Access Structure Hiding Verifiable Tensor Designs

Anandarup Roy[1] Bimal Kumar Roy[1] Kouichi Sakurai[2]
Suprita Talnikar[3]

[1] Indian Statistical Institute, Kolkata, India

[2] Kyushu University, Kyushu, Japan

[3] Radboud University, Nijmegen, The Netherlands

Abstract

The field of verifiable secret sharing schemes was introduced by Verheul et al. and has evolved over time, including well-known examples by Feldman and Pedersen. Stinson made advancements in combinatorial design-based secret sharing schemes in 2004. Desmedt et al. introduced the concept of frameproofness in 2021, while recent research by Sehrawat et al. in 2021 focuses on LWE-based access structure hiding verifiable secret sharing with malicious-majority settings. Furthermore, Roy et al. combined the concepts of reparable threshold schemes by Stinson et al. and frameproofness by Desmedt et al. in 2023, to develop extendable tensor designs built from balanced incomplete block designs, and also presented a frameproof version of their design. This paper explores ramp-type verifiable secret sharing schemes, and the application of hidden access structures in such cryptographic protocols. Inspired by Sehrawat et al.'s access structure hiding scheme, we develop an ϵ-almost access structure hiding scheme, which is verifiable as well as frameproof. We detail how the concept ϵ-almost hiding is important for incorporating ramp schemes, thus making a fundamental generalisation of this concept.

Keywords— Combinatorial Secret Sharing, Tensor Designs, Ramp Schemes, Access Structure Hiding, Verifiability, Frameproofness

1 Introduction

A verifiable secret sharing scheme [35, 22, 14, 21, 7] is a cryptographic protocol that allows a dealer to distribute shares of a secret to a group of parties in such a way that (i) the secret remains confidential and cannot be determined by any unauthorized collection of parties, (ii) the secret can be reconstructed correctly by the authorized collection of parties when they combine their shares, (iii) there is a mechanism for parties to verify the correctness of the shares they receive and for the reconstruction process, and (iv) the scheme can withstand

malicious behavior from both the dealer and the parties, thus ensuring the security and integrity of the secret sharing process.

Repairable Threshold Schemes (RTSs) [34, 16] are cryptographic schemes that allow for the reconstruction of lost or corrupted shares in a threshold scheme without the need for the dealer who initially set up the scheme to be involved in the repair process. In RTSs, a subset of authorized parties can collaboratively reconstruct the lost share, ensuring the integrity and availability of the shared secret. [26] explores the concept of repairable ramp schemes for secret sharing and various applications, including cloud storage, sensor-based IoTs, and electronic identification cards. It proposes a protocol for extending schemes that allow for the retrieval of shares through collaborative efforts in case of loss or corruption, thereby enhancing data security and privacy. [26] also introduces the concept of tensor products of balanced incomplete block designs (BIBDs), which help securely combine individual secrets from various systems, enabling multi-level or multi-system secret sharing schemes in a robust and efficient manner. [8] introduced the concept of frameproofness of secret sharing schemes, which ensures the security and integrity of shared secrets and analyses the resistance of a scheme to attempts of falsely implicating (framing) a (set of) player(s) in the unauthorized disclosure of secret information. [26] establishes a theoretical framework for frameproofness within its extension protocol, and ensures that its extended scheme upholds the principles of frameproofness by leveraging concepts from combinatorial design theory.

[28] provides a detailed discussion on how secret sharing can be achieved with hidden access structures, allowing for a wide range of access policies to be enforced in the secret sharing process. The scheme is designed to support verifiability even when a majority of the parties are malicious, and its verification procedure does not incur any communication overhead, making it "free" in terms of computational resources. The scheme provides a maximum share size formula that allows for efficient sharing of secrets while maintaining security guarantees. The share size is optimized to balance security and efficiency considerations. It also includes mechanisms to detect and identify malicious behavior during the secret sharing process.

1.1 Our Contribution

This motivation clearly begs the question of verifiability of secret sharing schemes constructed as the extended tensor designs from [26], and how frameproofness applies to the resulting composition. Our approach results in a fundamental generalisation of the novel access structure hiding technique introduced by [28] to incorporate ramp schemes, thus allowing for a wider range of secret sharing schemes to use this technique. We provide detailed explanations for how our generalised ϵ-almost access structure hiding ramp-type tensor design satisfies all properties of an almost-verifiable secret sharing scheme, as well as almost fully hides its access structure, and has a frameproof version that does not lose any original information.

1.2 Organisation of the Paper

Beginning with the introduction of various important types of secret sharing schemes such as VSS schemes, RTSs, BIBDs and access structure hiding schemes in Section 1, we define various notations, definitions and other preliminaries in Section 2. We introduce our modified concept of ϵ-almost access structure hiding ramp-type tensor designs in section 3, where we provide a background of the existing theory of extending tensor designs by Roy et al. [26], as well as demonstrate various secret sharing properties (such as correctness, ϵ-correctness and computational secrecy for their tensor design schemes. We also recall the concept of frame-proof tensor designs through an example and show that it is also applicable to our scheme, and detail an algorithm for access structure token generation according to our requirements. In section 4, we state the mains results of this paper in the form of Theorems 3, 4, 5 and 6. Sections 5 and 6 present detailed proofs of these theorems. In Section 7, we enumerate a few applications of our results in the real world, and then conclude in Section 8.

2 Preliminaries

Given a collection $\mathbf{P} = \{P_1, \ldots, P_\ell\}$ of (say) players in a secret sharing scheme, we denote the power set of $\mathbf{P}$, i.e. the set of all subsets of $\mathbf{P}$, by $2^{\mathbf{P}}$. The closure of a subset $\mathbf{A} \in 2^{\mathbf{P}}$ is the set $cl(\mathbf{A}) \coloneqq \{\mathbf{C} : \mathbf{C}^* \subseteq \mathbf{C} \subseteq \mathbf{P} \text{ for some } \mathbf{C}^* \in \mathbf{A}\}$. Given a security parameter ω, a function $\delta(\omega)$ is called *negligible* if for all $c > 0$, there exists an ω_0 such that $(\omega) < 1/\omega_c$ for all $\omega > \omega_0$. Given a probability distribution X, the notation $\Pr[t \leftarrow X]$ denotes a sampling of t by the distribution X.

Definition 1. *Let $X = \{X_\lambda\}_{\lambda \in \mathbb{N}}$ and $Y = \{Y_\lambda\}_{\lambda \in \mathbb{N}}$ be collections of probability distributions (or* ensembles*) X_λ and Y_λ over $\{0,1\}^{\kappa(\lambda)}$ for some polynomial $\kappa(\lambda)$. These two ensembles are* polynomially or computationally indistinguishable *if for every (probabilistic) polynomial-time algorithm $\mathbf{D}$, for all $\lambda \in \mathbb{N}$, and a negligible function δ,*

$$|\Pr[t \leftarrow X_\lambda : \mathbf{D}(t) = 1] - \Pr[t \leftarrow Y_\lambda : \mathbf{D}(t) = 1]| \leq \delta(\lambda).$$

Assume that there exist positive integers θ, Θ and ℓ, where $\theta < \Theta \leq \ell$. A (θ, Θ, ℓ)-*ramp scheme* [20] involves a dealer selecting a secret and then distributing a share to each of ℓ players in a manner that fulfills the following criteria:

Reconstruction: Any subset of Θ players has the ability to collectively determine the secret using the shares they possess.

Secrecy: No subset of θ players is able to deduce any details regarding the secret.

The terms θ and Θ are referred to as the lower and upper thresholds of the scheme, respectively. For the sake of convenience, we shall refer to collections of players $\mathbf{C} \in 2^{\mathbf{P}}$ such that $\theta < |\mathbf{C}| < \Theta$ by the term *ramp collection*. In the event where $\Theta = \theta + 1$, the scheme is

recognized as a (Θ, ℓ)-threshold scheme. In the context of such a Θ-threshold scheme, the problem of *share repairability* pertains to the identification of a secure protocol for restoring the lost share of a specific player ($P_{\mathsf{i}} \in \mathbf{P}$). This process involves a certain subset of d players (excluding $P_{\mathsf{i}} \in \mathbf{P}$) engaging in message exchange amongst themselves and with $P_{\mathsf{i}} \in \mathbf{P}$, with the objective of successfully repairing its share. The smallest integer d required to accomplish this task is known as the *repairing degree* of the scheme. If an honest-but-curious coalition of no more than $\Theta - 1$ players of a (Θ, ℓ)-threshold scheme combines all the information it holds (this includes their shares, as well as all messages that they send or receive during the protocol) and still obtains no information about the secret, then we say that it is a (Θ, ℓ, d)-*repairable threshold scheme*, or a (Θ, ℓ, d)-RTS.

Definition 2. *Suppose $2 \leq k < v$. A (b, v, k, r, λ)-balanced incomplete block design or a (b, v, k, r, λ)-BIBD is a design $(X, \mathcal{B})$ such that:*

1. *$|X| = v$;*
2. *each block $B \in \mathcal{B}$ contains exactly k points;*
3. *every pair of distinct points from X is contained in exactly λ blocks.*

Observe that if each point occurs in exactly r blocks, then the parameters b, v, k, r, λ of a BIBD satisfy the following relations [33]:

(i) $bk = vr$;

(ii) $\lambda(v-1) = r(k-1)$;

(iii) $b \geq v$ *(and hence $r > k$).*

We sometimes refer to a (b, v, k, r, λ)-BIBD as simply a (v, k, λ)-BIBD.

Definition 3. *Let $\mathbf{P} = \{P_1, \ldots, P_\ell\}$ be a set of parties or players. A collection $\Gamma \subseteq 2^{\mathbf{P}}$ is monotone if $\mathbf{A} \in \Gamma$ and $\mathbf{A} \subseteq \mathbf{B}$ imply that $\mathbf{B} \in \Gamma$. An* access structure *$\Gamma \subseteq 2^{\mathbf{P}}$ is a monotone collection of non-empty subsets of $\mathbf{P}$. Sets in γ are called* authorized*, and sets not in Γ are called* unauthorized*.*

Definition 4. *For an access structure Γ, $\Gamma_0 = \{\mathbf{A} \in \Gamma : \mathbf{B} \not\subset \mathbf{A}$ for all $\mathbf{B} \in \Gamma \setminus \mathbf{A}\}$ is the family of* minimal authorized subsets *in Γ.*

Definition 5. *A* computational secret sharing scheme *with respect to an access structure Γ, security parameter ω, a set of ℓ polynomial-time parties or players $\mathbf{P} = \{P_1, \ldots, P_\ell\}$, and a set of secrets $\mathbf{K}$, consists of a pair of polynomial-time algorithms* (Share, Recon)*, where:*

- Share *is a randomized algorithm that gets a secret $k \in \mathbf{K}$ and access structure Γ as inputs, and outputs ℓ shares, $\{s_1^{(k)}, \ldots, s_\ell^{(k)}\}$, of k, and*

- Recon *is a deterministic algorithm that gets as input the shares of a subset* $\mathbf{A} \subseteq \mathbf{P}$*, denoted by* $\left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}$*, and outputs a string in* $\mathbf{K}$*,*

such that the following two requirements are satisfied:

1. (Perfect Correctness) *for all secrets* $k \in \mathbf{K}$ *and every authorized collection* $\mathbf{A} \in \Gamma$*, it holds that:* $\Pr\left[\mathsf{Recon}\left(\left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}, \mathbf{A}\right) = k\right] = 1$*,*
2. (Computational Secrecy) *for every unauthorized collection* $\mathbf{B} \notin \Gamma$ *and all distinct secrets* $k_1, k_2 \in \mathbf{K}$*, it holds that the distributions* $\left\{s_i^{(k_1)}\right\}_{i\in\mathbf{A}}$ *and* $\left\{s_i^{(k_2)}\right\}_{i\in\mathbf{A}} \in \mathbf{B}$ *are computationally indistinguishable (with respect to* ω*).*

Traditionally, secret sharing relies on honest participants. However, a *verifiable secret sharing (VSS) scheme* is also required to withstand active attacks, specifically:

- a dealer sending inconsistent or incorrect shares to some of the participants during the distribution protocol, and
- participants submitting incorrect shares during the reconstruction protocol.

VSS schemes were first introduced by [35]. Clearly, Shamir's threshold scheme is not a VSS scheme, since it does not exclude either of these attacks. Well-known examples of VSS schemes are Feldman's VSS scheme [14] and Pedersen's VSS scheme [21].

The access structure hiding verifiable (computational) secret sharing scheme of [28] defined below guarantees a relaxed definition of verifiability of shares of authorised collections of players even when a majority of the parties are malicious. Their scheme supports all monotone access structures, and its security — in particular, verifiability — relies on the hardness of the LWE problem.

Definition 6. *An* access structure hiding verifiable (computational) secret sharing scheme *with respect to an access structure* Γ*, security parameter* ω*, a set of* ℓ *polynomial-time parties or players* $\mathbf{P} = \{P_1, \ldots, P_\ell\}$*, and a set of secrets* $\mathbf{K}$*, consists of two sets of polynomial-time algorithms,* $(\mathsf{HsGen}, \mathsf{HsVer})$ *and* $(\mathsf{VerShr}, \mathsf{Recon}, \mathsf{Ver})$*, which are defined as follows:*

- VerShr *is a randomized algorithm that gets a secret* $k \in \mathbf{K}$ *and access structure* Γ *as inputs, and outputs* ℓ *shares,* $\{s_1^{(k)}, \ldots, s_\ell^{(k)}\}$*, of* k*,*
- Recon *is a deterministic algorithm that gets as input the shares of a subset* $\mathbf{A} \subseteq \mathbf{P}$*, denoted by* $\left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}$*, and outputs a string in* $\mathbf{K}$*, and*
- Ver *is a deterministic Boolean algorithm that gets* $\left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}$ *and a secret* $k' \in \mathbf{K}$ *as inputs, and outputs* $b \in \{0, 1\}$*,*

such that the following three requirements are satisfied:

1. (Perfect Correctness) *for all secrets* $k \in \mathbf{K}$ *and every authorized collection* $\mathbf{A} \in \Gamma$*, it holds that:* $\Pr\left[\mathsf{Recon}\left(\left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}, \mathbf{A}\right) = k\right] = 1$.

2. (Computational Secrecy) *for every unauthorized collection* $\mathbf{B} \notin \Gamma$ *and all distinct secrets* $k_1, k_2 \in \mathbf{K}$*, it holds that the distributions* $\left\{s_i^{(k_1)}\right\}_{i\in\mathbf{A}}$ *and* $\left\{s_i^{(k_2)}\right\}_{i\in\mathbf{A}} \in \mathbf{B}$ *are computationally indistinguishable (with respect to* ω*).*

3. (Computational Verifiability) *Every authorized collection* $\mathbf{A} \in \Gamma$ *can use* Ver *to verify whether its set of shares* $\left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}$ *is consistent with a given secret* $k \in \mathcal{K}$*. Formally, for a negligible function* δ*, it holds that:*

   - *If all shares* $s_i^{(k)} \in \left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}$ *are consistent with the secret* k*, then*

   $$\Pr\left[\mathsf{Ver}\left(k, \left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}\right) = 1\right] = 1 - \delta(\omega)$$

   - *If any share* $s_i^{(k)} \in \left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}$ *is inconsistent with the secret* k*, then*

   $$\Pr\left[\mathsf{Ver}\left(k, \left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}\right) = 0\right] = 1 - \delta(\omega).$$

- HsGen *is a randomized algorithm that gets* $\mathbf{P}$ *and* Γ *as inputs, and outputs* ℓ access structure tokens $\left\{\mho_1^{(\Gamma)}, \ldots, \mho_\ell^{(\Gamma)}\right\}$*, and*

- HsVer *is a deterministic algorithm that gets as input the access structure tokens of a subset* $\mathbf{A} \subseteq \mathbf{P}$ $\left(\text{denoted } \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{A}}\right)$*, and outputs* $b \in \{0, 1\}$*,*

such that the following three requirements are satisfied:

1. (Perfect completeness) *Every authorized collection of parties* $\mathbf{A} \in \Gamma$ *can identify itself as a member of the access structure* Γ*, i.e.* $\Pr\left[\mathsf{HsVer}\left(\left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{A}}\right) = 1\right] = 1$.

2. (Perfect soundness) *Every unauthorized collection of parties* $\mathbf{B} \notin \Gamma$ *can identify itself to be outside of the access structure* Γ*, i.e.* $\Pr\left[\mathsf{HsVer}\left(\left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}\right) = 0\right] = 1$.

3. (Statistical hiding) *For all access structures* $\Gamma, \Gamma' \subseteq 2^{\mathbf{P}}$ *where* $\Gamma \neq \Gamma'$*, and for all unauthorised collections* $\mathbf{B} \notin \Gamma, \Gamma'$*,*

$$\left|\Pr\left[\Gamma \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}, \left\{s_i^{(k)}\right\}_{i\in\mathbf{B}}\right] - \Pr\left[\Gamma' \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}, \left\{s_i^{(k)}\right\}_{i\in\mathbf{B}}\right]\right| = 2^{-\omega}.$$

3 ϵ-Almost Access Structure Hiding Ramp-Type Tensor Designs

We incorporate the novel access structure hiding technique of [28] in the tensor design obtained by extending BIBDs as introduced in the work of [26]. Since the scheme of [26] is a ramp scheme for both variants (non-frameproof and frameproof, defined below) of the tensor design, we introduce the new concept of an ϵ-almost access structure hiding ramp scheme.

Definition 7. *Consider a (θ, Θ, ℓ)-ramp scheme, so that its access structure Γ is characterised by the ramp bounds (θ, Θ). For $\epsilon = (\epsilon_{\text{Corr}}, \epsilon_1, \epsilon_2, \epsilon_3)$, an* ϵ-almost access structure hiding (θ, Θ, ℓ)-ramp scheme *with respect to a security parameter ω, a set of ℓ polynomial-time parties or players $\mathbf{P} = \{P_1, \ldots, P_\ell\}$, and a set of secrets $\mathbf{K}$, consists of two sets of polynomial-time algorithms, $(\mathsf{HsGen}, \mathsf{HsVer})$ and $(\mathsf{VerShr}, \mathsf{Recon}, \mathsf{Ver})$, which are defined as follows:*

- VerShr *is a randomized algorithm that gets a secret $k \in \mathbf{K}$ and the bounds θ, Θ as inputs, and outputs ℓ shares, $\{s_1^{(k)}, \ldots, s_\ell^{(k)}\}$, of k,*
- Recon *is a deterministic algorithm that gets as input the shares of a subset $\mathbf{A} \subseteq \mathbf{P}$, denoted by $\left\{s_i^{(k)}\right\}_{i \in \mathbf{A}}$, and outputs a string in $\mathbf{K}$, and*
- Ver *is a deterministic Boolean algorithm that gets $\left\{s_i^{(k)}\right\}_{i \in \mathbf{A}}$ and a secret $k' \in \mathbf{K}$ as inputs, and outputs $b \in \{0, 1\}$,*

such that the following four requirements are satisfied:

1. (Perfect Correctness) *for all secrets $k \in \mathbf{K}$ and every authorized collection $\mathbf{A}$ such that $|\mathbf{A}| \geq \Theta$, it holds that:* $\Pr\left[\mathsf{Recon}\left(\left\{s_i^{(k)}\right\}_{i \in \mathbf{A}}, \mathbf{A}\right) = k\right] = 1$.
2. (ϵ_{corr}-Correctness) *for all secrets $k \in \mathbf{K}$ and every ramp collection $\mathbf{C}$ such that $\theta < |\mathbf{C}| < \Theta$, there exists $\epsilon_{\text{corr}} > 0$ such that:* $\Pr\left[\mathsf{Recon}\left(\left\{s_i^{(k)}\right\}_{i \in \mathbf{A}}, \mathbf{A}\right) = k\right] = \epsilon_{\text{corr}}$.
3. (Computational Secrecy) *for every unauthorized collection $\mathbf{B}$ with $|\mathbf{B}| \leq \theta$ and all distinct secrets $k_1, k_2 \in \mathbf{K}$, it holds that the distributions $\left\{s_i^{(k_1)}\right\}_{i \in \mathbf{A}}$ and $\left\{s_i^{(k_2)}\right\}_{i \in \mathbf{A}} \in \mathbf{B}$ are computationally indistinguishable (with respect to ω).*
4. (Computational Verifiability) *Every authorized collection $\mathbf{A}$ such that $|\mathbf{A}| \geq \Theta$ can use Ver to verify whether its set of shares $\left\{s_i^{(k)}\right\}_{i \in \mathbf{A}}$ is consistent with a given secret $k \in \mathcal{K}$. Formally, for a negligible function δ, it holds that:*

   - *If all shares $s_i^{(k)} \in \left\{s_i^{(k)}\right\}_{i \in \mathbf{A}}$ are consistent with the secret k, then*

$$\Pr\left[\mathsf{Ver}\left(k, \left\{s_i^{(k)}\right\}_{i \in \mathbf{A}}\right) = 1\right] = 1 - \delta(\omega)$$

- *If any share* $s_i^{(k)} \in \left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}$ *is inconsistent with the secret* k*, then*

$$\Pr\left[\mathsf{Ver}\left(k, \left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}\right) = 0\right] = 1 - \delta(\omega).$$

- HsGen *is a randomized algorithm that gets* $\mathbf{P}$*,* θ *and* Θ *as inputs, and outputs* ℓ access structure tokens $\left\{\mho_1^{(\Gamma)}, \ldots, \mho_\ell^{(\Gamma)}\right\}$*, and*

- HsVer *is a deterministic algorithm that gets as input the access structure tokens of a subset* $\mathbf{A} \subseteq \mathbf{P}$ $\left($*denoted* $\left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{A}}\right)$*, and outputs* $b \in \{0, 1\}$*,*

such that the following six requirements are satisfied:

1. (Perfect completeness) *Every authorized collection of parties* $\mathbf{A}$ *such that* $|\mathbf{A}| \geq \Theta$ *can identify itself as a member of the access structure* Γ*, i.e.* $\Pr\left[\mathsf{HsVer}\left(\left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{A}}\right) = 1\right] = 1$.

2. (ϵ_1-Completeness) *Every ramp collection of parties* $\mathbf{C}$ *(where* $\theta < |\mathbf{C}| < \Theta$*) can almost always identify itself as a member of the access structure* Γ*),*
i.e. $\Pr\left[\mathsf{HsVer}\left(\left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{A}}\right) = 1\right] = 1 - \epsilon_1$.

3. (Perfect soundness) *Every unauthorized collection of parties* $\mathbf{B}$ *with* $|\mathbf{B}| \leq \theta$ *can identify itself to be outside of the access structure* Γ*, i.e.* $\Pr\left[\mathsf{HsVer}\left(\left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}\right) = 0\right] = 1$.

4. (ϵ_2-Soundness) *Every ramp collection of parties* $\mathbf{C}$ *(where* $\theta < |\mathbf{C}| < \Theta$*) can almost always identify itself to be outside of the access structure* Γ*, i.e.* $\Pr\left[\mathsf{HsVer}\left(\left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}\right) = 0\right] = 1 - \epsilon_2$.

5. (Statistical hiding) *For all ramp access structures* $\Gamma \neq \Gamma'$ *and for all unauthorised collections* $\mathbf{B}$ *with* $|\mathbf{B}| \leq \theta, \theta'$*,*

$$\left|\Pr\left[\Gamma \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}, \left\{s_i^{(k)}\right\}_{i\in\mathbf{B}}\right] - \Pr\left[\Gamma' \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}, \left\{s_i^{(k)}\right\}_{i\in\mathbf{B}}\right]\right| = 2^{-\omega}.$$

6. (ϵ_3-Statistical Hiding) *For all ramp access structures* $\Gamma, \Gamma' \subseteq 2^{\mathbf{P}}$ *where* $\Gamma \neq \Gamma'$*, and for all ramp collections* $\mathbf{C}$ *such that* $\theta < |\mathbf{C}| < \Theta$*,*

$$\left|\Pr\left[\Gamma \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{C}}, \left\{s_i^{(k)}\right\}_{i\in\mathbf{C}}\right] - \Pr\left[\Gamma' \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{C}}, \left\{s_i^{(k)}\right\}_{i\in\mathbf{C}}\right]\right| \leq \epsilon_3(\omega).$$

3.1 Tensor Design

Let $\mathcal{A}$ and $\mathcal{B}$ be the share matrices generated by ramp schemes with respectively b_1 and b_2 blocks having shares of sizes k_1 and k_2. Suppose $\mathcal{A}$ and $\mathcal{B}$ also denote the $b_1 \times k_1$ and $b_2 \times k_2$ matrices corresponding to the two schemes. The Krönecker product of $\mathcal{A} \otimes \mathcal{B}$ is therefore

$$M = \begin{pmatrix} \mathfrak{a}_{11}\mathcal{B} & \mathfrak{a}_{12}\mathcal{B} & \dots & \mathfrak{a}_{1k_1}\mathcal{B} \\ \mathfrak{a}_{21}\mathcal{B} & \mathfrak{a}_{22}\mathcal{B} & \dots & \mathfrak{a}_{2k_1}\mathcal{B} \\ \vdots & & & \\ \mathfrak{a}_{b_1 1}\mathcal{B} & \mathfrak{a}_{b_1 2}\mathcal{B} & \dots & \mathfrak{a}_{b_1 k_1}\mathcal{B} \end{pmatrix}. \tag{1}$$

If the share matrix $\mathcal{A}$ is defined over the field $\mathbb{F}_{p_1}$ and $\mathcal{B}$ over the field $\mathbb{F}_{p_2}$ for some primes p_1 and p_2, then we define the scalar multiplication as the simple integer multiplication:

$$\begin{aligned} \mathbb{F}_{p_1} \times \mathbb{F}_{p_2} &\to \mathbb{Z} \\ \text{such that } (x_1, x_2) &\mapsto x_1 \cdot x_2. \end{aligned}$$

The reason behind taking such a multiplication is that the product elements are not distinguishable from integers. Therefore, M is a matrix over the integer ring $\mathbb{Z}$.

Theorem 1 (Reconstruction from Tensor Designs, [26])**.** *Consider a $(v_1, k_1, \lambda_1, b_1, r_1)$-BIBD $\mathcal{A}$ and a $(v_2, k_2, \lambda_2, b_2, r_2)$-BIBD $\mathcal{B}$.*

1. *The matrix $\mathcal{A} \otimes \mathcal{B}_d$ produces a tensor design (over the integer ring $\mathbb{Z}$) for a (public) integer d such that there are no multiplicative collisions of the type $x_i(y_j+d) = x_k(y_l+d)$ for $(i,j) \neq (k,l)$.*

2. - *If $\gcd(x_1, x_2, \dots, x_{v_1}) = 1$;*
   - *if $\gcd(y_1, y_2, \dots, y_{v_2}) = 1$;*

   then $\mathcal{A}$ and $\mathcal{B}$ can be reproduced from a collection of players in the new scheme $\mathcal{A} \otimes \mathcal{B}_d$, hence enabling share repair and secret reconstruction.

For the purpose of real-world implementation, we consider a prime power q, which is computed from p_1, p_2 and d such that it is sufficiently greater than all the elements in $\mathcal{A} \otimes \mathcal{B}_d$.

3.2 Secret Sharing Properties of $\mathcal{A} \otimes \mathcal{B}_d$

Since $\mathcal{A} \otimes \mathcal{B}_d$ is a (θ, Θ, ℓ)-ramp scheme, it clearly satisfies the following properties of Definition 7:

Perfect Correctness: From Lemmas 4–9 of [26], it is clear that $\mathcal{A} \otimes \mathcal{B}_d$ is a (θ, Θ, ℓ)-ramp scheme, for $\theta = (\tau_1 - 1)(\tau_2 - 1) + 1$ and $\Theta = \min\{(\tau_1 - 1)b_2 + 1, (\tau_2 - 1)b_1 + 1\}$. Hence, any $\mathbf{A}$ with $|\mathbf{A}| \geq \Theta$ can reconstruct the secret with probability 1,
i.e. $\Pr\left[\mathsf{Recon}\left(\left\{s_i^{(k)}\right\}_{i \in \mathbf{A}}, \mathbf{A}\right) = k\right] = 1$.

ϵ_{corr}**-Correctness:** Suppose $\theta < |\mathbf{C}| < \Theta$ and $\mathbf{C}$ gets partial information about $\mathcal{A} \otimes \mathcal{B}_d$, i.e. it can reconstruct exactly one of $\mathcal{A}$ and $\mathcal{B}_d$, say $\mathcal{A}$ (respectively $\mathcal{B}_d$). Then it must guess the secret of the other factor, i.e. $\mathcal{B}_d$ (respectively $\mathcal{A}$) uniformly at random at best, ie. with probability $\frac{1}{p_2}$ (respectively $\frac{1}{p_1}$). Therefore, for all secrets $k \in \mathbf{K}$ and such a ramp collection $\mathbf{C}$, we denote $\epsilon_{\text{corr}} := \max\left\{\frac{1}{p_1}, \frac{1}{p_2}\right\}$. Therefore, $\Pr\left[\mathsf{Recon}\left(\left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}, \mathbf{A}\right) = k\right] \leq \epsilon_{\text{corr}}$.

Computational Secrecy: Consider an unauthorised collection $\mathbf{B}$, with $|\mathbf{B}| \leq \theta$ or $\theta < |\mathbf{B}| < \Theta$. Thus, $\mathbf{B}$ gets no information about the secret, which means it must guess (at best) uniformly at random, the secrets of both the factors $\mathcal{A}$ and $\mathcal{B}_d$ of $\mathcal{A} \otimes \mathcal{B}_d$. Hence, given the access structure Γ, it holds for every unauthorised collection $\mathbf{B} \notin \Gamma$ and every pair of different secrets $k_1 \neq k_2$ in $\mathcal{K}$ that the distributions $\left\{s_i^{(k_1)}\right\}_{i\in\mathbf{B}}$ and $\left\{s_i^{(k_2)}\right\}_{i\in\mathbf{B}}$ are computationally indistinguishable w.r.t. the parameter $\delta := \frac{1}{p_1 p_2}$, according to Definition 1.

3.3 Frameproofness

The concept of *framing* a player (or a collection of players), and subsequently the property of frameproofness of a secret sharing scheme was introduced by Desmedt et al. in [8]. [28] proposes an access structure hiding verifiable secret sharing scheme, where it establishes indistinguishability of authorisation of any collection of players by use of *access structure tokens*. For the collection $\mathbf{P}$ of all players in the scheme, they make the following claim regarding its frameproofness:

> "...the share of each party P_i is sealed as a PRIM-LWE instance such that the lattice basis, A_i, used to generate it is known only to P_i. Since A_i is required to generate P_i's share, it is infeasible for any coalition of polynomial-time parties $\mathbf{A} \subset \mathbf{P}$ to compute the share of $P_i \in \mathbf{P} \setminus \mathbf{A}$ without solving the LWE problem."

Furthermore, [26] shows that for the tensor design in Equation (1), only two players — one from the $r_1 - 1$ players possessing $\mathfrak{a}_{11}\mathfrak{b}_{11}$ and one from the $b_2 - 1$ players possessing $\frac{\mathfrak{a}_{12}}{\mathfrak{a}_{11}}, \frac{\mathfrak{a}_{13}}{\mathfrak{a}_{11}}, \ldots$ — can reconstruct the entire share of player P_1, and hence, frame this player. They address this problem by reducing the repetitive nature of shares of the participants — by decreasing the size of each share, while retaining all the information that a player had in the previous construction. In fact, the secret reconstruction for the modified scheme is then shown to require at $\tau_1 + \tau_2$ players. Additionally, Theorem 2 below ensures that $\mathcal{F}(\mathcal{A}, \mathcal{B})$ is simply a Θ-threshold scheme for $\Theta = \tau_1 + \tau_2$ (and not a ramp scheme like (AoB).

Example

Consider an example, where matrix $\mathcal{A}$ represents a $2-(4,3,2)$-BIBD and $\mathcal{B}$ a $2-(5,4,3)$-BIBD over the points $\{1,2,3,4\}$ and $\{1,2,3,4,5\}$, respectively (note that $r_1 = 3, r_2 = 4$), and $d = 21$. The Krönecker product tensor design obtained from these two matrices is represented by the matrix $\mathcal{A} \otimes \mathcal{B}_d$ as defined in [26]:

$$\begin{pmatrix}
22 & 23 & 24 & 25 & 44 & 46 & 48 & 50 & 66 & 69 & 72 & 75 \\
23 & 24 & 25 & 26 & 46 & 48 & 50 & 52 & 69 & 72 & 75 & 78 \\
24 & 25 & 26 & 22 & 48 & 50 & 52 & 44 & 72 & 75 & 78 & 66 \\
25 & 26 & 22 & 23 & 50 & 52 & 44 & 46 & 75 & 78 & 66 & 69 \\
26 & 22 & 23 & 24 & 52 & 44 & 46 & 48 & 78 & 66 & 69 & 72 \\
44 & 46 & 48 & 50 & 66 & 69 & 72 & 75 & 88 & 92 & 96 & 100 \\
46 & 48 & 50 & 52 & 69 & 72 & 75 & 78 & 92 & 96 & 100 & 104 \\
48 & 50 & 52 & 44 & 72 & 75 & 78 & 66 & 96 & 100 & 104 & 88 \\
50 & 52 & 44 & 46 & 75 & 78 & 66 & 69 & 100 & 104 & 88 & 92 \\
52 & 44 & 46 & 48 & 78 & 66 & 69 & 72 & 104 & 88 & 92 & 96 \\
66 & 69 & 72 & 75 & 88 & 92 & 96 & 100 & 22 & 23 & 24 & 25 \\
69 & 72 & 75 & 78 & 92 & 96 & 100 & 104 & 23 & 24 & 25 & 26 \\
72 & 75 & 78 & 66 & 96 & 100 & 104 & 88 & 24 & 25 & 26 & 22 \\
75 & 78 & 66 & 69 & 100 & 104 & 88 & 92 & 25 & 26 & 22 & 23 \\
78 & 66 & 69 & 72 & 104 & 88 & 92 & 96 & 26 & 22 & 23 & 24 \\
88 & 92 & 96 & 100 & 22 & 23 & 24 & 25 & 44 & 46 & 48 & 50 \\
92 & 96 & 100 & 104 & 23 & 24 & 25 & 26 & 46 & 48 & 50 & 52 \\
96 & 100 & 104 & 88 & 25 & 26 & 22 & 23 & 48 & 50 & 52 & 44 \\
100 & 104 & 88 & 92 & 25 & 26 & 22 & 23 & 50 & 52 & 44 & 46 \\
104 & 88 & 92 & 96 & 26 & 22 & 23 & 24 & 52 & 44 & 46 & 48
\end{pmatrix}$$

On applying certain permutations on each block of $\mathcal{A} \otimes \mathcal{B}_d$ (and removing zeroes), we obtain a scheme that extends the BIBDs $\mathcal{A}$ and $\mathcal{B}$, where it is no longer possible to reconstruct the secret from just two players. The full algorithm may be found in [26]. The shares of players

in this version, which we shall denote here by $\mathcal{F}(\mathcal{A}, \mathcal{B})$, are:

$$\begin{pmatrix}
22 & 50 & 72 \\
23 & 46 & 78 \\
25 & 48 & 72 \\
22 & 52 & 75 \\
24 & 46 & 66 \\
50 & 72 & 88 \\
46 & 78 & 92 \\
48 & 72 & 100 \\
52 & 75 & 88 \\
46 & 66 & 96 \\
72 & 88 & 25 \\
78 & 92 & 23 \\
72 & 100 & 24 \\
75 & 104 & 26 \\
66 & 92 & 23 \\
88 & 25 & 48 \\
92 & 23 & 52 \\
100 & 25 & 48 \\
88 & 26 & 50 \\
96 & 23 & 44
\end{pmatrix}$$

3.4 Secret Sharing Properties of $\mathcal{F}(\mathcal{A}, \mathcal{B})$

From Theorem 2 stated below, it is clear that $\mathcal{F}(\mathcal{A}, \mathcal{B})$ is a (θ, Θ, ℓ)-ramp scheme, for $\theta = \tau_1 + \tau_2$ and $\Theta = \min\{(\tau_1 - 1)b_2 + 1, (\tau_2 - 1)b_1 + 1\}$. Therefore, it clearly satisfies the following properties of perfect correctness for all authorised collections of players of size greater than Θ, ϵ_{corr}-correctness for ramp collections of players that are authorised, and computational secrecy for all unauthorised collections of players (irrespective of size), from Definition 7.

A complete explanation is very similar to that for $\mathcal{A} \otimes \mathcal{B}_d$ given in Section 3.4.

3.5 Graphical Representation

Definition 8. *A bipartite graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is said to* induce *a tensor design $\mathcal{B}$ if*

- *the vertex set $\mathcal{V} = \mathbf{P} \sqcup \mathbf{V}$ the disjoint union of the set of players $\mathbf{P} = \{P_1, \ldots, P_b\}$ and the set of points $\mathbf{V} = \{x_1, \ldots, x_v\}$ of $\mathcal{B}$, and*
- *the edge set is the collection $\bigcup_{\substack{i \in [b] \\ j \in [v]}} \{(P_i, x_j) : x_j \in \text{ share of } P_i\}$.*

Theorem 2. *Given a bipartite graph $\mathcal{G}$ inducing a tensor design $\mathcal{B}$, and given subsets $\delta(P_i) \subseteq N(P_i)$ of size s,*

(i) If $\bigcup_{i\in[b]} \delta(P_i) = \mathbf{V}$*, then reconstruction of the modified scheme* $\mathcal{F}(\mathcal{A},\mathcal{B})$ *is possible.*

(ii) If $s \geq 1$*, then (i) holds.*

3.6 Defining Access Structure Tokens

Consider first, the Krönecker product tensor design $\mathcal{A} \otimes \mathcal{B}_d$ as defined in Equation (1).

Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_{v_1} \in \mathbb{F}_{p_1}$ be the elements in $\mathcal{A}$ and $\mathfrak{b}_1, \ldots, \mathfrak{b}_{v_2} \in \mathbb{F}_{p_2}$ be the elements in $\mathcal{B}$. The access structure tokens for the share of each player are elements of $\in \mathbb{Z}_2^{v_1} \times \in \mathbb{Z}_2^{v_1}$, computed according to Algorithm 1.

Algorithm 1 HsGen: Access structure tokens for the tensor designs $\mathcal{A} \otimes \mathcal{B}_d$ and $\mathcal{F}(\mathcal{A},\mathcal{B})$

$\gamma \xleftarrow{\$} \mathsf{Perm}\left(\{0,1\}^{v_1} \times \{0,1\}^{v_2}\right)$.
for $1 \leq i \leq b_1 b_2$ **do**: *//player* P_i
  for $1 \leq j \leq v_1$ **do**: *//element* $\mathfrak{a}_j$
    $\hat{\mho}_i^{(1,\Gamma)} \leftarrow (\omega_1, \ldots, \omega_{v_1})$ such that $\omega_j = 1$ if and only if element $\mathfrak{a}_j$ of $\mathcal{A}$ occurs as a product $\mathfrak{a}_j\mathfrak{b}_l$ in the share of P_i.
  end for
  for $1 \leq l \leq v_2$ **do**: *//element* $\mathfrak{b}_l$
    $\hat{\mho}_i^{(2,\Gamma)} \leftarrow (\omega_1, \ldots, \omega_{v_2})$ such that $\omega_l = 1$ if and only if element $\mathfrak{b}_l$ of $\mathcal{B}$ occurs as a product $\mathfrak{a}_j\mathfrak{b}_l$ in the share of P_i.
  end for
  $\left(\mho_1^{(\Gamma)}, \ldots, \mho_{b_1 b_2}^{(\Gamma)}\right) \leftarrow \gamma\left(\hat{\mho}_1^{(1,\Gamma)} \| \hat{\mho}_1^{(2,\Gamma)}, \ldots, \hat{\mho}_{b_1}^{(1,\Gamma)} \| \hat{\mho}_{b_2}^{(2,\Gamma)}\right)$. *//permutation*
end for

Logical Condition

From Algorithm 1, it is clear that the authorisation of a collection of players $\mathbf{B}$ can be determined directly from the intermediate vectors $\hat{\mho}_i^{(1,\Gamma)}$ and $\hat{\mho}_i^{(2,\Gamma)}$ used to compute their access structure tokens. Consider the two logical statements P and Q:

$$P \;:\; \mathbf{B} \in \Gamma \tag{2}$$
$$Q \;:\; \left(\bigvee_{i\in\mathbf{B}} \hat{\mho}_i^{(1,\Gamma)} \text{ has Hamming weight } \geq \tau_1\right) \wedge \left(\bigvee_{i\in\mathbf{B}} \hat{\mho}_i^{(2,\Gamma)} \text{ has Hamming weight } \geq \tau_2\right).$$

Then from the definition of $\hat{\mho}_i^{(1,\Gamma)}$ and $\hat{\mho}_i^{(2,\Gamma)}$, it is clear that $P \leftrightarrow Q$. The proceeding lemma easily follows from this observation:

Lemma 1. *Let* Γ *denote the access structure for the tensor design* $\mathcal{A} \otimes \mathcal{B}_d$*. Then there exist parameters* θ *and* Θ *such that* Γ *is fully characterised by the following three conditions on any collection of players* $\mathbf{B} \in 2^{\mathbf{P}}$*:*

1. *If* $|\mathbf{B}| < \theta$, *then* $\mathbf{B} \notin \Gamma$.

2. *If* $\theta \leq |\mathbf{B}| < \Theta$, *then* $\mathbf{B}$ *may or may not belong to* Γ, *i.e. it may or may not be authorised.*

3. *If* $|\mathbf{B}| \geq \Theta$, *then* $\mathbf{B} \in \Gamma$.

Proof. The proof follows by checking which collections of players satisfy the condition Q. If τ_1 and τ_2 are the reconstruction numbers of $\mathcal{A}$ and $\mathcal{B}$, respectively. Then from Lemmas 4 and 7 of [26], $\theta = (\tau_1 - 1)(\tau_2 - 1) + 1$. Also, from Lemmas 5, 6, 8 and 9 of [26], $\Theta = \min\{(\tau_1 - 1)b_2 + 1, (\tau_2 - 1)b_1 + 1\}$. □

Further observe that the permutation γ in Algorithm 1 ensures that a collection of players $\mathbf{B}$ of size $t < \Theta$ cannot simply examine their tokens and conclude (with probability 1) whether or not it is authorised.

4 Main results

Theorem 3. *Given a positive integer* d *that satisfies Theorem 1, consider the tensor designs* $\mathcal{A} \otimes \mathcal{B}_d$ *with ramp structure* (θ, Θ, ℓ), *for a secret* k, *and shares* $s_i^{(k)}$ *for each player* $P_i \in \mathbf{P}$. *Then there exists an access structure token generation algorithm that makes* $\mathcal{A} \otimes \mathcal{B}_d$ *an* ϵ*-almost access structure hiding* (θ, Θ, ℓ)*-ramp tensor design.*

Theorem 4. *Given a positive integer* d *that satisfies Theorem 1, consider the tensor designs* $\mathcal{F}(\mathcal{A}, \mathcal{B})$ *with ramp structure* (θ, Θ, ℓ), *for a secret* k, *and shares* $s_i^{(k)}$ *for each player* $P_i \in \mathbf{P}$. *Then there exists an access structure token generation algorithm that makes* $\mathcal{F}(\mathcal{A}, \mathcal{B})$ *an* ϵ*-almost access structure hiding* (θ, Θ, ℓ)*-ramp tensor design.*

Theorem 5. *The access structure hiding tensor design* $\mathcal{A} \otimes \mathcal{B}_d$ *is verifiable.*

Theorem 6. *The access structure hiding tensor design* $\mathcal{F}(\mathcal{A}, \mathcal{B})$ *is verifiable.*

5 Proof of Theorems 3 and 4

Proof of Theorem 3. This is easily seen as the scheme $\mathcal{A} \otimes \mathcal{B}_d$ satisfies the six properties enumerated in Definition 7.

Completeness and ϵ_1-completeness:

Case 1: $|\mathbf{A}| \geq \Theta$. Since the access structure tokens of any collection of size at least Θ always satisfy the logical condition (2), $\mathbf{A}$ can simply check this condition and output 1. Therefore,

$$\Pr\left[\mathsf{HsVer}\left(\left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{A}}\right) = 1\right] = 1.$$

Case 2: $\theta < |\mathbf{C}| < \Theta$, and $\mathbf{C}$ is authorised. Let $|\mathbf{C}| = T$, such that $\theta < T < \Theta$ and $\mathbf{C}$ is an authorised collection of players.

$$\begin{aligned} \text{Number of permutations that fix the access structure tokens of } \mathbf{C} &= (\ell - T)! \\ \text{Total number of permutations on all } \ell \text{ access structure tokens} &= \ell! \end{aligned}$$

As there is a uniformly random distribution on the access structure tokens, $\mathbf{C}$ can make a uniformly random guess from $\{0, 1\}$ about its authorisation status. Therefore, the probability that any collection of size T can identify itself as authorised can be bounded above by the summation

$$\begin{aligned} \sum_{\substack{\mathbf{C}\in\Gamma \\ \text{with } |\mathbf{C}|=T}} \frac{(\ell - T)!}{\ell!} &\leq \frac{1}{\binom{\ell}{T}}, \\ \text{and thus, } \Pr\left[\mathsf{HsVer}\left(\left\{\mathfrak{V}_i^{(\Gamma)}\right\}_{i\in\mathbf{C}}\right) = 1\right] &\leq \sum_{\theta<T<\Theta} \frac{1}{\binom{\ell}{T}}. \end{aligned} \tag{3}$$

Denoting $\epsilon_1 \coloneqq \sum_{\theta<T<\Theta} \frac{1}{\binom{\ell}{T}}$, we then have

$$\Pr\left[\mathsf{HsVer}\left(\left\{\mathfrak{V}_i^{(\Gamma)}\right\}_{i\in\mathbf{C}}\right) = 1\right] \geq 1 - \epsilon_1.$$

Soundness and ϵ_2-soundness:

Case 1: $|\mathbf{B}| \leq \theta$. Since the access structure tokens of any collection of size at most θ never satisfy the logical condition (2), $\mathbf{B}$ can simply check this condition and output 0. Therefore,

$$\Pr\left[\mathsf{HsVer}\left(\left\{\mathfrak{V}_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}\right) = 0\right] = 1.$$

Case 2: $\theta < |\mathbf{C}| < \theta$, and $\mathbf{C}$ is unauthorised. Let $|\mathbf{C}| = T$, such that $\theta < T < \Theta$ and $\mathbf{C}$ is an unauthorised collection of players. We arrive at the upper bound $\epsilon_2 \coloneqq \sum_{\theta<T<\Theta} \frac{1}{\binom{\ell}{T}}$ as in Equation (3), by the same argument as for ϵ_1-completeness above. Hence,

$$\Pr\left[\mathsf{HsVer}\left(\left\{\mathfrak{V}_i^{(\Gamma)}\right\}_{i\in\mathbf{C}}\right) = 0\right] \geq 1 - \epsilon_2.$$

Statistical hiding and ϵ_2-statistical hiding: As $\mathcal{A} \otimes \mathcal{B}_d$ is a (θ, Θ, ℓ)-ramp scheme, any non-ramp collection pf parties can simply count the access structure tokens of all its players and determine its authorisation.

Case 1: $|\mathbf{B}| \leq \theta$. By definition of the access structure tokens, $\bigvee_{i\in\mathbf{B}} \hat{\mathfrak{V}}_i^{(1,\Gamma)} < \tau_1$ and $\bigvee_{i\in\mathbf{B}} \hat{\mathfrak{V}}_i^{(2,\Gamma)} < \tau_2$.

Thus, for any such collection and for any access structure $\Gamma' \subseteq 2^{\mathbf{P}}$ characterised by the ramp bounds (θ, Θ) such that $\mathbf{B} \notin \Gamma'$, $\Gamma' \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}$ follows the uniform distribution. Hence,

$$\Pr\left[\Gamma' \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}\right] = \frac{2}{\ell(\ell-3)} = \frac{2}{2^{b_1 b_2}(2^{b_1 b_2}-3)}.$$

And therefore, $\left|\Pr\left[\Gamma \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}, \left\{s_i^{(k)}\right\}_{i\in\mathbf{B}}\right] - \Pr\left[\Gamma' \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}, \left\{s_i^{(k)}\right\}_{i\in\mathbf{B}}\right]\right| = 0.$

If Γ' is any other type of access structure (which does not characterise a ramp scheme), then $\Pr\left[\Gamma' \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}, \left\{s_i^{(k)}\right\}_{i\in\mathbf{B}}\right] = 0.$

And therefore, $\left|\Pr\left[\Gamma \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}, \left\{s_i^{(k)}\right\}_{i\in\mathbf{B}}\right] - \Pr\left[\Gamma' \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}, \left\{s_i^{(k)}\right\}_{i\in\mathbf{B}}\right]\right|$
$= \frac{2}{2^{b_1 b_2}(2^{b_1 b_2}-3)}.$

Case 2(a): $\theta < |\mathbf{C}| < \Theta$ and $\mathbf{C}$ is unauthorised. Since $\mathbf{C}$ is an unauthorised collection of parties, it knows no information about either factor, $\mathcal{A}$, $\mathcal{B}_d$, of $\mathcal{A} \otimes \mathcal{B}_d$. Therefore, by the same arguments as for Case 1,

$$\left|\Pr\left[\Gamma \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}, \left\{s_i^{(k)}\right\}_{i\in\mathbf{B}}\right] - \Pr\left[\Gamma' \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}, \left\{s_i^{(k)}\right\}_{i\in\mathbf{B}}\right]\right| = \frac{2}{2^{b_1 b_2}(2^{b_1 b_2}-3)}.$$

Case 2(b): $\theta < |\mathbf{C}| < \Theta$ and $\mathbf{C}$ has partial information about the secret. Let us assume $\mathbf{C}$ knows the secret of the factor $\mathcal{A}$ of $\mathcal{A} \otimes \mathcal{B}_d$. Then it must guess the shares of players of $\mathcal{B}_d$ at best uniformly at random. So, a similar computation as in Case 1 allows us to arrive at the bound

$$\left|\Pr\left[\Gamma \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}, \left\{s_i^{(k)}\right\}_{i\in\mathbf{B}}\right] - \Pr\left[\Gamma' \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}, \left\{s_i^{(k)}\right\}_{i\in\mathbf{B}}\right]\right| \leq \frac{2}{2^{b_2}(2^{b_2}-3)}.$$

On the other hand, if $\mathbf{C}$ knows the secret of the factor $\mathcal{B}_d$ of $\mathcal{A} \otimes \mathcal{B}_d$, then the bound becomes

$$\left|\Pr\left[\Gamma \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}, \left\{s_i^{(k)}\right\}_{i\in\mathbf{B}}\right] - \Pr\left[\Gamma' \mid \left\{\mho_i^{(\Gamma)}\right\}_{i\in\mathbf{B}}, \left\{s_i^{(k)}\right\}_{i\in\mathbf{B}}\right]\right| \leq \frac{2}{2^{b_1}(2^{b_1}-3)}.$$

The required value for the parameter ϵ_3 is therefore the maximum of these two bounds.

□

The proof of Theorem 4 is exactly similar to the proof above.

6 Proof of Theorems 5 and 6

Proof. If $\mathbf{A}$ is an authorised collection of parties (irrespective of its size), then clearly,

$$\Pr\left[\mathsf{Ver}\left(k, \left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}\right) = 1\right] = 1$$

as $\mathbf{A}$ can reconstruct the secret perfectly.

Recall the definition of the prime power q from Section 3.1. For an unauthorised collection of parties $\mathbf{A}$ such that $\mathbf{A}$ cannot compute all elements of even one of $\mathcal{A}$ or $\mathcal{B}_d$,

$$\begin{aligned} \Pr\left[\mathsf{Ver}\left(k, \left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}\right) = 1\right] &\leq \frac{1}{q} \\ \text{and therefore, } \Pr\left[\mathsf{Ver}\left(k, \left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}\right) = 0\right] &\geq 1 - \frac{1}{q}. \end{aligned} \tag{4}$$

For a ramp collection of parties $\mathbf{A}$ such that $\theta < |\mathbf{A}| < \Theta$, i.e. $\mathbf{A}$ can compute all elements of exactly one of $\mathcal{A}$ or $\mathcal{B}_d$,

$$\begin{aligned} \Pr\left[\mathsf{Ver}\left(k, \left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}\right) = 1\right] &\leq \max\left\{\frac{1}{p_1}, \frac{1}{p_2}\right\} \\ \text{and therefore, } \Pr\left[\mathsf{Ver}\left(k, \left\{s_i^{(k)}\right\}_{i\in\mathbf{A}}\right) = 0\right] &\geq 1 - \max\left\{\frac{1}{p_1}, \frac{1}{p_2}\right\}. \end{aligned} \tag{5}$$

The bounds in Equations (4) and (5) are simply because $\mathcal{A}$ and $\mathcal{B}_d$ are τ_1- and τ_2-threshold schemes based on Shamir schemes [29], which means any collection of players that cannot reconstruct the entire secret cannot obtain any information about the secret. □

The proof of Theorem 6 is exactly similar to the proof above.

7 Applications

Our technique has real-world applications in a very wide range of domains, including secure multiparty computation [5, 2, 32], secure distributed storage [12, 25], attribute-based encryption [18, 15, 27, 3], access control mechanisms [10, 9, 13, 19], secure cloud computing [38, 6], e-voting systems [24], secure data sharing in blockchain technology [40, 1, 37], and privacy-preserving machine learning algorithms [4, 39, 23, 17], to name a few.

For example in cloud storage systems [30], our technique can enhance data integrity and availability by enabling authorized parties to reconstruct lost or corrupted shares without involving the initial dealer, avoiding framing of various parties, and computationally easy verification of shares against malicious adversary interactions.

Within sensor-based IoT systems [31], repairable ramp schemes safeguard the confidentiality and integrity of sensitive information exchanged among devices. The ability to repair lost or

corrupted shares while maintaining frameproofness, and verifiability of these shares, along with the ability to ensure their completeness and soundness without the need to actually access the shares ensures uninterrupted operation and security, critical for IoT applications.

Furthermore, repairable ramp schemes are instrumental in multi-level security systems [11, 36], such as those employed by government agencies and financial institutions. Our techniques would only improve their guarantees of security, while maintaining accessibility of critical information. They would also enable secure collaborative data sharing in environments where multiple parties require access to confidential data.

8 Conclusion and Future Work

In this paper, we discuss verifiability and frameproofness of access structure hiding ramp-type tensor designs. We do this through the introduction of a new type of secret sharing scheme, called an ϵ-almost access structure hiding (θ, Θ, ℓ)-ramp tensor design, thus making an essential generalisation of the existing novel design introduced by Sehrawat et al.. We explore ways of enhancing data security and privacy, especially Roy et al.'s concept of extending repairable threshold schemes, using tensor products of balanced incomplete block designs. This concept provides a fundamental generalization of existing designs, and thus plays an important role in enhancing the security and verifiability of secret sharing schemes by providing a mechanism for parties to verify the correctness of the shares they receive and ensuring that the reconstruction process is accurate. By incorporating ramp schemes, the construction becomes more robust against malicious behavior and unauthorized access, thus strengthening the overall security and integrity of the secret sharing process. We also list a few real-world applications where our techniques could be utilised for improved security.

While we demonstrate our concept of ϵ-almost access structure hiding for only extendable combinatorial tensor designs, it opens up a wide range of possibilities for any ramp-type scheme to incorporate this technique for further improvement of confidentiality, secrecy and verifiability.

References

[1] Suhair Alshehri, Omaimah Bamasag, Daniyal M. Alghazzawi, and Arwa Jamjoom. Dynamic secure access control and data sharing through trusted delegation and revocation in a blockchain-enabled cloud-iot environment. *IEEE Internet Things J.*, 10(5):4239–4256, 2023.

[2] Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski, and Lukasz Mazurek. Secure multiparty computations on bitcoin. *Commun. ACM*, 59(4):76–84, 2016.

[3] Sasikumar Asaithambi, Logesh Ravi, Malathi Devarajan, A. Selvalakshmi, Abdulaziz T. Almaktoom, Abdulaziz S. Almazyad, Guojiang Xiong, and Ali Wagdy Mohamed.

Blockchain-assisted hierarchical attribute-based encryption scheme for secure information sharing in industrial internet of things. *IEEE Access*, 12:12586–12601, 2024.

[4] Ferhat Özgür Çatak. Secure multi-party computation based privacy preserving extreme learning machine algorithm over vertically distributed data. In Sabri Arik, Tingwen Huang, Weng Kin Lai, and Qingshan Liu, editors, *Neural Information Processing - 22nd International Conference, ICONIP 2015, Istanbul, Turkey, November 9-12, 2015, Proceedings, Part II*, volume 9490 of *Lecture Notes in Computer Science*, pages 337–345. Springer, 2015.

[5] David Chaum. The spymasters double-agent problem: Multiparty computations secure unconditionally from minorities and cryptographically from majorities. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, volume 435 of *Lecture Notes in Computer Science*, pages 591–602. Springer, 1989.

[6] Hui Cui and Xun Yi. Secure internet of things in cloud computing via puncturable attribute-based encryption with user revocation. *IEEE Internet Things J.*, 11(2):3662–3670, 2024.

[7] Massoud Hadian Dehkordi, Seyed Taghi Farahi, and Samaneh Mashhadi. Lwe-based verifiable essential secret image sharing scheme ((t , s , k , n) $({t,s,k,n})$ - VESIS). *IET Image Process.*, 18(4):1053–1072, 2024.

[8] Yvo Desmedt, Songbao Mo, and Arkadii M. Slinko. Framing in secret sharing. *IEEE Trans. Inf. Forensics Secur.*, 16:2836–2842, 2021.

[9] Sabrina De Capitani di Vimercati. Access control policies, models, and mechanisms. In Henk C. A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security, 2nd Ed*, pages 13–14. Springer, 2011.

[10] Nancy Eland. *Language-Based Access Control Mechanisms for Shared Databases*. PhD thesis, Cornell University, USA, 1978.

[11] Chao-Qin Gao and Chuang-Bai Xiao. A security model for information systems with multi-level security. In Yuping Wang, Yiu-ming Cheung, Ping Guo, and Yingbin Wei, editors, *Seventh International Conference on Computational Intelligence and Security, CIS 2011, Sanya, Hainan, China, December 3-4, 2011*, pages 620–624. IEEE Computer Society, 2011.

[12] Juan A. Garay, Rosario Gennaro, Charanjit S. Jutla, and Tal Rabin. Secure distributed storage and retrieval. In Marios Mavronicolas and Philippas Tsigas, editors, *Distributed Algorithms, 11th International Workshop, WDAG '97, Saarbrücken, Germany, September 24-26, 1997, Proceedings*, volume 1320 of *Lecture Notes in Computer Science*, pages 275–289. Springer, 1997.

[13] Mandeep Kaur Gondara. Access control mechanisms for semantic web services-a discussion on requirements & future directions. *CoRR*, abs/1105.0141, 2011.

[14] Thomas Hofmeister, Matthias Krause, and Hans Ulrich Simon. Contrast-optimal k out of n secret sharing schemes in visual cryptography. *Theor. Comput. Sci.*, 240(2):471–485, 2000.

[15] Luan Ibraimi, Qiang Tang, Pieter H. Hartel, and Willem Jonker. Efficient and provable secure ciphertext-policy attribute-based encryption schemes. In Feng Bao, Hui Li, and Guilin Wang, editors, *Information Security Practice and Experience, 5th International Conference, ISPEC 2009, Xi'an, China, April 13-15, 2009, Proceedings*, volume 5451 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2009.

[16] Thalia M. Laing and Douglas R. Stinson. A survey and refinement of repairable threshold schemes. *J. Math. Cryptol.*, 12(1):57–81, 2018.

[17] Soumia Zohra El Mestari, Gabriele Lenzini, and Hüseyin Demirci. Preserving data privacy in machine learning systems. *Comput. Secur.*, 137:103605, 2024.

[18] Deholo Nali, Carlisle M. Adams, and Ali Miri. Using threshold attribute-based encryption for practical biometric-based access control. *Int. J. Netw. Secur.*, 1(3):173–182, 2005.

[19] Boubakr Nour, Hakima Khelifi, Rasheed Hussain, Spyridon Mastorakis, and Hassine Moungla. Access control mechanisms in named data networks: A comprehensive survey. *ACM Comput. Surv.*, 54(3):61:1–61:35, 2022.

[20] Maura B. Paterson and Douglas R. Stinson. A simple combinatorial treatment of constructions and threshold gaps of ramp schemes. *Cryptogr. Commun.*, 5(4):229–240, 2013.

[21] Torben P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In Joan Feigenbaum, editor, *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings*, volume 576 of *Lecture Notes in Computer Science*, pages 129–140. Springer, 1991.

[22] Kun Peng. Critical survey of existing publicly verifiable secret sharing schemes. *IET Inf. Secur.*, 6(4):249–257, 2012.

[23] Hong Qin, Debiao He, Qi Feng, Muhammad Khurram Khan, Min Luo, and Kim-Kwang Raymond Choo. Cryptographic primitives in privacy-preserving machine learning: A survey. *IEEE Trans. Knowl. Data Eng.*, 36(5):1919–1934, 2024.

[24] Fatih Rabia, Sara Arezki, and Taoufiq Gadi. A review of blockchain-based e-voting systems: Comparative analysis and findings. *Int. J. Interact. Mob. Technol.*, 17(23):49–67, 2023.

[25] P. Rajasekaran and M. Duraipandian. Secure cloud storage for iot based distributed healthcare environment using blockchain orchestrated and deep learning model. *J. Intell. Fuzzy Syst.*, 46(1):1069–1084, 2024.

[26] Bimal Kumar Roy and Anandarup Roy. Iot-applicable generalized frameproof combinatorial designs. *IoT*, 4(3):466–485, 2023.

[27] Ahmed Saidi, Abdelouahab Amira, and Omar Nouali. A secure multi-authority attribute based encryption approach for robust smart grids. *Concurr. Comput. Pract. Exp.*, 36(7), 2024.

[28] Vipin Singh Sehrawat, Foo Yee Yeo, and Yvo Desmedt. Extremal set theory and LWE based access structure hiding verifiable secret sharing with malicious-majority and free verification. *Theor. Comput. Sci.*, 886:106–138, 2021.

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

[30] Young-joo Shin, Dongyoung Koo, and Junbeom Hur. A survey of secure data deduplication schemes for cloud storage systems. *ACM Comput. Surv.*, 49(4):74:1–74:38, 2017.

[31] Amit Kumar Sikder, Giuseppe Petracca, Hidayet Aksu, Trent Jaeger, and A. Selcuk Uluagac. A survey on sensor-based threats to internet-of-things (iot) devices and applications. *CoRR*, abs/1802.02041, 2018.

[32] Nigel Smart, Joshua W. Baron, Sanjay Saravanan, Jordan Brandt, and Atefeh Mashatan. Multiparty computation: To secure privacy, do the math: A discussion with nigel smart, joshua w. baron, sanjay saravanan, jordan brandt, and atefeh mashatan. *ACM Queue*, 21(6):78–100, 2024.

[33] Douglas R. Stinson. *Combinatorial designs - constructions and analysis*. Springer, 2004.

[34] Douglas R. Stinson and Ruizhong Wei. Combinatorial repairability for threshold schemes. *Des. Codes Cryptogr.*, 86(1):195–210, 2018.

[35] Eric R. Verheul and Henk C. A. van Tilborg. Constructions and properties of k out of n visual secret sharing schemes. *Des. Codes Cryptogr.*, 11(2):179–196, 1997.

[36] Gerd Wagner. Multi-level security in multiagent systems. In Peter Kandzia and Matthias Klusch, editors, *Cooperative Information Agents, First International Workshop, CIA' 97, Kiel, Germany, February 26-28, 1997, Proceedings*, volume 1202 of *Lecture Notes in Computer Science*, pages 272–285. Springer, 1997.

[37] Na Wang, Junsong Fu, Shancheng Zhang, Zheng Zhang, Jiawen Qiao, Jianwei Liu, and Bharat K. Bhargava. Secure and distributed iot data storage in clouds based on secret sharing and collaborative blockchain. *IEEE/ACM Trans. Netw.*, 31(4):1550–1565, 2023.

[38] Jin-Song Xu, Ru-Cheng Huang, Wan-Ming Huang, and Geng Yang. Secure document service for cloud computing. In Martin Gilje Jaatun, Gansen Zhao, and Chunming Rong, editors, *Cloud Computing, First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009. Proceedings*, volume 5931 of *Lecture Notes in Computer Science*, pages 541–546. Springer, 2009.

[39] Kaihe Xu, Hao Yue, Linke Guo, Yuanxiong Guo, and Yuguang Fang. Privacy-preserving machine learning algorithms for big data systems. In *35th IEEE International Conference on Distributed Computing Systems, ICDCS 2015, Columbus, OH, USA, June 29 - July 2, 2015*, pages 318–327. IEEE Computer Society, 2015.

[40] Aiqing Zhang and Xiaodong Lin. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *J. Medical Syst.*, 42(8):140:1–140:18, 2018.