. This proof follows from Theorem 27 applied to any specific evolving scheme and a tailor crafted GIDT scheme [1, Construction 3.9], and is deferred to the full version [11].

[8] We use a "working definition" of linear evolving secret-sharing schemes specified by an IMSP, which is a natural extension of the finite case. An arguably more intuitive definition requires that all shares are linear combinations of the r_i's and s (over a field $\mathbb{F}$) without the restriction on reconstruction. Beimel has demonstrated in [3] that linear schemes imply MSPs of similar share complexity, so the definitions are equivalent. We do not demonstrate such a result in this paper, but it would be useful to demonstrate in future work on the theory of linear evolving schemes.

▶ **Theorem 44.** *Consider an evolving access structure Γ such that there exists $\tilde{h} \in [n]$, and an infinite collection of minterms $A = \{T_i\}_{i\in\mathbb{N}}$ where $\tilde{h} \in T_i$ for all $i \in \mathbb{N}$. Then, for any linear scheme $\tilde{\Pi}$ specified by M over $\mathbb{F}_2$, there exists an evolving linear scheme $\tilde{\Pi}'$ specified by M' over $\mathbb{F}_2$ for Γ, such that $\tilde{\Pi}'$ is not convertible to $\tilde{\Pi}$.*

Next, using results obtained in Section 6, we prove the absence of a maximal evolving scheme in a wide class of evolving secret-sharing schemes, even not necessarily linear.

▶ **Definition 45** (Trivial Evolving Access Structures)**.** *An evolving access structure Γ is said to be* trivial if there exists $N \in \mathbb{N}$ such that, for all $n > N$, $\{n\} \in \Gamma$ or for all finite set A, $A \in \Gamma$ only if $A \setminus \{n\} \in \Gamma$.

▶ **Theorem 46.** *Any non-trivial evolving access structure Γ and finite field $\mathbb{F}$ has no maximal evolving secret-sharing scheme over $\mathbb{F}$.*

Proof. We will need the following technical claim on evolving access structures (see [11] for a proof).

▷ Claim 47. If Γ is nontrivial, then for any $k \in \mathbb{N}$, there exists $n \in \mathbb{N}$ such that $|\{F \in \mathcal{F}_n : 1 \notin F\}| \geq k$, where $\mathcal{F}_n$ is the set of max-terms of Γ_n.

Now, let Π be a purported maximal secret-sharing scheme for one bit secrets realizing the access structure Γ. Let $|\mathsf{sh}_1|$ be the share size of the share assigned to party 1 by Π. By the above claim, there exists n such that, when $\mathcal{F}_n$ is the set of max-terms of Γ_n, $|\{F \in \mathcal{F}_n : 1 \notin F\}| > |\mathsf{sh}_1|$. Consider the GIDT-based construction Π' for Γ of [1] with the first generation consisting of n parties, and a CNF implementation of Γ_n, in the edge going from the root to a leaf. By Theorem 40, Π does not have a share conversion to Π' since the size of share i is less than $|\{F \in \mathcal{F}_n : 1 \notin F\}| > |\mathsf{sh}_1|$. ◀

8 Extensions and applications

Above, we considered secret-share conversion for schemes defined over the same field. It this section, we discover the possibility to perform share conversion between schemes over different fields. We show that the most of our impossibility results is applicable to the case when the source and target schemes are defined over the fields of the same characteristic, and when characteristics are different, the conversion is not possible for many access structures.

8.1 Extending impossibility results to schemes over different fields of the same characteristics

In this section, we extend our impossibility results following from Theorem 27 to secret sharing schemes defined over distinct fields of the same characteristic. For this, we slightly restate Lemma 25 and Theorem 27 such that Π and Π' are two secret sharing schemes defined over $\mathbb{F}$ and $\mathbb{F}'$, respectively, which are the extension fields of $\mathbb{F}_p$.

▶ **Observation 48.** *Lemma 25 holds for secret-sharing schemes Π defined by MSP $(\mathbb{F}, M \in \mathbb{F}^{m\times k}, \rho)$ and Π' defined by MSP $(\mathbb{F}', M' \in \mathbb{F}'^{m'\times k'}, \rho')$ with the secret domain $\mathbb{F}_p$, where $\mathbb{F}$ and $\mathbb{F}'$ are extension fields of $\mathbb{F}_p$ for prime p.*

Proof. The proof is the same as the proof of Lemma 25, with the difference that (1) holds over $\mathbb{F}'$, Equation (2) is over $\mathbb{F}^*$ which is the extension field for both $\mathbb{F}$ and $\mathbb{F}'$, and Equation (3) is over $\mathbb{F}'$ (where function c is over $\mathbb{F}^*$ with the output in $\mathbb{F}'$). ◀

▶ **Observation 49.** *Theorem 27 holds for secret-sharing schemes* Π *defined by MSP* $(\mathbb{F}, M \in \mathbb{F}^{m\times k}, \rho)$ *and* Π' *defined by MSP* $(\mathbb{F}', M' \in \mathbb{F}'^{m'\times k'}, \rho')$ *with the secret domain* $\mathbb{F}_p$*, where* $\mathbb{F}$ *and* $\mathbb{F}'$ *are extension fields of* $\mathbb{F}_p$ *for prime* p*.*

Proof. The proof of this observation is the same as the proof of Theorem 27, where all the equations before (4) are over $\mathbb{F}$. To obtain Equation (4), we apply Theorem 27 under Observation 48 which facilitates the transition to the field $\mathbb{F}'$. Equations (4), (5), and all the following proof are constructed over $\mathbb{F}'$. ◀

We rely on the above observation to extend our impossibility result in Corollary 28 for conversion from certain linear schemes to CNF. In the observation below, both source and target schemes work for sharing secrets in the larger domains $\mathbb{F}$, $\mathbb{F}'$, but are used only to share secrets in the base field $\mathbb{F}_p$. Any such scheme may be viewed as a scheme over the smaller field S, where each party, including h receives several field elements, which correspond to operations over $\mathbb{F}_p$. Shamir over a large extension field of $\mathbb{F}_p$ is one example of such a scheme.

▶ **Observation 50.** *Corollary 28 holds for secret-sharing schemes* Π *defined by MSP* $(\mathbb{F}, M \in \mathbb{F}^{m\times k}, \rho)$ *and* $\Pi' = CNF_{\Gamma,\mathbb{F}'}$ *with the secret domain* $\mathbb{F}_p$*, where* $\mathbb{F}$ *and* $\mathbb{F}'$ *are extension fields of* $\mathbb{F}_p$ *for prime* p*.*

Proof. The proof of this observation is the same as the proof of Corollary 28, where Theorem 27 is applied under Observation 48. ◀

The above result is not subsumed by Theorem 40, as it allows $\mathbb{F}$ to be much larger than $\mathbb{F}'$.

8.2 Negative result for the inter-field conversion

It is often useful in applications to perform share conversion between schemes over different fields of different characteristic. A natural choice of a secret domain for such a conversion is $\{0, 1\}$, as these values belong to all finite fields. Furthermore, these values can be viewed as bits, which is the most useful setting for most MPC protocols. In this section, we show that a local conversion, in general, is not possible (even from CNF) for many access structures. However, below we show a specially tailored leaky secret-sharing scheme over field $\mathbb{Z}_p$ which allows local conversion to a different field $\mathbb{Z}_q$ for $q < n/2$ for (n, n)-threshold.

Next, we observe that for all pairs $p \neq q$, and many access structures Γ, one can not convert from $CNF_{\Gamma,\mathbb{F}_p}$ to $\Pi_{\Gamma,\mathbb{F}_q}$, where $\Pi_{\Gamma,\mathbb{F}_q}$ is any linear scheme over q for that share. More precisely, we have

▶ **Theorem 51.** *Let* Γ *denote an access structure for* $n > 1$ *parties, such that for all maxterms* B_1, B_2*,* $B_1 \cup B_2 = [n]$.[9] *Let* $p \neq q$ *be primes, and* $CNF_{\Gamma,\mathbb{F}_p}$ *and* $\Pi_{\Gamma,\mathbb{F}_q}$ *linear schemes for* Γ *over* $\mathbb{F}_p, \mathbb{F}_q$ *respectively. Then* $CNF_{\Gamma,\mathbb{F}_p}$ *is not convertible to* $\Pi_{\Gamma,\mathbb{F}_q}$ *for secret domain* $S = \{0, 1\}$ *(that is, we do not care how other secrets are converted).*

The theorem follows almost immediately from a variant of Lemma 25 for different fields p, q which we provide below (see full version [11] for a proof).

▷ Claim 52. Let $\Pi = (\mathbb{F}_p, M \in \mathbb{F}_p^{m\times\ell}, \rho)$, $\Pi' = (\mathbb{F}_q, M' \in \mathbb{F}_q^{m'\times\ell'}, \rho')$ for a pair of primes $p \neq q$, and let $T \cup \{h\}$ denote a minterm of Γ. Let $\alpha_{T\cup h}, \alpha'_{T\cup h}$ be reconstruction functions for $T \cup \{h\}$ in Π and Π' respectively. Assume $L = \text{Rowspan}(M_T) \cap \text{Rowspan}(M_h) = \{\mathbf{0}\}$. Then for every

[9] For instance, the $(\lceil n/2\rceil + 1, n)$-threshold access structure.

conversion scheme g from Π to Π' there exists a sequence $\mathbf{r}_1, \ldots, \mathbf{r}_i, \ldots \in \mathbb{Z}^\ell$ and constant $c \in \mathbb{Z}$ such that (1) $(\alpha'_h)^\mathsf{T} g_h(M_h\mathbf{r}_i \mod p) \equiv i + c \pmod q$; (2) $(\alpha_h)^\mathsf{T} M_h\mathbf{r}_i \equiv i \pmod p$ for all $i \in \mathbb{N}^+$, and (3) $\langle \mathbf{r}_i, \mathbf{e}_1 \rangle \mod p \in \{0, 1\}$. We conclude that such a g does not exist if $p \neq q$.

Proof of Theorem 51. Finally, the theorem follows from Claim 52 by observing that for $n > 2$, in $CNF_{\Gamma,\mathbb{F}_p}$ each party p_i gets a subset of independent random vectors over $\mathbb{F}_p$, namely $\mathbf{r}_T$ of each maxterm T such that $i \notin T$. The sets of $\mathbf{r}_H$'s that h holds, vs those T holds. Assume the contrary – that $h \notin H$ and $T \cap H = \emptyset$. In that case $i \notin T \cup H$, contradicting the assumptions that $T \cup H = [n]$ (as T, H are maxterms). This implies that for $CNF_{\Gamma,\mathbb{F}_p}$, $L = \{\mathbf{0}\}$, so the conditions of Claim 52 are indeed satisfied by $\Pi = CNF_{\Gamma,\mathbb{F}_p}$ and $\Pi' = \Pi_{\Gamma,\mathbb{F}_q}$. ◀

8.3 The specially tailored additive secret-sharing scheme allowing inter-field conversion

Next, we build the secret-sharing scheme over the field $\mathbb{Z}_p$, and define the conversion function to the field $\mathbb{Z}_q$. The scheme implies some restrictions on the randomness of the dealer, and also is not perfectly secure. However it's existence raises a question if there are statistical secure secret-sharing schemes allowing an inter-field conversion, and how small the leakage could be. The other question is about the possibility to convert the original additive scheme over $\mathbb{F}_p$ to a perfectly private scheme over $\mathbb{F}_q$, by using the entire randomness domain of the former. This way, privacy of the converted scheme automatically holds by locality of the conversion scheme. Correctness is the only measure that suffers, with some small probability. This way, we are talking about a conversion scheme between the same pair of perfect schemes Π, Π', while the conversion scheme itself is statistically correct.

The n-party additive convertible scheme $ADD_{p\to q}$.
Parameters: $p \neq q$ are primes such that $q < n/2$.
Sharing algorithm:

(1) the dealer for each $i \in [n]$ samples $r_i \leftarrow \mathbb{Z}_p$.
(2) If $\sum_{i=1}^n r_i = kpq + s$, where $s \in \{0, 1\}$ for some k then output $\mathsf{sh}_i := r_i$ and terminate. Otherwise go to Step 1.

Conversion function: Each p_i computes $\mathsf{sh}'_i = \mathsf{sh}_i \mod q$.

This scheme is **correct** by construction, with **polynomial computational complexity**, and statistical **leakage** less or equal to $p_{leak} = \frac{1}{p} + o\left(\frac{1}{p^2 n}\right)$ (see the full version [11]).

The convertible additive scheme is the basic case for creating the convertible CNF and DNF schemes. However, even directly it could have several applications, similar to applications of *dBits*. For more details, we refer to the full version [11]. We leave the existence of practical inter-field convertible secret-sharing schemes with the statistical, or even computational security, as the open question for the future research.

References

1 Bar Alon, Amos Beimel, Tamar Ben David, Eran Omri, and Anat Paskin-Cherniavsky. New upper bounds for evolving secret sharing via infinite branching programs. Cryptology ePrint Archive, Paper 2024/419, 2024. URL: `https://eprint.iacr.org/2024/419`.

2 Abdelrahaman Aly, Emmanuela Orsini, Dragos Rotaru, Nigel P Smart, and Tim Wood. Zaphod: Efficiently combining LSSS and garbled circuits in SCALE. In *Proceedings of the 7th ACM Workshop on Encrypted Computing & Applied Homomorphic Cryptography*, pages 33–44, New York, NY, USA, 2019. Association for Computing Machinery. `doi:10.1145/3338469.3358943`.

3 A. Beimel. Secure schemes for secret sharing and key distribution. *Phd thesis*, 1996.

4 Amos Beimel. Secret-sharing schemes: A survey. In Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing, editors, *Coding and Cryptology*, pages 11–46, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg. `doi:10.1007/978-3-642-20901-7_2`.

5 Amos Beimel, Yuval Ishai, Eyal Kushilevitz, and Ilan Orlov. Share conversion and private information retrieval. In *Proceedings - 2012 IEEE 27th Conference on Computational Complexity, CCC 2012*, Proceedings of the Annual IEEE Conference on Computational Complexity, pages 258–268, September 2012. IEEE Computer Society Technical Committee on Mathematical Foundations of Computing ; Conference date: 26-06-2012 Through 29-06-2012. `doi:10.1109/CCC.2012.23`.

6 Aner Ben-Efraim. On multiparty garbling of arithmetic circuits. In *Advances in Cryptology–ASIACRYPT 2018: 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part III 24*, pages 3–33, Cham, 2018. Springer, Springer International Publishing. `doi:10.1007/978-3-030-03332-3_1`.

7 Aner Ben-Efraim, Lior Breitman, Jonathan Bronshtein, Olga Nissenbaum, and Eran Omri. MYao: Multiparty "Yao" garbled circuits with row reduction, half gates, and efficient online computation. *Cryptology ePrint Archive*, 2024. URL: `https://eprint.iacr.org/2024/1430`.

8 Dan Boneh, Yuval Ishai, Alain Passelègue, Amit Sahai, and David J Wu. Exploring crypto dark matter: New simple PRF candidates and their applications. In *Theory of Cryptography Conference*, pages 699–729, Cham, 2018. Springer, Springer International Publishing. `doi:10.1007/978-3-030-03810-6_25`.

9 Ronald Cramer, Ivan Damgård, and Yuval Ishai. Share conversion, pseudorandom secret-sharing and applications to secure computation. In Joe Kilian, editor, *Theory of Cryptography*, pages 342–362, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg. `doi:10.1007/978-3-540-30576-7_19`.

10 Ivan Damgard and Rune Thorbek. Efficient conversion of secret-shared values between different fields. *Cryptology ePrint Archive*, 2008. URL: `https://eprint.iacr.org/2008/221`.

11 Tamar Ben David, Varun Narayanan, Olga Nissenbaum, and Anat Paskin-Cherniavsky. New results in share conversion, with applications to evolving access structures. *Cryptology ePrint Archive*, 2024. URL: `https://eprint.iacr.org/2024/1781`.

12 Itai Dinur, Steven Goldfeder, Tzipora Halevi, Yuval Ishai, Mahimna Kelkar, Vivek Sharma, and Greg Zaverucha. MPC-friendly symmetric cryptography from alternating moduli: candidates, protocols, and applications. In *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part IV 41*, pages 517–547, Cham, 2021. Springer, Springer International Publishing. `doi:10.1007/978-3-030-84259-8_18`.

13 Daniel Escudero, Satrajit Ghosh, Marcel Keller, Rahul Rachuri, and Peter Scholl. Improved primitives for MPC over mixed arithmetic-binary circuits. In *Advances in Cryptology–CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020, Proceedings, Part II 40*, pages 823–852, Cham, 2020. Springer, Springer International Publishing. `doi:10.1007/978-3-030-56880-1_29`.

14 Niv Gilboa and Yuval Ishai. Compressing cryptographic resources. In *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 591–608. Springer, 1999. `doi:10.1007/3-540-48405-1_37`.

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

16 Mauricio Karchmer and Avi Wigderson. On span programs. *[1993] Proceedings of the Eigth Annual Structure in Complexity Theory Conference*, pages 102–111, 1993. doi:10.1109/SCT.1993.336536.

17 Ilan Komargodski, Moni Naor, and Eylon Yogev. How to share a secret, infinitely. *IEEE Trans. Inf. Theory*, 64(6):4179–4190, 2018. doi:10.1109/TIT.2017.2779121.

18 Ilan Komargodski and Anat Paskin-Cherniavsky. Evolving secret sharing: Dynamic thresholds and robustness. In Yael Kalai and Leonid Reyzin, editors, *Theory of Cryptography*, pages 379–393, Cham, 2017. Springer International Publishing. doi:10.1007/978-3-319-70503-3_12.

19 Eleftheria Makri, Dragos Rotaru, Frederik Vercauteren, and Sameer Wagh. Rabbit: Efficient comparison for secure multi-party computation. In *International Conference on Financial Cryptography and Data Security*, pages 249–270, Berlin, Heidelberg, 2021. Springer, Springer Berlin Heidelberg. doi:10.1007/978-3-662-64322-8_12.

20 Eleftheria Makri and Tim Wood. Full-threshold actively-secure multiparty arithmetic circuit garbling. In *Progress in Cryptology–LATINCRYPT 2021: 7th International Conference on Cryptology and Information Security in Latin America, Bogotá, Colombia, October 6–8, 2021, Proceedings 7*, pages 407–430, Cham, 2021. Springer, Springer International Publishing. doi:10.1007/978-3-030-88238-9_20.

21 Anat Paskin-Cherniavsky and Olga Nissenbaum. New bounds and a generalizati-on for share conversion for 3-server PIR. *Entropy*, 24(4), 2022. doi:10.3390/e24040497.

22 Anat Paskin-Cherniavsky and Leora Schmerler. On share conversions for private information retrieval. *Entropy*, 21(9), 2019. doi:10.3390/e21090826.

23 Naty Peter. Evolving conditional disclosure secrets. In *Information Security: 26th International Conference, ISC 2023, Groningen, The Netherlands, November 15–17, 2023, Proceedings*, pages 327–347, Berlin, Heidelberg, 2023. Springer-Verlag. doi:10.1007/978-3-031-49187-0_17.

24 Dragos Rotaru and Tim Wood. Marbled circuits: Mixing arithmetic and boolean circuits with active security. In *International Conference on Cryptology in India*, pages 227–249, Cham, 2019. Springer International Publishing. doi:10.1007/978-3-030-35423-7_12.

25 Adi Shamir. How to share a secret. In *Communications of the ACM, 22*, pages 612–613, 1979. doi:10.1145/359168.359176.