From Anonymity to Accountability: Advances in Traceable Secret Sharing

Anandarup ROY[1,3] Suprita TALNIKAR[1,2] Kouichi SAKURAI[1]

Abstract: We present a unified cryptographic framework for anonymity in verifiable secret sharing (VSS), combining the ε-almost anonymity paradigm by Roy et al. with the collusion-deterrent mechanism of Gong et al. (2025). Our generalisation supports ramp schemes with verifiability and frameproofness, enabling secure sharing under malicious-majority conditions. Gong et al.'s concept of *trackable access structures* (TAS)—a refinement of homogeneous access structures—achieves zero fairness hazard and maximal robustness via combinatorial tools like partial Steiner systems, constant-weight codes, and hypergraph covers. We show that ε-almost hiding designs can be instantiated over TAS to yield secret sharing schemes that are simultaneously verifiable, frameproof, and collusion-resilient. Moreover, Roy et al.'s access tokens encode TAS membership, ensuring compatibility with deterrence mechanisms. This synthesis advances the game-theoretic security paradigm by modelling rational adversaries and leveraging subgame perfect equilibrium to disincentivize privacy-targeted collusion, bridging cryptographic hardness with mechanism design.

Keywords: Access Structure Hiding, Verifiable Secret Sharing, Trackable Access Structures

1. Foundations of Secure and Private Secret Sharing

The study of collusion deterrence in cryptography spans foundational work in broadcast encryption and group signatures, evolving into a rich ecosystem of privacy-preserving and accountability-focused mechanisms. In broadcast encryption, techniques such as the Subset Difference (SD) method and traitor tracing aim to limit key sharing and identify compromised users. Later developments introduced efficient revocation (e.g., tree-based methods) and anonymous broadcasting [5], with optimal constructions and tight bounds for anonymity and authentication [6].

Group and ring signature schemes extend these ideas by balancing anonymity with traceability, incorporating properties like frameproofness and dynamic group management [9], [10]. Threshold cryptography, introduced in early frameworks [2], laid the groundwork for secure multi-party computation and key distribution. More recent advances, such as threshold fully homomorphic encryption [4], demonstrate the continued evolution of threshold-based systems under adversarial conditions. Techniques from interactive fingerprinting codes and the hardness of preventing false discovery offer conceptual tools for robust detection and accountability in data release and collusion scenarios, complementing game-theoretic deterrence strategies [7]. Additionally, anonymity has emerged as a key privacy goal across domains such as biometrics, emphasising resistance to cross-instance linkages—an intuition closely aligned with access structure hiding and the need to keep share provenance untraceable [8].

Complementary perspectives arise from fingerprinting codes and interactive protocols, which address collusion through ex post accountability and robustness [7]. The notion of unlinkability, studied in biometric privacy [8], adds a further dimension by minimising cross-instance leakage—conceptually aligned with access-structure hiding.

This report introduces a unified cryptographic framework that synthesises anonymity, verifiable secret sharing (VSS), and game-theoretic deterrence to enhance collusion resistance. Central to this framework is the use of *Trackable Access Structures (TAS)*, which reinterpret combinatorial access tokens as TAS encodings. This enables verifiability, frameproofness, and robustness—even in malicious-majority settings—while aligning cryptographic hardness with rational deterrence.

The following table provides a glossary of key terms and notations used throughout this report for clarity and precision.

2. Verifiable Secret Sharing (VSS) in Malicious-Majority Settings

Verifiable Secret Sharing (VSS) is a fundamental cryptographic primitive that allows a dealer to distribute shares of

[1] Department of Advanced Informatics, Kyushu University, Fukuoka, Japan

[2] Applied Statistics Unit, Indian Statistical Institute, Kolkata, India

[3] Dr. ROY is supported by the National Institute of Information and Communications Technology(NICT), Japan, under the NICT International Invitational Program.

This paper is work in progress and not peer-reviewed.

Table 1 Glossary of Key Terms and Notations

Term/Notation	Formal Definition	Source(s)
VSS	Verifiable Secret Sharing: A protocol for sharing a secret where parties can verify the validity of their shares.	[2]
$\mathcal{F}_{VSS}$	Ideal functionality for non-interactive VSS, parameterized by fault tolerance t and access structure $\mathcal{A}$.	-
(W, P)	A public mechanism consisting of a Winner selection rule (W) and a Payment rule (P) to deter collusion.	-
SPE	Subgame Perfect Equilibrium: A solution concept in game theory where the strategy profile is a Nash Equilibrium for every subgame.	-
t_e, t_f, φ	Metrics for collusion deterrence: effectiveness (t_e), fairness (t_f), and fairness hazard (φ).	-
Ramp Scheme	A secret sharing scheme with a lower threshold θ (for secrecy) and an upper threshold Θ (for reconstruction).	-
ε-almost Hiding	A relaxed notion of access structure hiding applicable to ramp schemes, parameterised by ε.	-
TAS	Trackable Access Structure: A k-homogeneous access structure where any ω parties belong to at most one minimal set.	-
$S_p(n, k, \omega)$	Partial Steiner System: A set system where every ω-subset is contained in at most one k-subset (block). Equivalent to an (n, k, ω)-TAS.	-
TSS	Traceable Secret Sharing: A scheme that allows for the identification of parties who leak their shares.	[14]

a secret among a set of parties while providing a mechanism for those parties to verify the correctness of their shares. This verification property is critical for ensuring the integrity of the shared secret, particularly in the presence of a malicious dealer who might distribute inconsistent shares or malicious participants who might submit incorrect shares during the reconstruction phase.

A VSS scheme is formally defined by a pair of algorithms, `Share` and `Recon`, which must satisfy properties of correctness and secrecy. However, in settings with active adversaries, VSS must also withstand attacks where a dealer sends incorrect shares or participants submit invalid shares during reconstruction. Well-known examples of VSS schemes include those by Feldman and Pedersen.

In addition to these classical constructions, the broader landscape of threshold cryptography and modern threshold cryptosystems (e.g., constructions leveraging threshold fully homomorphic encryption) provides context for VSS deployments in adversarial environments [2], [4]. The security of these schemes is often analysed within an ideal functionality framework.

The ideal functionality for a non-interactive VSS protocol, denoted $\mathcal{F}_{VSS}^{(t,\mathcal{A})}$, interacts with a dealer, an adversary (or simulator $\mathcal{S}$), and a set of n parties. It is parameterised by an access structure $\mathcal{A}$ and a corruption threshold t, which represents the number of parties the adversary $\mathcal{S}$ can maliciously corrupt. The $\mathcal{F}_{VSS}^{(t,\mathcal{A})}$ functionality operates in three phases.

Security Bound: According to Gong et al., the proposed VSS scheme achieves collusion deterrence with a security bound of $\left(1 - \frac{t}{n}\right)^2$, where t is the number of corrupted parties and n is the total number of participants.

The $\mathcal{F}_{VSS}^{(t,\mathcal{A})}$ functionality operates in three phases:

(1) **Dealing:** Upon receiving a secret s from an honest dealer, the functionality computes shares $\{s_i\}$ and a commitment `cmt`. It distributes the shares to the respective parties and stores the secret. If the dealer is corrupted, the functionality accepts shares from the simulator $\mathcal{S}$, provided they comply with the access structure $\mathcal{A}$.

(2) **Verification:** Any party can request verification of the commitment `cmt`. The functionality confirms if the shares are consistent and notifies all parties of the validity.

(3) **Reconstruction:** Upon a reconstruction request, the functionality collects shares from all parties. Once the set of parties providing valid shares constitutes an authorised set within the access structure $\mathcal{A}$, the functionality reveals the secret s to all parties.

A protocol is considered a secure non-interactive VSS if it can securely realise this ideal functionality. The challenge, however, intensifies in *malicious-majority settings*, where the number of corrupted parties t can exceed half the total number of parties ($t \geq n/2$). In such scenarios, a malicious majority can trivially reconstruct the secret at will by pooling their shares, rendering traditional cryptographic protections insufficient. This problem, termed “privacy-targeted collusion,” is commonplace in applications like multi-device cryptocurrency wallets, secure multi-party computation (MPC), and distributed key generation, where the compromise of a threshold number of servers leads to catastrophic failure. The core issue is that if a sufficient number of parties collude over unobserved channels (e.g., outsourced cloud computing), no purely cryptographic mechanism can prevent them from reconstructing the secret. This limitation motivates a fundamental shift in the security paradigm, moving from preventing collusion to disincentivising it, which requires a new set of tools based on game theory and rational behavior.

3. Our Contributions

We introduce a unified cryptographic framework that integrates ε-almost access structure hiding for ramp schemes with game-theoretic collusion-deterrence mechanisms over Trackable Access Structures (TAS). It provides a robust solution for secure secret sharing in malicious-majority settings against rational adversaries. Key contributions include:

(1) **Unified Framework:** Reinterprets access structure tokens in combinatorial VSS as TAS encodings, enabling the use of optimally fair collusion-deterrence mechanisms.

(2) **Optimal Fairness:** Achieves zero fairness hazard via the (W_1, P) mechanism, ensuring honest parties are never wrongly penalized—even under $(k-1)$-party collusion.

(3) **Multi-Layered Security:** Offers verifiability, cryptographic and game-theoretic frameproofness, collusion-resilience, and ε-almost access structure hiding.

(4) **Practical Construction for $\omega = 2$:** Provides an efficient VSS scheme for $(n, k, 2)$-TAS with linear information rate, demonstrating practical feasibility.

This work highlights the power of interdisciplinary methods, combining game theory, combinatorics, and coding theory to advance cryptographic security.

4. Open Problems

Despite its strengths, the framework opens several avenues for future research:

- **Efficient VSS for General TAS ($\omega \geq 3$):** Current constructions for higher ω are inefficient. Designing tailored VSS schemes with improved information rates remains a major challenge.
- **Robustness-Effectiveness Trade-off:** Understanding the trade-off between effectiveness (which decreases with ω) and robustness ($f^{(n,k)}(\omega)$) is essential. Characterizing and optimizing this balance is an open problem.
- **Real-World Applications:** Applying the framework to systems like multi-device wallets, secure MPC, randomness beacons, and DeFi protocols requires practical instantiation and parameter tuning.
- **Extension to Non-Homogeneous Structures:** Generalizing trackability and deterrence mechanisms to non-homogeneous access structures would broaden applicability.
- **Randomized Constructions:** Exploring randomized combinatorial constructions (e.g., partial Steiner systems [1]) may yield TAS with better parameters, though challenges in verifiability and efficiency remain.

5. Game-Theoretic Models for Collusion Deterrence

To address privacy-targeted collusion in malicious-majority settings, we shift from traditional cryptographic models to a game-theoretic framework that accounts for rational adversaries maximising their utility. Rather than proving that collusion is computationally infeasible, the goal is to make them irrational. This transformation aligns with mechanism design principles, modeling interactions as dynamic games where parties choose actions (e.g., collude, report) based on utility outcomes. The framework employs **Subgame Perfect Equilibrium (SPE)** to ensure credible strategies across all subgames, eliminating non-credible threats. Effectiveness, fairness, and fairness hazard are formalised as metrics to evaluate deterrence: a mechanism is t_e-effective if non-collusion is the SPE for up to t_e malicious parties; t_f-fair if honest parties are not penalized; and has $\varphi = 0$ fairness hazard if no innocent party is wrongly punished. Inspired by Gong et al.'s *Trackable Access Structures (TAS)*, which leverage combinatorial constructs like Steiner systems and constant-weight codes, we assume a public mechanism (W, P)—a winner selection and payment rule—that adjudicates collusion claims and distributes utilities. This model, supported by works in secure auctions and blockchain consensus, reframes security as incentive alignment: rational adversaries refrain from collusion not due to cryptographic barriers, but because it yields lower utility. The effectiveness of a collusion-deterrent mechanism is evaluated using three game-theoretic metrics:

- **Effectiveness (t_e):** A mechanism is t_e-effective if non-collusion becomes the subgame perfect equilibrium (SPE) when up to t_e parties are malicious.
- **Fairness (t_f):** A mechanism is t_f-fair if honest, non-colluding parties retain their utility even in the presence of up to t_f malicious parties. The honest strategy must remain dominant regardless of adversarial behavior.
- **Fairness Hazard (φ):** This measures the worst-case risk of mislabeling innocent parties as colluders. For a k-homogeneous access structure, the maximum threat is $k-1$ malicious parties. An ideal mechanism achieves $\varphi = 0$, ensuring no wrongful penalties.

6. The Principle of Access Structure Hiding in Ramp Schemes

A parallel research direction in secret sharing focuses on **anonymity**, where the access policy itself remains hidden from participants. Traditional schemes often leak structural information through shares or require explicit knowledge of the access structure for reconstruction. In contrast, access structure hiding ensures unauthorized sets learn nothing about the policy, while authorized sets can reconstruct the secret. This is achieved via two algorithms: `HsGen`, which generates access structure tokens $\{W_i^{(\Gamma)}\}$ for each party, and `HsVer`, which verifies authorization without revealing Γ. A key property is *statistical hiding*, ensuring that tokens from different access structures are indistinguishable to unauthorized sets.

Roy et al. extend this with **ε-almost access structure hiding**, tailored for **ramp schemes**—secret sharing schemes with a secrecy threshold θ, reconstruction threshold Θ, and partial leakage for intermediate sets. Their construction uses **tensor designs** formed from Krönecker products of Balanced Incomplete Block Designs (BIBDs), allowing partial reconstruction when only one component is satisfied. This behavior is incompatible with binary hiding, which motivates the ε-almost paradigm. It introduces a vector $\varepsilon = (\varepsilon_{\text{corr}}, \varepsilon_1, \varepsilon_2, \varepsilon_3)$ to quantify:

- $\varepsilon_{\text{corr}}$**-Correctness:** Ramp sets reconstruct with probability $\varepsilon_{\text{corr}}$.
- ε_1**-Completeness /** ε_2**-Soundness:** Ramp sets identify membership with probability $1-\varepsilon_1$ or $1-\varepsilon_2$.
- ε_3**-Statistical Hiding:** Tokens offer at most ε_3 advantage in distinguishing access structures.

Related primitives like **anonymous broadcast encryption (ANOBE)** and policy-hiding encryption highlight the broader relevance of hiding recipient sets and access policies. Works such as Libert et al. [5], Kobayashi et al. [6], Perera et al. [9], and Zhou et al. [10] underscore the importance of anonymity and optimal trade-offs in cryptographic design.

7. Mechanism Design for Collusion Deterrence

The core of the framework's defense against rational adversaries lies in its game-theoretic mechanisms [1], [21], which are public algorithms for reporting collusion and assigning rewards and penalties [22]. This section analyzes two mechanisms proposed by [20], starting with a general but limited approach and progressing to a refined, optimally fair design.

7.1 A General Mechanism for Arbitrary Homogeneous Access Structures (W_0, P)

The (W_0, P) mechanism applies to any k-homogeneous access structure and induces a race among colluders to report first:

- **Winner Selection Rule (W_0):** The first party to submit verifiable proof of non-trivial knowledge of the secret is declared the winner; others are marked as colluders.
- **Payment Rule (P):** The winner receives a reward λ_r, colluders are penalized λ_p, and honest participants may receive a service fee λ_s.

To prevent false reporting and framing, penalties apply to incorrect reports, and "non-trivial" knowledge is formally defined. To mitigate prior knowledge attacks, the dealer shares q random strings alongside the secret.

Game-theoretic analysis shows the mechanism is $(k-2)$-effective and $(k-2)$-fair. It creates strategic tension among rational colluders:

(1) **Reporting Decision:** Rational parties who know the secret must decide whether to report. Since $\lambda_p > 0$, reporting becomes the dominant strategy.

(2) **The Race:** Only the first reporter wins. Slower parties (due to latency or disadvantage) face high penalty risk and low reward probability.

(3) **Collusion Decision:** Anticipating a net loss, slower rational parties opt not to collude. This holds if $\lambda_s > V + p(\lambda_r + \lambda_s) - (1-p)\lambda_p$, where V is the secret's value and $p \leq 1/2$.

However, the mechanism fails when $k-1$ malicious parties collude with one rational actor. The rational party, facing no competition, safely reports, claims λ_r, and avoids penalties. The mechanism wrongly penalizes up to $n-k$ honest parties, resulting in a fairness hazard of $n-k$. This highlights the need for mechanisms that not only detect collusion but also identify its participants precisely.

7.2 An Optimally Fair Mechanism with Trackable Access Structures ($\mathbf{W_1}$, P)

The failure of (W_0, P) motivates a more advanced mechanism, (W_1, P), designed to operate on access structures with ω-trackability—Trackable Access Structures (TAS)—to precisely identify colluders and achieve zero fairness hazard [1].

The winner selection rule W_1 introduces three key components:

- **Rule 2 (Core Identification):** If exactly ω parties report and belong to a unique minimal set, they are declared winners. The remaining $k-\omega$ members of that set are penalized.
- **Rule 1.A (Free-Rider Penalty):** If $\geq k$ parties report, any reporter not forming a complete access group with others is a "free rider." The last such reporter is penalized.
- **Rule 1.B (Last-Reporter Penalty):** If the number of reporters is between ω and k, or no free riders exist, the last reporter is penalized.

W_1 strategically manipulates incentives: only the fastest ω members of a colluding group report, while others stay silent to avoid penalties. Rational parties in slower groups or slower members within the same group anticipate penalties and opt not to collude. This backward induction ensures deterrence and isolates a single colluding group.

Compared to (W_0, P), (W_1, P) offers precise identification and optimal fairness, eliminating the fairness hazard and significantly improving system reliability.

The mechanism (W_1, P) is $(k-1-\omega)$**-effective** and, most importantly, $(k-1)$**-fair with zero fairness hazard**. The zero fairness hazard is a direct consequence of ω-trackability. When $k-1$ malicious parties collude, they can only frame innocent parties if they can create ambiguity about which minimal set is responsible. Trackability eliminates this ambiguity. Any ω reports from the malicious parties will point to at most one minimal set. If an innocent party is to be framed, they must be part of that unique set. The mechanism W_1 is designed to correctly identify and penalize the actual colluders within that set, preventing non-colluding parties from being implicated. This comes at a cost, revealing a fundamental trade-off. The effectiveness is reduced from $k-2$ to $k-1-\omega$, meaning a larger ω (stronger trackability) makes the mechanism effec-

Table 2 Comparison of Collusion-Deterrent Mechanisms. Adapted from Gong et al.

Mechanisms	Malicious Fault Bounds		Fairness	Applicable Access	Robustness
	Effectiveness	Fairness	Hazard	Structures	
(W_0, P)	$k-2$	$k-2$	$n-k$	Any k-homogeneous	$n-k+1$ (Optimal)
(W_1, P)	$k-1-\omega$	$k-1$	**0** (Optimal)	ω-trackable (TAS)	$f^{(n,k)}(\omega)$

tive against fewer malicious parties. Furthermore, robustness (the ability to tolerate absentees during reconstruction) becomes a function $f^{(n,k)}(\omega)$ that depends on the specific TAS construction, creating a trade-off between effectiveness and robustness. Despite these trade-offs, the achievement of zero fairness hazard is a paramount security guarantee, justifying the need for the specialized Trackable Access Structures. The impossibility of achieving zero fairness hazard on untrackable structures, as proven in Gong et al., further underscores that trackability is not just a useful feature but a necessary condition for this level of security.

8. Trackable Access Structures (TAS): A Combinatorial Approach to Security

The advanced collusion-deterrence mechanism (W_1, P) relies on access structures with a key combinatorial property: **trackability**. A *Trackable Access Structure (TAS)* enables not just detection but precise identification of colluding parties. This section explores the formal definition of TAS, its connections to combinatorial and coding-theoretic constructs, and its robustness.

8.1 Formal Definition and Combinatorial Equivalences of TAS

An (n, k, ω)**-TAS** is a k-homogeneous access structure over n parties where any ω-subset is in at most one minimal authorized set. The parameter ω $(1 \leq \omega < k)$ defines the mechanism's ability to trace colluders using minimal reports. TASs connect deeply to several mathematical structures:

(1) **Partial Steiner Systems:** An (n, k, ω)-TAS corresponds to a partial Steiner system $S_p(n, k, \omega)$, where each ω-subset appears in at most one block. Full Steiner systems $S(n, k, \omega)$ yield optimal TASs with maximal size.

(2) **Uniform Subsets with Restricted Intersections:** TASs are families of k-subsets with pairwise intersections bounded by $\omega - 1$, i.e., $|A \cap B| < \omega$ for distinct minimal sets A and B.

(3) **Binary Constant-Weight Codes:** Each minimal set maps to an n-bit indicator vector of Hamming weight k. The trackability condition ensures a minimum Hamming distance $d \geq 2k - 2(\omega - 1)$ between codewords. This equivalence allows the use of coding bounds (e.g., Johnson bound) to estimate the maximum number of minimal sets: $|\mathcal{A}^*| \leq \binom{n}{\omega}/\binom{k}{\omega}$.

8.2 Constructions of Optimal and Near-Optimal TAS

While the combinatorial equivalences provide a theoretical foundation, practical use of TAS requires explicit constructions. Building optimal TAS—those with the maximum number of minimal sets—is challenging, tied to open problems in combinatorial design and coding theory, such as constructing maximal constant-weight codes or Steiner systems for arbitrary parameters. Research thus focuses on both optimal cases and efficient near-optimal constructions.

- **Optimal Constructions:** For specific parameters, optimal TASs are known. For instance, $(n, 3, 2)$-TAS (Steiner triple systems) and $(n, 4, 3)$-TAS have been characterized for most n.
- **Near-Optimal Algebraic Constructions:** Efficient constructions are crucial for practical deployment. Two notable algebraic approaches include:
  - **Reed-Solomon Codes:** When $k = O(\sqrt{n})$, TASs can be built using polynomials over finite fields. Parties are grid points, and minimal sets correspond to graphs of degree-($< \omega$) polynomials. This yields near-optimal TASs with $|\mathcal{A}^*| \geq (\frac{n}{2k})^{\omega}$ and is efficiently constructible.
  - **Algebraic Geometry (AG) Codes:** For larger k (e.g., linear in n), AG codes generalize Reed-Solomon constructions using algebraic curves over finite fields. These offer efficient TASs for broader parameters, though with slightly weaker bounds.

8.3 Robustness, Hypergraphs, and Independence Numbers

Beyond trackability, a crucial property of an access structure is its **robustness**. In VSS, where shares are verifiable, robustness refers to the tolerance of absent parties during reconstruction. Formally, it is the minimum number of absentees that can prevent protocol-initiated reconstruction. Higher robustness improves resilience against benign failures and denial-of-service attacks.

Robustness maps naturally to extremal graph theory: an access structure can be modeled as a **hypergraph**, with parties as vertices and minimal authorized sets as hyperedges. The robustness corresponds to the **minimum vertex cover** $\tau(H)$—a set intersecting all hyperedges. If these parties are absent, no authorized set can form. Due to the duality $\tau(H) + \alpha(H) = n$, maximizing robustness ($\tau(H)$) is equivalent to minimizing the independence number $\alpha(H)$.

This equivalence enables the use of deep combinatorial results. For fixed k and ω, randomized constructions using the Rödl nibble method yield (n, k, ω)-TAS with asymptotically optimal robustness, where $r(\mathcal{A})/n \to 1$ as n grows. More recently, deterministic constructions based on BCH codes and additive combinatorics offer explicit methods for building highly robust structures. The table below summarises known lower bounds for robustness across parameter regimes, highlighting both resolved and open cases. This framework exemplifies the deep interplay between cryptography, game theory, and combinatorics, where security properties akin to robustness align with core mathematical concepts.

8.4 Hiding and Deterrence

Building on Gong et al.'s game-theoretic deterrence and Roy et al.'s ε-almost access structure hiding for ramp schemes, this section presents their synthesis into a unified framework. The key innovation is reinterpreting access structure tokens as proofs of TAS membership, enabling the (W_1, P) mechanism to operate on a verifiable, frameproof VSS.

9. Access Structure Tokens as TAS Membership Proofs

Roy et al.'s original tokens, derived from tensor products of BIBDs $\mathcal{A} \otimes \mathcal{B}_d$, encode share membership via bit-vectors $U_i^{(1,\Gamma)}$ and $U_i^{(2,\Gamma)}$. While sufficient for ramp-based authorisation, these tokens lack the trackability needed for Gong et al.'s deterrence mechanism.

The unified framework defines an (n, k, ω)-TAS with minimal sets $M_1, M_2, \ldots$, adapting the VSS so each M_i corresponds to a uniquely reconstructible sub-secret. The token generation algorithm `HsGen` is modified as follows:

Token Redefinition: Each token vector's position i corresponds to a minimal set M_i. TAS Membership Encoding: A party P_j has a '1' at position i iff $P_j \in M_i$. Trackability Verification (`HsVer`): A bitwise AND of ω reporters' tokens yields a vector of Hamming weight 1 if they belong to a unique M_i. Preserving Hiding: A permutation γ is applied to obscure token positions, maintaining ε-almost hiding. This reinterpretation enables the ramp-based VSS to support ω-trackability, making it compatible with Gong et al.'s optimally fair deterrence mechanism.

9.1 Instantiating the Unified VSS Scheme

The unified scheme integrates standard VSS algorithms (`VerShr`, `Recon`, `Ver`) with access structure hiding (`HsGen`, `HsVer`) under the public (W_1, P) mechanism:

Setup: The dealer defines an (n, k, ω)-TAS Γ with minimal sets $M_1, M_2, \ldots$, balancing effectiveness and robustness. `VerShr` (Share Generation): The dealer uses a verifiable, frameproof VSS scheme to distribute shares aligned with the TAS structures. The frameproof tensor design $\mathcal{F}(\mathcal{A}, \mathcal{B})$ from Roy et al. is a suitable candidate .

9.2 Hiding and Deterrence

This framework exemplifies the deep interplay between cryptography, game theory, and combinatorics, where security properties like robustness align with core mathematical concepts. Building on Gong et al.'s game-theoretic deterrence [1] and Roy et al.'s ε-almost access structure hiding [14], this section presents their synthesis into a unified framework. The key innovation is reinterpreting access structure tokens as proofs of TAS membership, enabling the (W_1, P) mechanism [22] to operate on a verifiable, frameproof VSS [21].

10. Access Structure Tokens as TAS Membership Proofs

Roy et al.'s original tokens, derived from tensor products of BIBDs $\mathcal{A} \otimes \mathcal{B}_d$, encode share membership via bit-vectors $U_i^{(1,\Gamma)}$ and $U_i^{(2,\Gamma)}$. While sufficient for ramp-based authorization, these tokens lack the trackability needed for Gong et al.'s deterrence mechanism.

The unified framework defines an (n, k, ω)-TAS with minimal sets $\{M_1, M_2, \ldots\}$, adapting the VSS so each M_i corresponds to a uniquely reconstructible sub-secret. The token generation algorithm `HsGen` is modified as follows:

(1) **Token Redefinition:** Each token vector's position i corresponds to a minimal set M_i.
(2) **TAS Membership Encoding:** A party P_j has a '1' at position i iff $P_j \in M_i$.
(3) **Trackability Verification (`HsVer`):** A bitwise AND of ω reporters' tokens yields a vector of Hamming weight 1 if they belong to a unique M_i.
(4) **Preserving Hiding:** A permutation γ is applied to obscure token positions, maintaining ε-almost hiding.

This reinterpretation enables the ramp-based VSS to support ω-trackability, making it compatible with Gong et al.'s optimally fair deterrence mechanism.

10.1 Instantiating the Unified VSS Scheme

The unified scheme integrates standard VSS algorithms (`VerShr`, `Recon`, `Ver`) with access structure hiding (`HsGen`, `HsVer`) under the public (W_1, P) mechanism:

- **Setup:** The dealer defines an (n, k, ω)-TAS Γ with minimal sets $\{M_1, M_2, \ldots\}$, balancing effectiveness and robustness.
- **`VerShr` (Share Generation):** The dealer uses a verifiable, frameproof VSS scheme to distribute shares aligned with the TAS structure.

10.2 Security Analysis of the Unified Scheme

In summary, the unified framework successfully composes these properties to create a VSS scheme that is simultaneously verifiable, frameproof, collusion-resilient, and access-structure-hiding, providing a robust solution for securing secrets against powerful, rational adversaries in malicious-majority environments.

Collusion-Resilience, Fairness, and Frameproofness

The unified framework derives its collusion-resilience from the (W_1, P) mechanism and the use of *Trackable Access Structures (TAS)*. It achieves $(k - 1 - \omega)$-effectiveness and optimal fairness with zero fairness hazard, disincentivising rational adversaries from colluding and protecting honest

Table 3 Lower Bounds for Optimal Robustness of (n, k, ω)-TAS.

	$\omega = 1$	$\omega = 2$	$\omega = 3$	$\omega = 3k/4$	$\omega = k - 1$
$k = n$	1	1	1	1	1
$k = n/3$	?	?	?	?	?
$k = n^c, c < 1/8$	n^{1-c}	?	?	$n - k^4 n^{1/2}$	$n - k^4 n^{2/n^c}$
$k = (\log n)^d$	n/k	?	?	$n - k^4 n^{1/2}$	$n - k^4 n^{2/k}$
$k = 4$	$n/4$	$n - n^{0.973}$	$n(1 - o(1))$		
$k = 3$	$n/3$	$n - (\log n)$ LOT			
$k = 2$	$n/2$				

parties from false accusations. Frameproofness is ensured both cryptographically—via the tensor design $\mathcal{F}(\mathcal{A}, \mathcal{B})$ that prevents share forgery—and game-theoretically, as the mechanism reliably identifies true colluders, rendering framing attempts strategically futile.

Verifiability and Robustness

Verifiability is inherited from the underlying VSS scheme based on Roy et al.'s tensor design [14]. Parties can verify share consistency, and authorised groups can reconstruct the secret correctly, even under malicious-majority conditions. This guarantees robustness and correctness in adversarial environments.

10.3 Access Structure Hiding

The framework supports ε-almost access structure hiding through randomised token permutations γ, which obscure mappings to minimal sets. While unauthorised sets gain no information, ramp collections may leak a bounded amount, quantified by ε_3. This aligns with the statistical privacy guarantees of ramp schemes and supports broader anonymity goals in cryptographic systems [5], [6], [9], [10].

11. Efficient Secret Sharing on TAS

The information rate—defined as the ratio of secret size to share size—is a key efficiency metric in secret sharing. Generic VSS constructions (e.g., monotone span programs [11]) applied to TAS yield poor rates, with share sizes proportional to $|\mathcal{A}^*| = O((n/k)^\omega)$ for near-optimal (n, k, ω)-TAS.

Gong et al. propose a more efficient construction for $(n, k, 2)$-TAS, achieving an information ratio of $O(n)$—a major improvement over the generic $O(n^2)$ approach. Their method uses graph-theoretic decomposition:

(1) **Ideal Structures:** Based on Martí-Farré and Padró's characterization, ideal $(n, *, 2)$-TAS consist of complete bipartite graphs, stars, the Fano plane, etc.

(2) **Star Decomposition:** General $(n, k, 2)$-TAS can be decomposed into n star structures, each centered on a party.

(3) **Composition:** These ideal star schemes are composed into a single linear scheme with an overall information ratio of n.

This enables practical implementation for $\omega = 2$, balancing trackability and efficiency. For $\omega \geq 3$, efficient VSS constructions remain an open challenge.

12. Collusion Deterrence vs. Traceable Secret Sharing (TSS)

To appreciate the unified framework's novelty, it must be contrasted with **Traceable Secret Sharing (TSS)** [3], which addresses share leakage with a fundamentally different philosophy.

1. Core Goal:

- **Unified Framework (Deterrence):** Aims to prevent collusion proactively by making it economically irrational via game-theoretic incentives.
- **TSS (Tracing):** Focuses on post-collusion accountability, identifying culprits after a pirate reconstruction is detected.

2. Adversary Model and Mechanism:

- **Unified Framework:** Assumes rational actors interacting with a public mechanism (W, P) that assigns deterministic rewards and penalties based on reported behavior.
- **TSS:** Assumes a cryptographic adversary who builds a reconstruction box $\mathcal{R}$ from leaked shares. Authorities use a tracing key tk and a `Trace` algorithm with oracle access to $\mathcal{R}$ to identify a guilty party.

3. Role of Anonymity and Identification

- **Unified Framework (Trackability):** This framework relies on the public identification of reporters. The key property is not anonymity but **ω-trackability**, which ensures that the *set* of colluders can be uniquely identified from the reports of just ω members. The identities of the reporters are public inputs to the mechanism W_1.
- **TSS (Anonymity):** Anonymity and policy/recipient hiding are classic and adjacent concerns that help mitigate probing and framing attempts in related primitives (e.g., group/ring signatures, anonymous broadcast). These literatures provide both constructions and lower bounds for anonymity, offering additional context for access-structure hiding and the tracing-vs-deterrence contrast [5], [6], [9], [10].

13. Conclusion and Future Work

The unified framework and Traceable Secret Sharing (TSS) address distinct goals rooted in share leakage: deterrence versus attribution. The framework excels in closed, incentive-driven systems, while TSS supports post-breach forensic analysis. Future work should optimize efficiency and explore broader applications and access structures.

Acknowledgments We express our gratitude to the National Institute of Information and Communications Technology (NICT). This research was made possible through the support provided for Dr. Anandarup ROY's visit to Sakurai Lab at Kyushu University by the Foreign Researcher Invitation Program of NICT.

References

[1] Tiantian Gong, Aniket Kate, Hemanta K. Maji, and Hai H. Nguyen. Disincentivize Collusion in Verifiable Secret Sharing. IACR Cryptology ePrint Archive, Report 2025/446, 2025. https://eprint.iacr.org/2025/446

[2] Yvo Desmedt. Threshold Cryptography. In: Encyclopedia of Cryptography and Security, pp. 1288–1293. Springer, 2011. https://link.springer.com/rwe/10.1007/978-1-4419-5906-5_330

[3] Oriol Farràs and Miquel Guiot. Traceable Secret Sharing Schemes for General Access Structures. IACR Cryptology ePrint Archive, Report 2025/1120, 2025. https://eprint.iacr.org/2025/1120

[4] Dan Boneh, Rosario Gennaro, Steven Goldfeder, Aayush Jain, Sam Kim, Peter M. R. Rasmussen, and Amit Sahai. Threshold Cryptosystems From Threshold Fully Homomorphic Encryption. IACR Cryptology ePrint Archive, Report 2017/956, 2017. https://eprint.iacr.org/2017/956.pdf

[5] Benoît Libert, Kenneth G. Paterson, and Elizabeth A. Quaglia. Anonymous Broadcast Encryption: Adaptive Security and Efficient Constructions in the Standard Model. In: PKC 2012, LNCS 7293, pp. 206–224. Springer, 2012. https://iacr.org/archive/pkc2012/72930210/72930210.pdf

[6] Hirokazu Kobayashi, Yohei Watanabe, Kazuhiko Minematsu, and Junji Shikata. Tight lower bounds and optimal constructions of anonymous broadcast encryption and authentication. Designs, Codes and Cryptography, 91:2523–2562, 2023. https://link.springer.com/article/10.1007/s10623-023-01211-x

[7] Thomas Steinke and Jonathan Ullman. Interactive Fingerprinting Codes and the Hardness of Preventing False Discovery. Proceedings of COLT 2015, JMLR W&CP 40, pp. 1–41. https://proceedings.mlr.press/v40/Steinke15.pdf

[8] Debanjan Sadhya. Achieving unlinkability in fingerprint templates via k-anonymity and random projection. Sādhanā 49:224, 2024. https://link.springer.com/article/10.1007/s12046-024-02571-3

[9] M. N. S. Perera, Toru Nakamura, Masayuki Hashimoto, Hiroyuki Yokoyama, Chen-Mou Cheng, and Kouichi Sakurai. A Survey on Group Signatures and Ring Signatures: Traceability vs. Anonymity. Cryptography 6(1):3, 2022. https://www.mdpi.com/2410-387X/6/1/3

[10] Sujing Zhou and Dongdai Lin. On Anonymity of Group Signatures. In: Computational Intelligence and Security (CIS 2005), LNCS 3802, pp. 131–136. Springer, 2005. https://link.springer.com/chapter/10.1007/11596981_19

[11] Josh Benaloh and Jerry Leichter. Generalized Secret Sharing and Monotone Functions. In: Advances in Cryptology — CRYPTO '88, LNCS 403, pp. 27–35. Springer, 1990. https://www.cs.umd.edu/~gasarch/TOPICS/secretsharing/monotone.pdf

[12] Paul Feldman. A Practical Scheme for Non-interactive Verifiable Secret Sharing. In: 28th Annual Symposium on Foundations of Computer Science (FOCS 1987), pp. 427–437. IEEE, 1987. http://cgis.cs.umd.edu/~gasarch/TOPICS/secretsharing/feldmanVSS.pdf

[13] Torben P. Pedersen. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In: CRYPTO '91, LNCS 576, pp. 129–140. Springer, 1992. https://link.springer.com/content/pdf/10.1007/3-540-46766-1_9.pdf

[14] A. Roy, B. K. Roy, S. Talnikar, and K. Sakurai. Access Structure Hiding Verifiable Tensor Designs. *Journal of Statistics and Applications*, 22(3):535–554, 2024. https://www.ssca.org.in/media/31_SA22122024_Tapan_GE_Anadarup_Bimal_Roy_30092024_FINAL_Finally_cRlfzG7.pdf Let m

[15] Benny Applebaum, Amos Beimel, Oriol Farràs, Oded Nir, and Naty Peter. Secret-Sharing Schemes for General and Uniform Access Structures. In: EUROCRYPT 2019, LNCS 11478, pp. 441–471. Springer, 2019. https://link.springer.com/chapter/10.1007/978-3-030-17659-4_15

[16] Vipin Singh Sehrawat and Yvo Desmedt. Access Structure Hiding Secret Sharing from Novel Set Systems and Vector Families. In: COCOON 2020, LNCS 12273, pp. 246–261. Springer, 2020. https://link.springer.com/chapter/10.1007/978-3-030-58150-3_20

[17] 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. Theoretical Computer Science, 886:106–138, 2021. https://doi.org/10.1016/j.tcs.2021.07.022

[18] Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Towards Breaking the Exponential Barrier for General Secret Sharing. In: EUROCRYPT 2018, LNCS 10820, pp. 567–596. Springer, 2018. https://link.springer.com/chapter/10.1007/978-3-319-78381-9_21

[19] Shahrzad Gholami, Arunesh Sinha, Bryan Wilder, Nicole Sintov, Matthew Brown, and Milind Tambe. SPECTRE: A Game Theoretic Framework for Preventing Collusion in Security Games. In *Proceedings of the 15th International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, 2016. https://www.ifaamas.org/Proceedings/aamas2016/pdfs/p1498.pdf.

[20] Joshua S. Gans and Richard T. Holden. Mechanism Design Approaches to Blockchain Consensus. Technical Report 30189, National Bureau of Economic Research, 2022. https://www.nber.org/papers/w30189.

[21] Brandon Collins, Shouhuai Xu, and Philip N. Brown. Game-Theoretic Cybersecurity: the Good, the Bad and the Ugly. *arXiv preprint arXiv:2401.13815*, 2024. https://arxiv.org/pdf/2401.13815.

[22] Chaya Ganesh, Bhavana Kanukurthi, and Girisha Shankar. Secure Auctions in the Presence of Rational Adversaries. Technical Report 2022/1541, IACR Cryptology ePrint Archive, 2022. https://eprint.iacr.org/2022/1541.pdf.