Noname manuscript No.
(will be inserted by the editor)

Multiplicative and Verifiably Multiplicative Secret Sharing for Multipartite Adversary Structures

Reo Eriguchi · Noboru Kunihiro · Koji Nuida

Received: date / Accepted: date

Abstract d-Multiplicative secret sharing enables n players to locally compute additive shares of the product of d secrets from their shares. Barkol et al. (Journal of Cryptology, 2010) show that it is possible to construct a d-multiplicative scheme for any adversary structure satisfying the Q_d property, in which no d sets cover the whole set of players. In this paper, we focus on multipartite adversary structures and propose efficient multiplicative and verifiably multiplicative secret sharing schemes tailored to them. First, our multiplicative scheme is applicable to any multipartite Q_d-adversary structure. If the number of parts is constant, our scheme achieves a share size polynomial in the number n of players while the general construction by Barkol et al. results in exponentially large share size in the worst case. We also propose its variant defined over smaller fields. As a result, for a special class of bipartite adversary structures with two maximal points, it achieves a constant share size for arbitrary n while the share size of the first scheme necessarily incurs a logarithmic factor of n. Secondly, we devise a more efficient scheme for a special class of multipartite ones such that players in each part have the same weight and a set of players belongs to the adversary structure if and only if the sum of their weights is at most a threshold. Thirdly, if the adversary structure

This paper was presented in part at Information-Theoretic Cryptography 2020 [12]. This research was partially supported by the Ministry of Internal Affairs and Communications SCOPE Grant Number 182103105, JST CREST Grant Numbers JPMJCR19F6 and JPMJCR14D6, Japan, and JSPS KAKENHI Grant Numbers JP20J20797 and JP19K22838.

R. Eriguchi
The University of Tokyo, Tokyo, Japan,
National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan
E-mail: reo-eriguchi@g.ecc.u-tokyo.ac.jp

N. Kunihiro
University of Tsukuba, Ibaraki, Japan

K. Nuida
Kyushu University, Fukuoka, Japan
AIST, Tokyo, Japan

is Q_{d+1}, our first scheme is shown to be a verifiably multiplicative scheme that detects incorrect outputs with probability 1. For multipartite adversary structures with a constant number of parts, it improves the worst-case share and proof sizes of the only known general construction by Yoshida and Obana (IEEE Transactions on Information Theory, 2019). Finally, we propose a more efficient verifiably multiplicative scheme by allowing small error probability δ and focusing on a more restricted class of multipartite adversary structures. Our scheme verifies computation of polynomials and can achieve a share size independent of δ while the previous construction only works for monomials and results in a share size involving a factor of $\log \delta^{-1}$.

Keywords Secure multiparty computation · Multiplicative secret sharing · Verifiability · Multipartite adversary structure

1 Introduction

1.1 Background

Secret sharing is a cryptographic primitive introduced in [3,23] to protect a secret from leakage by dividing it into shares and distributing them among a set P of n players. The efficiency of a secret sharing scheme is measured by the (average) information ratio, which is defined as the ratio of the average size of shares to that of a secret. The secret sharing scheme is said to tolerate an adversary structure Δ, a family of subsets of P, if players in any $T \in \Delta$ learn no information on a secret.

d-Multiplicative secret sharing (d-MSS) [1] is a variant of secret sharing, which allows the players to locally compute additive shares of the product of d secrets. It is a central building block of information-theoretically secure multiparty computation (MPC) for degree-d polynomials. Since d-MSS non-interactively computes a multiplication of d (not just two) secrets, a protocol based on it achieves better round and communication complexity than the standard secret-sharing based protocol interactively evaluating an arithmetic circuit gate by gate. Specifically, based on a d-MSS scheme tolerating an adversary structure Δ, Barkol et al. [1] propose a two-round MPC protocol which is secure against an adversary corrupting a set of players $T \in \Delta$ and whose communication complexity is proportional to the information ratio. It is shown in [1] that the CNF scheme [18] is d-multiplicative if the adversary structure Δ satisfies the Q_d property, that is, no d sets in Δ cover P. Conversely, they also show that d-MSS for Δ is possible only if Δ satisfies the Q_d property. There are also d-MSS schemes applicable only to threshold adversary structures [23, 2,6,5,7].[1]

When obtaining a value of a function from shares, an output player would need to detect the existence of an incorrect value. Yoshida and Obana [25]

[1] The multiplicative property of Shamir's scheme was not mentioned in the original paper [23] but it was later implicitly used in [2,6].

introduce verifiably d-multiplicative secret sharing (d-VMSS), which allows the players to locally convert their shares into proofs showing that the output is indeed the correct value of a degree-d polynomial. They propose an error-free d-VMSS based on the CNF scheme for any Q_{d+1}-adversary structure, which detects cheating with probability 1. In the particular case of computing degree-d monomials, they also devise a transformation to make any d-MSS scheme verifiable while small error probability is required.

However, since they are based on the CNF scheme, the general constructions of MSS and error-free VMSS schemes [1,25] result in exponentially large information ratios in the worst case. Furthermore, a VMSS scheme provided by the general transformation [25] necessarily has a share size involving a factor of $\log \delta^{-1}$ for the error probability δ.

1.2 Our Results

In this paper, we focus on multipartite adversary structures Δ [14], in which P is divided into ℓ parts P_j and players in each P_j play the same role. Formally, whether each subset X is in Δ is determined by $(|X \cap P_1|, \ldots, |X \cap P_\ell|)$. We aim at more efficient MSS and VMSS schemes tailored to given multipartite adversary structures than those obtained by the general constructions [1,25]. We also further improve efficiency when Δ satisfies a stronger property than Q_d since the Q_d property just comes from the information-theoretic limit [1] rather than from actual privacy requirements.

- **d-MSS for Q_d-adversary structures.** Our first scheme can tolerate any ℓ-partite Q_d-adversary structure Δ. The information ratio is equal to the number of all points representing maximal sets in Δ, which is at most $O(n^\ell)$ (Theorem 1). It is polynomial in n when ℓ is constant. This scheme has to be defined over a finite field $\mathbb{F}_q$ with $q > n$. As shown in Table 1, our scheme improves the worst-case information ratio of the general MSS scheme [1] for multipartite adversary structures with $\ell = O(1)$. Our scheme tolerates a wider class of adversary structures than the threshold schemes [23,2,6, 5,7]. We also propose its variant in which q can be chosen independent of n if the partition is *balanced*, i.e., there is a constant $\mu > 0$ such that $\min_{j \in [\ell]} |P_j| \geq \mu n$ (Theorem 2). As a result, for a special class of 2-partite adversary structures with two maximal points, it achieves a constant share size for arbitrary n while the share size of our first scheme necessarily incurs a logarithmic factor of n. A price to pay for the efficiency gain is that the adversary structure must satisfy a stronger property than Q_d, which we term the Q_d property with margin κ.
- **d-MSS for weighted threshold adversary structures.** We propose a more efficient MSS scheme than Theorem 1 for multipartite adversary structures Δ such that players in each part have the same weight and a set of players is in Δ if and only if the sum of their weights is at most a threshold (Theorem 3). More specifically, using the geometric representation [13], ℓ-partite adversary structures can be embedded in $\mathbb{R}^\ell$ via the map

Table 1 Comparison of d-MSS schemes. Define $\mathcal{T}_k^n = \{X : |X| \leq k\}$, Δ^+ as the family of all maximal sets in Δ, and $\max \Phi^{\Pi}(\Delta)$ as the set of all points representing maximal sets in Δ (see Section 2 for formal definitions). Let κ denote a constant such that $0 < \kappa < 1$. The notations $O_\epsilon(\cdot)$ and $\Omega_\epsilon(\cdot)$ hide any constant depending on ϵ.

Scheme	Adversary structure Δ	Information ratio	Field size q
[23,2,6]	$\mathcal{T}_k^n$ with $dk < n$	1	$q > n$
[5,7]	$\mathcal{T}_k^n$ with $dk < (1-\kappa)n$	1	independent of n
[1]	Q_d	$\lvert\Delta^+\rvert$	independent of n
Theorem 1	ℓ-partite and Q_d	$\lvert\max \Phi^{\Pi}(\Delta)\rvert$	$q > n$
Theorem 2	ℓ-partite and Q_d with margin κ	$\lvert\max \Phi^{\Pi}(\Delta)\rvert$	independent of n
Theorem 3	ℓ-partite and $\mathrm{dist}(\boldsymbol{p}, \mathrm{Conv}(\Phi^{\Pi}(\Delta))) \geq \epsilon$	$O_\epsilon(\ell n)$	$q > \Omega_\epsilon(\ell n^2)$

$\Phi^{\Pi} : 2^P \to \mathbb{R}^\ell$, $\Phi^{\Pi}(X) = (|X \cap P_1|, \ldots, |X \cap P_\ell|)$. Let $C = \mathrm{Conv}(\Phi^{\Pi}(\Delta))$ be the convex hull of $\Phi^{\Pi}(\Delta)$ in $\mathbb{R}^\ell$ and set $\boldsymbol{p} = (1/d)\Phi^{\Pi}(P)$. If $\mathrm{dist}(\boldsymbol{p}, C)$, the distance between $\boldsymbol{p}$ and C, is at least $\epsilon > 0$, then the scheme achieves an information ratio $(\ell n/\epsilon) + 1$, which is smaller than Theorem 1 if ϵ is constant.

- **Error-free d-VMSS for Q_{d+1}-adversary structures.** We show that the scheme in Theorem 1 detects incorrect outputs with probability 1 if the adversary structure is Q_{d+1} (Theorem 4). For multipartite adversary structures with a constant number of parts, our VMSS scheme improves the worst-case share and proof sizes of the general construction [25] (see Table 2).
- **More efficient d-VMSS for Q_{d+1}-adversary structures with margin κ.** We also propose a d-VMSS scheme with smaller proof size than Theorem 4 while it requires small error probability and the adversary structure to satisfy the Q_{d+1} property with margin κ for some κ (Theorem 5). It is possible to combine the general transformation [25] with Theorem 1 and to obtain a d-VMSS scheme for any multipartite Q_d-adversary structure with non-zero error probability. A significant advantage is that our scheme in Theorem 5 can verify computation of *polynomials* while the resulting scheme of [25] can only work for *monomials*. Even in the particular case of computing monomials, our scheme still has an advantage that the share size can be independent of error probability δ for a special class of 2-partite adversary structures with two maximal points while the share size of [25] necessarily involves a factor of $\log \delta^{-1}$ (Corollary 1).
- **Application to MPC.** The MPC protocols based on MSS and VMSS schemes [1,25] have communication complexity proportional to the share sizes. Thus, if we focus on multipartite adversary structures with a constant number of parts, our MSS schemes lead to MPC protocols with polynomial communication complexity while the previous schemes require exponential communication cost in the worst case.

Table 2 Comparison of error-free d-VMSS schemes. Share and proof sizes are measured by the number of field elements.

Scheme	Adversary structure Δ	Share size	Proof size	Field size q
[25]	Q_{d+1}	$\lvert\Delta^+\rvert$	$\lvert\Delta^+\rvert$	independent of n
Theorem 4	ℓ-partite and Q_{d+1}	$\lvert\max\Phi^{\Pi}(\Delta)\rvert$	$\lvert\max\Phi^{\Pi}(\Delta)\rvert$	$q > n$

1.3 Related Work

In the threshold setting, Shamir's scheme [23,2,6] is d-multiplicative if its threshold k satisfies $dk < n$. The arithmetic codex based on certain algebraic geometric codes [5,7] provides a d-MSS scheme defined over smaller fields than Shamir's scheme while the range of its tolerable threshold must degrade. However, they are inapplicable to a multipartite adversary structure if it contains at least one set of size exceeding their tolerable thresholds.

In [9], it is shown that a 2-MSS scheme can be generically constructed from a linear secret sharing scheme for any Q_2-adversary structure with only constant overhead. However, it is currently unknown whether their method can be extended to a construction of d-MSS for $d > 2$. In [20,21], more efficient 2-MSS schemes are proposed for specific classes of Q_2-adversary structures.

It is classically known that information-theoretically secure MPC is possible if and only if the family of all possible corruption subsets satisfies the Q_2 property [16]. However, the existing protocols in that setting (e.g., [9,11, 17,20–22]) interactively evaluate an arithmetic circuit gate by gate and hence result in communication complexity $O(n^d)$ for a degree-d polynomial. On the other hand, MPC protocols based on d-MSS schemes require interaction only in the sharing and reconstruction phase. Hence, they require only two rounds of interaction and communication cost proportional to the share size, which is smaller than $O(n^d)$ depending on adversary structures.

1.4 Publication Note

The preliminary version appeared in the proceedings of Information-Theoretic Cryptography 2020 [12]. The current version provides a construction of multiplicative secret sharing schemes over smaller fields. In addition, this paper proves that the scheme proposed in [12] can be extended into verifiably multiplicative schemes in two ways.

2 Preliminaries

Notations Let $\mathbb{Z}_+$ and $\mathbb{R}_+$ denote the set of all non-negative integers and all non-negative real numbers, respectively. Define $[\ell] = \{1, \ldots, \ell\}$ for $\ell \in \mathbb{N}$. The power set of a set X is denoted by 2^X and X^m is the Cartesian product of m copies of X. We write $x \leftarrow\!\!\$\, X$ if x is chosen at random from X. Let $\mathbb{F}_q$ denote the finite field of size q for a prime power q. Let $h \in \mathbb{F}_q[X_1, \ldots, X_n]$ be an

n-variate polynomial over $\mathbb{F}_q$. We say that h is degree-d if its total degree is at most d. The vector $\mathbf{1} \in \mathbb{R}^m$ is the one whose entries are all one and $\boldsymbol{e}_i \in \mathbb{R}^m$ is the i-th unit vector, i.e., the vector such that the i-th entry is one and the other entries are all zero. The i-th component of $\boldsymbol{v}$ is denoted by $\boldsymbol{v}(i)$. For two real vectors $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{R}^m$, we write $\boldsymbol{v} \leq \boldsymbol{w}$ if $\boldsymbol{v}(i) \leq \boldsymbol{w}(i)$ for every $i \in [m]$ and $\boldsymbol{v} < \boldsymbol{w}$ if $\boldsymbol{v} \leq \boldsymbol{w}$ and $\boldsymbol{v} \neq \boldsymbol{w}$. The standard inner product of $\boldsymbol{v}$ and $\boldsymbol{w}$ is $\boldsymbol{v} \cdot \boldsymbol{w} = \boldsymbol{v}(1)\boldsymbol{w}(1) + \cdots + \boldsymbol{v}(m)\boldsymbol{w}(m)$. The length of $\boldsymbol{v} \in \mathbb{R}^m$ is measured by the Euclidean norm $\|\boldsymbol{v}\| := \sqrt{\boldsymbol{v} \cdot \boldsymbol{v}}$ and the distance between $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{R}^m$ is given by $\mathrm{dist}(\boldsymbol{v}, \boldsymbol{w}) := \|\boldsymbol{v} - \boldsymbol{w}\|$. For a closed subset C in $\mathbb{R}^m$, we abuse notation and define the distance between $\boldsymbol{v}$ and C by $\mathrm{dist}(\boldsymbol{v}, C) = \inf\{\mathrm{dist}(\boldsymbol{v}, \boldsymbol{w}) : \boldsymbol{w} \in C\}$.

2.1 Adversary Structures

We define an adversary structure Δ on a set P of n players as a monotonically decreasing family of subsets of P, by which we mean that $A \in \Delta$ and $A \supseteq B$ imply $B \in \Delta$ for any $A, B \subseteq P$. The set of all the maximal subsets in Δ is denoted by Δ^+. We say that Δ satisfies the Q_d property if $A_1 \cup \cdots \cup A_d \neq P$ for any $A_1, \ldots, A_d \in \Delta$.

The (k, n)-threshold adversary structure $\mathcal{T}_k^n$ is defined as $\mathcal{T}_k^n = \{A \subseteq P : |A| \leq k\}$. It can be seen that $\mathcal{T}_k^n$ is Q_d if and only if $n > dk$.

Let $\Pi = (P_1, \ldots, P_\ell)$ be a partition of P, i.e., $P_i \cap P_j = \emptyset$ for $i \neq j$ and $P = \bigcup_{j \in [\ell]} P_j$. A permutation τ on P is called a Π-permutation if $\tau(P_j) = P_j$ for every $j \in [\ell]$. An adversary structure Δ is called Π-partite if $\tau(B) \in \Delta$ for any $B \in \Delta$ and any Π-permutation τ. Let $\Phi^\Pi : 2^P \to \mathbb{R}^\ell$ be a map defined by $\Phi^\Pi(X) = (|X \cap P_j|)_{j \in [\ell]}$. A Π-partite adversary structure Δ is uniquely determined by $\Phi^\Pi(\Delta)$. Since $\boldsymbol{a} \in \Phi^\Pi(\Delta)$ and $\boldsymbol{a} \geq \boldsymbol{b}$ imply $\boldsymbol{b} \in \Phi^\Pi(\Delta)$ for any $\boldsymbol{a}, \boldsymbol{b} \in \Phi^\Pi(2^P)$, a Π-partite adversary structure Δ is uniquely determined only by specifying the set of all maximal points $\max \Phi^\Pi(\Delta) := \{\boldsymbol{a} \in \Phi^\Pi(\Delta) : \boldsymbol{a} < \boldsymbol{b} \leq \Phi^\Pi(P) \Rightarrow \boldsymbol{b} \notin \Phi^\Pi(\Delta)\}$. Note that $|\max \Phi^\Pi(\Delta)| = O(n^\ell)$.

The class of weighted threshold adversary structures [23] is a natural generalization of the threshold one. Let $\Pi = (P_1, \ldots, P_\ell)$ be a partition, $\boldsymbol{w} \in \mathbb{Z}_+^\ell$, and $t \in \mathbb{Z}_+$. Define $\mathcal{W}_{\boldsymbol{w},t}^\Pi$ as the Π-partite adversary structure such that $\Phi^\Pi(\mathcal{W}_{\boldsymbol{w},t}^\Pi) = \{\boldsymbol{x} \in \Phi^\Pi(2^P) : \boldsymbol{w} \cdot \boldsymbol{x} \leq t\}$.

We fix the following notations throughout the paper unless otherwise indicated:

- $P = [n]$ denotes the set of n players.
- $\Pi = (P_1, \ldots, P_\ell)$ is a partition of P.
- Δ is a Π-partite adversary structure on P.
- N is the number $|\max \Phi^\Pi(\Delta)|$ of maximal points in Δ.
- $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N\}$ is the set $\max \Phi^\Pi(\Delta)$ of all maximal points in Δ.

2.2 Secret Sharing

We follow formalization given by [1], which is non-standard but almost equivalent to the standard ones. A secret sharing scheme is a tuple $\Sigma = (\mathcal{K}, \mathcal{R}, \mathcal{S}, \mathsf{SHARE})$, where $\mathcal{K}$ is a domain of secrets, $\mathcal{R}$ is a set of strings, $\mathcal{S}$ is a domain of shares, and $\mathsf{SHARE} : \mathcal{K} \times \mathcal{R} \to \mathcal{S}^n$ is a map. For $A \subseteq P$, $\mathsf{SHARE}(s,r)_A$ denotes the restriction of $\mathsf{SHARE}(s,r)$ to the entries indexed by A. The (average) information ratio $\rho(\Sigma)$ is defined as $\rho(\Sigma) = (1/n)\sum_{i\in P} \log|\mathcal{S}_i|/\log|\mathcal{K}|$, where $\mathcal{S}_i = \{\mathsf{SHARE}(s,r)_{\{i\}} : s \in \mathcal{K}, r \in \mathcal{R}\}$. We say that Σ is Δ-private for an adversary structure Δ if the distributions of $\mathsf{SHARE}(s,r)_A$ and $\mathsf{SHARE}(t,r)_A$ induced by $r \leftarrow_{\$} \mathcal{R}$ are perfectly identical for any $A \in \Delta$ and any $s,t \in \mathcal{K}$. A set $A \subseteq P$ is called authorized if there is a reconstruction algorithm that determines the secret s from shares $\mathsf{SHARE}(s,r)_A$ for any $r \in \mathcal{R}$. In contrast to traditional secret sharing, we do not require that any set $A \notin \Delta$ should be authorized. Instead, we say that Σ is correct if P is authorized.

We say that Σ is a d-multiplicative secret sharing scheme (d-MSS) if there exists a map $\mathsf{MULT} : P \times \mathcal{S}^d \to \mathbb{F}_q$ such that

$$\prod_{j\in[d]} s^{(j)} = \sum_{i\in P} \mathsf{MULT}(i, \gamma_i^{(1)}, \ldots, \gamma_i^{(d)}),$$

for any $s^{(1)}, \ldots, s^{(d)} \in \mathbb{F}_q$ and any $r^{(1)}, \ldots, r^{(d)} \in \mathcal{R}$, where $(\gamma_i^{(j)})_{i\in P} = \mathsf{SHARE}(s^{(j)}, r^{(j)})$ is a tuple of shares for $s^{(j)}$. We remark that the existence of MULT does not imply that given shares of two secrets $s_1, s_2 \in \mathbb{F}_q$, the players can non-interactively compute valid shares of the secret $s_1 + s_2$. It only enables players to generate additive shares of the product of secrets. To compute shares of the sum, Σ needs to satisfy the following linearity requirement. We say that Σ is $\mathbb{F}_q$-linear if $\mathcal{K}$, $\mathcal{S}$, and $\mathcal{R}$ are linear spaces and SHARE is a linear map over $\mathbb{F}_q$ such that $\mathsf{SHARE}(\cdot)_{\{i\}}$ is surjective for all $i \in [n]$. We assume that $\mathcal{K} = \mathbb{F}_q$ if we refer to $\mathbb{F}_q$-linear schemes except in Section 6.

Application to MPC Assume that there are n input players each holding their private inputs $x^{(i)}$, an output player, and an adversary who can corrupt the output player and a subset of input players in an adversary structure Δ. Let Σ be a Δ-private d-MSS scheme. Let $h \in \mathbb{F}_q[X_1, \ldots, X_n]$ be a homogeneous n-variate degree-d polynomial $h = \sum_{\boldsymbol{u}=(u_1,\ldots,u_d)\in[n]^d} c_{\boldsymbol{u}} X_{u_1} \cdots X_{u_d}$, where $c_{\boldsymbol{u}} \in \mathbb{F}_q$. Barkol et al. [1] construct a two-round MPC protocol to compute $h(x^{(1)}, \ldots, x^{(n)})$ based on Σ such that the adversary corrupting a subset $T \in \Delta$ obtains no information on $(x^{(i)})_{i\notin T}$ beyond what follows from $(x^{(i)})_{i\in T}$ and $h(x^{(1)}, \ldots, x^{(n)})$. The point-to-point communication complexity is linear in the share size and hence the total one is $O(n^2\rho(\Sigma)\log q)$. We may assume that h is homogeneous since we can pad any monomial of degree $d' < d$ with $d - d'$ copies of a dummy variable X_0. We set the corresponding input to $x^{(0)} = 1$ and the shares of $x^{(0)}$ to some predetermined ones.

$$\mathrm{Exp}(x^{(1)}, \ldots, x^{(n)}, h, T, \mathsf{Adv})$$

1. For each $j \in [n]$, sample $r^{(j)} \leftarrow\!\!\$\, \mathcal{R}$ and set $(\gamma_i^{(j)})_{i \in P} = \mathsf{SHARE}(x^{(j)}, r^{(j)})$.
2. For $i \in T$, let (ζ_i', σ_i') be a modified share and proof outputted by $\mathsf{Adv}((\gamma_i^{(j)})_{i \in T, j \in P})$.
3. For $i \notin T$, let

$$\zeta_i' = \sum_{\boldsymbol{u}} c_{\boldsymbol{u}} \mathsf{MULT}(i, \gamma_i^{(u_1)}, \ldots, \gamma_i^{(u_d)}) \text{ and } \sigma_i' = \mathsf{PROOF}(i, h, \gamma_i^{(1)}, \ldots, \gamma_i^{(n)}).$$

4. Compute $\zeta' = \sum_{i \in P} \zeta_i'$ and $\sigma' = \mathsf{Dec}(\sigma_1', \ldots, \sigma_n')$.
5. If $\zeta' \neq h(x^{(1)}, \ldots, x^{(n)})$ and $\mathsf{VER}(\zeta', \sigma') = 1$, then output 1 and else 0.

Fig. 1 The verifiability experiment for VMSS.

2.3 Verifiably Multiplicative Secret Sharing

Verifiably multiplicative schemes [25] enable the output player to verify that he indeed receives $h(x^{(1)}, \ldots, x^{(n)})$ even if a subset of input players in the adversary structure Δ submits incorrect elements.

Let $\mathsf{Dec} : (\mathbb{F}_q^c)^n \to \mathbb{F}_q^{c'}$ be a map called a decoder. We call Dec linear if Dec is an $\mathbb{F}_q$-linear map. We also call Dec additive if $c = c'$ and $\mathsf{Dec}(a_1, \ldots, a_n) = \sum_{i \in [n]} a_i$ for $a_i \in \mathbb{F}_q^c$. Let Σ be a d-MSS scheme and $\delta \geq 0$. We say that Σ is a (δ, d)-verifiably multiplicative scheme ((δ, d)-VMSS) with a decoder $\mathsf{Dec} : (\mathbb{F}_q^c)^n \to \mathbb{F}_q^{c'}$ if there are two algorithms PROOF and VER, where:

- PROOF takes as input an index $i \in P$, (a description of) a degree-d polynomial h, and n shares $\gamma_i^{(1)}, \ldots, \gamma_i^{(n)}$ for $i \in P$, and outputs $\sigma_i \in \mathbb{F}_q^c$;
- VER takes as input $m \in \mathbb{F}_q$ and $\sigma \in \mathbb{F}_q^{c'}$, and outputs $b \in \{0, 1\}$;

satisfying the following property:

- Correctness: For any $x^{(j)} \in \mathbb{F}_q$ ($j \in P$), any degree-d polynomial h, and any $r^{(j)} \in \mathcal{R}$ ($j \in P$), let $(\gamma_i^{(j)})_{i \in P} = \mathsf{SHARE}(x^{(j)}, r^{(j)})$ and $\sigma_i = \mathsf{PROOF}(i, h, \gamma_i^{(1)}, \ldots, \gamma_i^{(n)})$. Then, it holds that

$$\mathsf{VER}\left(h(x^{(1)}, \ldots, x^{(n)}), \mathsf{Dec}(\sigma_1, \ldots, \sigma_n)\right) = 1;$$

- Verifiability: For any $x^{(j)} \in \mathbb{F}_q$ ($j \in P$), any degree-d polynomial $h = \sum_{\boldsymbol{u}} c_{\boldsymbol{u}} X_{u_1} \cdots X_{u_d}$, any $T \in \Delta$, and an adversary Adv who modifies shares and proofs of corrupted players, consider an experiment described in Fig. 1. Then, it holds that

$$\Pr\left[\mathrm{Exp}(x^{(1)}, \ldots, x^{(n)}, h, T, \mathsf{Adv}) = 1\right] \leq \delta.$$

We call an output $\sigma_i \in \mathbb{F}_q^c$ of PROOF a proof. We call Σ error-free if it is $(0, d)$-verifiably multiplicative with respect to some decoder. The above definition generalizes the original one [25], which assumes that h is a degree-d *monomial*.

Based on a (δ, d)-VMSS scheme with the additive decoder, it is possible to construct a protocol in which the output player outputs $h(x^{(1)}, \ldots, x^{(n)})$ or $\perp$ with probability at least $1 - \delta$ even if some corrupted players send incorrect messages [25]. The total communication complexity is given by $O(n^2(\rho(\Sigma) + c) \log q)$. If the decoder is linear, we need a more complicated re-randomizing technique than [25] to ensure that proofs do not reveal private information. We will provide a modified protocol for our specific linear decoder in Section 5.

2.4 Examples of MSS Schemes

The (k, n)-Shamir scheme [23] is $\mathcal{T}_k^n$-private, $\mathbb{F}_q$-linear for $q > n$, and d-multiplicative if $n > dk$ [2,6]. We briefly explain another threshold d-MSS scheme based on algebraic function fields [7,5]. Please refer to [24] for terminology and theory on algebraic geometry. Let F be an algebraic function field with full field of constants $\mathbb{F}_q$. Let $g = g(F)$ denote the genus of F and $\mathbb{P}_q^{(1)}(F)$ be the set of all places of degree 1. Let $\mathrm{Div}(F)$ denote the additive group of divisors on F. For $D \in \mathrm{Div}(F)$, its Riemann-Roch space is $\mathcal{L}(D)$. We denote the support of $D \in \mathrm{Div}(F)$ by $\mathrm{supp}(D)$. Assume $n < |\mathbb{P}_q^{(1)}(F)| - 1$, let $Q, R_0, R_1, \ldots, R_n \in \mathbb{P}_q^{(1)}(F)$ be $n + 2$ distinct places of degree 1, and set $D = (k + 2g)Q \in \mathrm{Div}(F)$. For a secret $s \in \mathbb{F}_q$, choose a random $f \in \mathcal{L}(D)$ conditioned on $f(R_0) = s$. Then, the i-th share is $f(R_i)$ for $i \in P$. We call this scheme the (k, n)-Algebraic Geometric (AG) secret sharing scheme based on F. If $d(k + 2g) < n$, it is d-multiplicative.

By assigning multiple shares of Shamir's scheme, we obtain a $\mathcal{W}_{\boldsymbol{w},t}^{\Pi}$-private secret sharing scheme, which is d-multiplicative due to the multiplicative property of Shamir's scheme [2,6].

Proposition 1 ([23, 2, 6]) *Let $\boldsymbol{w} \in \mathbb{Z}_+^\ell$, $t \in \mathbb{Z}_+$ and $\mathbb{F}_q$ be a finite field such that $q > \boldsymbol{w} \cdot \Phi^{\Pi}(P)$. If $\boldsymbol{w} \cdot \Phi^{\Pi}(P) > dt$, then there exists a $\mathcal{W}_{\boldsymbol{w},t}^{\Pi}$-private d-multiplicative $\mathbb{F}_q$-linear secret sharing scheme Σ with information ratio $\rho(\Sigma) = \boldsymbol{w} \cdot \Phi^{\Pi}(P)/n$.*

2.5 Coding Schemes

An Algebraic Manipulation Detection (AMD) code is a coding scheme with the ability to detect a certain type of tempering.

Definition 1 ([10]) Let $\mathcal{S}$ be a finite set and $\mathcal{C}$ be a finite commutative group. Let (E, D) be a pair formed by a probabilistic encoding map $\mathsf{E} : \mathcal{S} \to \mathcal{C}$ and a deterministic decoding map $\mathsf{D} : \mathcal{C} \to \mathcal{S} \cup \{\perp\}$ such that $\mathsf{D}(\mathsf{E}(s)) = s$ with probability 1 for every $s \in \mathcal{S}$. We say that (E, D) is a δ-AMD code if

$$\Pr[\mathsf{D}(\mathsf{E}(s) + c) \notin \{s, \perp\}] \leq \delta$$

for any $s \in \mathcal{S}$ and $c \in \mathcal{C}$ with $c \neq 0$.

We show a simple construction of an AMD code. Let m be a positive integer and naturally embed $\mathbb{F}_q$ into $\mathbb{F}_{q^m}$.

Proposition 2 ([4]) *Let $\mathcal{S} = \mathbb{F}_q$, $\mathcal{R} \subseteq \mathbb{F}_{q^m}$, $\mathcal{T} = \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$, and $\mathcal{C} = \mathcal{S} \times \mathcal{T}$. Define $\mathsf{E} : \mathcal{S} \times \mathcal{R} \to \mathcal{C}$ as $\mathsf{E}(s, r) = (s, r, sr)$ for $s \in \mathbb{F}_q$ and $r \in \mathcal{R}$ and define $\mathsf{D} : \mathcal{C} \to \mathcal{S} \cup \{\perp\}$ as*

$$\mathsf{D}(c) = \begin{cases} x, & \text{if } xy = z, \\ \perp, & \text{otherwise} \end{cases}$$

for $c = (x, y, z)$ with $x \in \mathbb{F}_q$, $y \in \mathbb{F}_{q^m}$, and $z \in \mathbb{F}_{q^m}$. Then (E, D) is a δ-AMD code with $\delta = |\mathcal{R}|^{-1}$.

We recall the classically known MDS property of Reed-Solomon codes.

Proposition 3 *Let n and k be positive integers. Let q be a prime power with $q \geq n$ and fix pairwise distinct n elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$. Define $\mathcal{C}$ as the set of all possible codewords of the (n, k)-Reed-Solomon code, that is, $\mathcal{C} = \{(f(\alpha_i))_{i \in [n]} : f \in \mathbb{F}_q[X], \deg f < k\}$. Then, for any $c, c' \in \mathcal{C}$ with $c \neq c'$, it holds that the number of non-zeros entries of $c - c'$ is more than $n - k$.*

3 d-MSS for Multipartite Q_d-Adversary Structures

In this section, we propose a d-MSS scheme which can be applied to any ℓ-partite Q_d-adversary structure. We also show that the field size can be reduced if the adversary structure satisfies a stronger property than Q_d.

First, we restate the Q_d property in the multipartite setting.

Proposition 4 *A Π-partite adversary structure Δ satisfies the Q_d property if and only if $\boldsymbol{x}_1 + \cdots + \boldsymbol{x}_d \ngeq \Phi^{\Pi}(P)$ for any (not necessarily distinct) d points $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_d \in \Phi^{\Pi}(\Delta)$.*

Proof Assume that P is covered by d subsets $B_1, \ldots, B_d \in \Delta$. Since Δ is monotonically decreasing, we may assume that the B_i's are pairwise disjoint. Then it holds that $\Phi^{\Pi}(B_i) \in \Phi^{\Pi}(\Delta)$ and $\Phi^{\Pi}(B_1) + \cdots + \Phi^{\Pi}(B_d) = \Phi^{\Pi}(P)$. Conversely, assume that there exists d points $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_d \in \Phi^{\Pi}(\Delta)$ such that $\boldsymbol{x}_1 + \cdots + \boldsymbol{x}_d \geq \Phi^{\Pi}(P)$. We can replace the $\boldsymbol{x}_i$'s with d points $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d \in \Phi^{\Pi}(\Delta)$ such that $\boldsymbol{b}_i \leq \boldsymbol{x}_i$ and $\boldsymbol{b}_1 + \cdots + \boldsymbol{b}_d = \Phi^{\Pi}(P)$. Then there exist pairwise disjoint d subsets $B_1, \ldots, B_d \in \Delta$ such that $\boldsymbol{x}_i = \Phi^{\Pi}(B_i)$. We have that $B_1 \cup \cdots \cup B_d = P$. □

We introduce a stronger notion of the Q_d property with margin κ for a parameter $0 \leq \kappa < 1$. Note that this notion depends on a choice of the partition Π. In view of Proposition 4, the Q_d property with margin 0 is equivalent to the Q_d property.

Definition 2 For κ with $0 \leq \kappa < 1$, we say that a Π-partite adversary structure Δ satisfies the Q_d property with margin κ if $\boldsymbol{x}_1 + \cdots + \boldsymbol{x}_d \ngeq (1 - \kappa)\Phi^{\Pi}(P)$ for any (not necessarily distinct) d points $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_d \in \Phi^{\Pi}(\Delta)$.

3.1 A Scheme over $\mathbb{F}_q$ with $q > n$

3.1.1 Technical Overview

Assume that Δ satisfies the Q_d property. We decompose Δ into $N = |\max \Phi^{\Pi}(\Delta)|$ sub-structures, i.e., $\Delta = \Delta_1 \cup \cdots \cup \Delta_N$, where $\Delta_m = \{A \subseteq P : \Phi^{\Pi}(A) \leq \boldsymbol{a}_m\}$. We construct a secret sharing scheme Σ_m for Δ_m as follows: Given a secret s, Σ_m shares it via the $(\boldsymbol{a}_m(k), |P_k|)$-Shamir scheme for each part P_k, $k \in [\ell]$. We combine these atomic schemes to obtain our final one Σ. That is, Σ first splits a secret s into N random elements $s_1, \ldots, s_N$ such that $s = s_1 + \cdots + s_N$. It then shares each element s_m via Σ_m. Clearly, the Δ-privacy holds since players in $T \in \Delta$ cannot learn at least one element s_m such that $T \in \Delta_m$, due to the Δ_m-privacy of Σ_m.

To see the d-multiplicativity of Σ, suppose that d secrets $s^{(1)}, \ldots, s^{(d)}$ are shared via Σ. Our goal is to allow each player to obtain an additive share of $s^{(1)} \cdots s^{(d)}$. Since each $s^{(j)}$ is split into N elements $s_1^{(j)}, \ldots, s_N^{(j)}$, the product can be computed as

$$s^{(1)} \cdots s^{(d)} = \sum_{i_1=1}^{N} \cdots \sum_{i_d=1}^{N} s_{i_1}^{(1)} \cdots s_{i_d}^{(d)}. \tag{1}$$

A key observation is that for every $(i_1, \ldots, i_d)$, there is some $k \in [\ell]$ such that $\boldsymbol{a}_{i_1}(k) + \cdots + \boldsymbol{a}_{i_d}(k) < |P_k|$ in view of Proposition 4. Then, we have a partition $(J_1, \ldots, J_k)$ of $[N]^d$ such that if $(i_1, \ldots, i_d) \in J_k$, then $\boldsymbol{a}_{i_1}(k) + \cdots + \boldsymbol{a}_{i_d}(k) < |P_k|$. Following the partition, we can decompose the sum of N^d monomials into k parts:

$$s^{(1)} \cdots s^{(d)} = \sum_{k \in [\ell]} \sum_{(i_1, \ldots, i_d) \in J_k} s_{i_1}^{(1)} \cdots s_{i_d}^{(d)}$$

It is now sufficient to have players in each P_k compute additive shares of $t_k := \sum_{(i_1, \ldots, i_d) \in J_k} s_{i_1}^{(1)} \cdots s_{i_d}^{(d)}$. As a share for $s_m^{(j)}$, a player in P_k receives a point on a polynomial whose constant term is $s_m^{(j)}$ and whose degree is $\boldsymbol{a}_m(k)$. Note that t_k can be viewed as a function of $s_{i_1}^{(1)}, \ldots, s_{i_d}^{(d)}$. By homomorphically evaluating the function on his shares, he can locally compute a point on a polynomial g_k whose constant term is t_k and whose degree is at most $\boldsymbol{a}_{i_1}(k) + \cdots + \boldsymbol{a}_{i_d}(k) < |P_k|$. Therefore, players in P_k can compute additive shares of $g_k(0) = t_k$ by Lagrange interpolation.

3.1.2 Formal Description

Now, we show our d-MSS scheme for any multipartite Q_d-adversary structure.

Theorem 1 *Assume that Δ satisfies the Q_d property. Let $\mathbb{F}_q$ be a finite field with $q > n$. Then, the scheme Σ described in Fig. 2 is a Δ-private d-multiplicative $\mathbb{F}_q$-linear secret sharing scheme with information ratio $\rho(\Sigma) = N = |\max \Phi^{\Pi}(\Delta)|$.*

Notations.
- Let $\alpha_1, \ldots, \alpha_n$ be n distinct non-zero elements of $\mathbb{F}_q$.

SHARE. Given a secret $s \in \mathbb{F}_q$:
1. Choose $s_j \in \mathbb{F}_q$, $j \in [N]$ at random such that $s = \sum_{j \in [N]} s_j$.
2. For each $j \in [N]$ and $k \in [\ell]$, choose $f_{jk} \in \mathbb{F}_q[X]$ at random such that $s_j = f_{jk}(0)$ and $\deg f_{jk} \leq \boldsymbol{a}_j(k)$.
3. Output $(f_{jk}(\alpha_i))_{j \in [N]}$ as a share for $i \in P_k$.

Fig. 2 A secret sharing scheme for an ℓ-partite adversary structure Δ

Proof To prove Δ-privacy, let $A \in \Delta$ and $j \in [N]$ be such that $\Phi^{\Pi}(A) \leq \boldsymbol{a}_j$. For each $k \in [\ell]$, players in $A \cap P_k$ have at most $|A \cap P_k| \leq \boldsymbol{a}_j(k)$ shares of the $(\boldsymbol{a}_j(k), |P_k|)$-Shamir scheme for s_j and hence obtain no information on s_j. Since Shamir's schemes are independently invoked, players in $A = \bigcup_{k \in [\ell]} (A \cap P_k)$ have no information on s_j, either. Therefore, s is private to A since it is masked by the unknown element s_j.

To prove d-multiplicativity, let $s^{(1)}, \ldots, s^{(d)}$ be any d secrets. Our goal is to allow players $i \in P$ to compute additive shares of $s^{(1)} \cdots s^{(d)}$. Since $s^{(m)}$ is split as $s^{(m)} = s_1^{(m)} + \cdots + s_N^{(m)}$, we have that

$$s^{(1)} \cdots s^{(d)} = \sum_{\boldsymbol{j} = (j_1, \ldots, j_d) \in [N]^d} s_{j_1}^{(1)} \cdots s_{j_d}^{(d)}.$$

Since Δ is Q_d, it holds that $\boldsymbol{a}_{j_1} + \cdots + \boldsymbol{a}_{j_d} \not\geq \Phi^{\Pi}(P)$ for every $\boldsymbol{j} = (j_1, \ldots, j_d) \in [N]^d$. In particular, there exists a map $\psi : [N]^d \to [\ell]$ such that $\boldsymbol{a}_{j_1}(\psi(\boldsymbol{j})) + \cdots + \boldsymbol{a}_{j_d}(\psi(\boldsymbol{j})) < |P_{\psi(\boldsymbol{j})}|$ for every $\boldsymbol{j} = (j_1, \ldots, j_d) \in [N]^d$. Let $J_k = \psi^{-1}(k) \subseteq [N]^d$ for $k \in [\ell]$. Then, $(J_1, \ldots, J_k)$ is a partition of $[N]^d$ and we have that

$$s^{(1)} \cdots s^{(d)} = \sum_{k \in [\ell]} \sum_{\boldsymbol{j} \in J_k} s_{j_1}^{(1)} \cdots s_{j_d}^{(d)} = \sum_{k \in [\ell]} t_k,$$

where $t_k := \sum_{\boldsymbol{j} \in J_k} s_{j_1}^{(1)} \cdots s_{j_d}^{(d)}$. It is then sufficient to allow each player $i \in P_k$ to compute ζ_i such that $t_k = \sum_{i \in P_k} \zeta_i$, since $(\zeta_i)_{i \in P}$ is now additive sharing of $s^{(1)} \cdots s^{(d)}$.

From Fig. 2, any share assigned to a player $i \in P_k$ for a secret $s^{(m)}$ has the form of $(f_{1k}^{(m)}(\alpha_i), \ldots, f_{Nk}^{(m)}(\alpha_i))$, where each $f_{jk}^{(m)}$ is a polynomial of degree at most $\boldsymbol{a}_j(k)$ and $s_j^{(m)} = f_{jk}^{(m)}(0)$ for $j \in [N]$. Therefore, for any $k \in [\ell]$ and $\boldsymbol{j} \in \psi^{-1}(k)$, we have that

$$s_{j_1}^{(1)} \cdots s_{j_d}^{(d)} = (f_{j_1 k}^{(1)} \cdots f_{j_d k}^{(d)})(0) \text{ and } \deg(f_{jk}^{(1)} \cdots f_{jk}^{(d)}) < |P_k|.$$

Define a polynomial g_k as $g_k = \sum_{\boldsymbol{j} \in J_k} f_{j_1 k}^{(1)} \cdots f_{j_d k}^{(d)}$. Then,

$$g_k(0) = \sum_{\boldsymbol{j} \in J_k} s_{j_1}^{(1)} \cdots s_{j_d}^{(d)} = t_k \text{ and } \deg g_k \leq \max_{\boldsymbol{j} \in J_k} \{\boldsymbol{a}_{j_1}(k) + \cdots + \boldsymbol{a}_{j_d}(k)\} < |P_k|.$$

Note that each player $i \in P_k$ can locally compute $g_k(\alpha_i)$ from his shares as $g_k(\alpha_i) = \sum_{\boldsymbol{j} \in J_k} f^{(1)}_{j_1 d}(\alpha_i) \cdots f^{(d)}_{j_d k}(\alpha_i)$. Thus, each player in P_k obtains ζ_i by Lagrange interpolation. Formally, there are constants $\lambda_i \in \mathbb{F}_q$ (independent of g_k) such that $g_k(0) = \sum_{i \in P_k} \lambda_i g_k(\alpha_i)$, which means that $\zeta_i := \lambda_i g_k(\alpha_i)$ sum up to t_k. In a nutshell, the d-multiplicativity follows by defining $\mathsf{MULT} : P \times (\mathbb{F}_q^N)^d \to \mathbb{F}_q$ as

$$\mathsf{MULT}(i, (x^{(1)}_1, \ldots, x^{(1)}_N), \ldots, (x^{(d)}_1, \ldots, x^{(d)}_N)) = \lambda_i \sum_{\boldsymbol{j} \in J_k} x^{(1)}_{j_1} \cdots x^{(d)}_{j_d} \text{ if } i \in P_k.$$

□

3.2 A Scheme over $\mathbb{F}_q$ with q independent of n

The scheme in Theorem 1 requires that the field size q is greater than n since it is based on Shamir's scheme. We show that it can be modified into the one in which q can be chosen independent of n.

3.2.1 Technical Overview

We replace each $(\boldsymbol{a}_m(k), |P_k|)$-Shamir scheme in the construction of Theorem 1 with the $(\boldsymbol{a}_m(k) + 2g, |P_k|)$-AG scheme based on an algebraic function field F of genus g over $\mathbb{F}_q$. The choice of F will be specified later. Instead of a polynomial, the AG scheme randomly chooses a function f from a Riemann-Roch space $\mathcal{L}(D)$ for a certain divisor D when sharing a secret.

We can make almost the same argument as Theorem 1 by replacing a polynomial with a function $f \in \mathcal{L}(D)$ and the degree of a polynomial with the degree of a divisor. In Theorem 1, players compute additive shares of all monomials $s^{(1)}_{i_1} \cdots s^{(d)}_{i_d}$ assigned to them in Eq. (1). A key condition was that the degree of a polynomial associated with each monomial $s^{(1)}_{i_1} \cdots s^{(d)}_{i_d}$ was less than the number of players in some part P_k. In the variant based on AG schemes, it means that the degree of an associated divisor D must be less than $|P_k|$ for some $k \in [\ell]$. If that condition holds, players in P_k can locally compute additive shares of a point of $f \in \mathcal{L}(D)$ from their shares analogous to Lagrange interpolation. The multiplication property then follows as in Theorem 1.

Due to an additive factor $2g$ in thresholds, the above condition is translated to that there is $k \in [\ell]$ such that $\boldsymbol{a}_{i_1}(k) + \cdots + \boldsymbol{a}_{i_d}(k) + 2gd < |P_k|$. A sufficient condition is that Δ satisfies the Q_d property with margin κ for

$$\kappa \geq \frac{2dg}{\min_{j \in [\ell]} |P_j|}, \tag{2}$$

since $\boldsymbol{a}_{i_1}(k) + \cdots + \boldsymbol{a}_{i_d}(k) < (1 - \kappa)|P_k| < |P_k| - 2dg$ from Definition 2. Our scheme is then d-multiplicative for such Δ (Proposition 5).

We have to choose F such that the number of places of degree 1 is more than $n+1$, which is analogous to the assumption $q > n$ of Shamir's scheme, and

Notations.
- Let F be an algebraic function field with $n+2$ distinct places $Q, R_0, R_1, \ldots, R_n \in \mathbb{P}_q^{(1)}(F)$ and let $D_{jk} = (\boldsymbol{a}_j(k) + 2g)Q \in \mathrm{Div}(F)$ for $j \in [N]$ and $k \in [\ell]$.

SHARE. Given a secret $s \in \mathbb{F}_q$:
1. Choose $s_j \in \mathbb{F}_q$, $j \in [N]$ at random such that $s = \sum_{j\in[N]} s_j$.
2. For each $j \in [N]$ and $k \in [\ell]$, choose $f_{jk} \in \mathcal{L}(D_{jk})$ at random such that $s_j = f_{jk}(R_0)$.
3. Output $(f_{jk}(R_i))_{j\in[N]}$ as a share for $i \in P_k$.

Fig. 3 A secret sharing scheme for an ℓ-partite adversary structure Δ based on AG schemes

also that the genus g satisfies the condition (2). We use a family of algebraic function fields $\{F_m\}_{m\in\mathbb{N}}$ [15]. If q exceeds a constant depending κ, d and $\mu := \min_{j\in[\ell]} |P_j|/n$ only, it is possible to choose a desired function field F_m from this family. Note that if μ is constant (i.e., Π is balanced), we obtain a d-MSS scheme whose shares are $N = |\max \Phi^{\Pi}(\Delta)|$ elements of a *constant* field for arbitrary n (Theorem 2). While N may depend on n in general, we present a practical example of Δ such that N is also constant (Example 1).

3.2.2 Formal Description

We first prove the following.

Proposition 5 *Assume that Δ satisfies the Q_d property with margin κ. Let F be an algebraic function field of genus g defined over $\mathbb{F}_q$ such that $n + 1 < |\mathbb{P}_q^{(1)}(F)|$ and $g \le \kappa \min_{k\in[\ell]} |P_k|/(2d)$. Then, the scheme Σ described in Fig. 3 is a Δ-private d-multiplicative $\mathbb{F}_q$-linear secret sharing scheme such that $\rho(\Sigma) = N = |\max \Phi^{\Pi}(\Delta)|$.*

Proof The Δ-privacy follows from an argument similar to the proof of Theorem 1 and the privacy of the underlying AG schemes.

To prove the d-multiplicativity, let $s^{(1)}, \ldots, s^{(d)}$ be any d secrets. It follows from $\kappa \ge 2gd/\min_{k\in[\ell]} |P_k|$ that $(1-\kappa)\Phi^{\Pi}(P) \le \Phi^{\Pi}(P) - 2gd\mathbf{1}$. We then have a map $\psi : [N]^d \to [\ell]$ such that $\boldsymbol{a}_{j_1}(\psi(\boldsymbol{j})) + \cdots + \boldsymbol{a}_{j_d}(\psi(\boldsymbol{j})) + 2gd < |P_{\psi(\boldsymbol{j})}|$ for every $\boldsymbol{j} = (j_1, \ldots, j_d) \in [N]^d$. Since $s^{(m)}$ is split as $s^{(m)} = s_1^{(m)} + \cdots + s_N^{(m)}$, we have that

$$s^{(1)} \cdots s^{(d)} = \sum_{k\in[\ell]} \sum_{\boldsymbol{j}\in J_k} s_{j_1}^{(1)} \cdots s_{j_d}^{(d)} = \sum_{k\in[\ell]} t_k,$$

where $J_k = \psi^{-1}(k)$ and $t_k := \sum_{\boldsymbol{j}\in J_k} s_{j_1}^{(1)} \cdots s_{j_d}^{(d)}$. As in Theorem 1, it is sufficient to allow each player $i \in P_k$ to compute ζ_i such that $t_k = \sum_{i\in P_k} \zeta_i$.

A share assigned to $i \in P_k$ for a secret $s^{(m)}$ has the form of $(f_{1k}^{(m)}(R_i), \ldots, f_{Nk}^{(m)}(R_i))$, where $f_{jk}^{(m)} \in \mathcal{L}(D_{jk})$ and $s_j^{(m)} = f_{jk}^{(m)}(R_0)$ for $j \in [N]$. Therefore, for any

$k \in [\ell]$ and $\boldsymbol{j} \in \psi^{-1}(k)$, we have that

$$s_{j_1}^{(1)} \cdots s_{j_d}^{(d)} = (f_{j_1 k}^{(1)} \cdots f_{j_d k}^{(d)})(R_0) \text{ and } f_{jk}^{(1)} \cdots f_{jk}^{(d)} \in \mathcal{L}(D_{j_1 k} + \cdots + D_{j_d k}).$$

Define a function g_k as $g_k = \sum_{\boldsymbol{j} \in J_k} f_{j_1 k}^{(1)} \cdots f_{j_d k}^{(d)}$. Then,

$$g_k(R_0) = \sum_{\boldsymbol{j} \in J_k} s_{j_1}^{(1)} \cdots s_{j_d}^{(d)} = t_k$$

and $g_k \in \mathcal{L}(D)$ for a divisor D such that

$$\deg(D) \leq \max_{\boldsymbol{j} \in J_k} \{\deg(D_{j_1 k} + \cdots + D_{j_d k})\} < |P_k|$$

since $\deg D_{jk} = \boldsymbol{a}_j(k) + 2g$ and $\boldsymbol{a}_{j_1}(k) + \cdots + \boldsymbol{a}_{j_d}(k) + 2gd < |P_k|$.

Note that each player $i \in P_k$ can locally compute $g_k(R_i)$ from his shares as $g_k(R_i) = \sum_{\boldsymbol{j} \in J_k} f_{j_1 d}^{(1)}(R_i) \cdots f_{j_d k}^{(d)}(R_i)$. He can then obtain ζ_i from the following lemma.

Lemma 1 ([7]) *Let $D \in \mathrm{Div}(F)$ with $\deg(D) = r$ and t be an integer larger than r. Let $R_0, R_1, \ldots, R_t \in \mathbb{P}_q^{(1)}(F)$ be such that $\mathrm{supp}(D) \cap \{R_0, R_1, \ldots, R_t\} = \emptyset$. Then there exist constants $\lambda_1, \ldots, \lambda_t \in \mathbb{F}_q$ such that $h(R_0) = \sum_{i \in [t]} \lambda_i h(R_i)$ for any $h \in \mathcal{L}(D)$.*

Thus, there are constants $\lambda_i \in \mathbb{F}_q$ for $i \in P_k$ such that $g_k(R_0) = \sum_{i \in P_k} \lambda_i g_k(R_i)$, which means that $\zeta_i := \lambda_i g_k(R_i)$ sum up to t_k. □

As an instantiation of the underlying function field, let q be a square and consider a family of algebraic function fields $\{F_m\}_{m \in \mathbb{N}}$ defined over $\mathbb{F}_q$ such that $|\mathbb{P}_q^{(1)}(F_m)| \geq (\sqrt{q} - 1)\sqrt{q}^{m-1}$ and $g(F_m) \leq \sqrt{q}^m$ [15]. Then, for a "balanced" partition Π, we can obtain a d-MSS scheme over a field whose size is independent of n.

Theorem 2 *Assume that Δ satisfies the Q_d property with margin κ. Let $\mu > 0$ be such that $|P_k| \geq \mu n$ for every $k \in [\ell]$. Let q be a square with $\sqrt{q} - 2 \geq 2d/(\mu\kappa)$ and $m \in \mathbb{N}$ be such that*

$$(\sqrt{q} - 2)\sqrt{q}^m < n < (\sqrt{q} - 1)\sqrt{q}^m - 1. \tag{3}$$

Then there exists a Δ-private d-multiplicative $\mathbb{F}_q$-linear secret sharing scheme Σ such that $\rho(\Sigma) = N = |\max \Phi^{\Pi}(\Delta)|$.

Proof Let $\{F_m\}_{m \in \mathbb{N}}$ be the above family of algebraic function fields. Let $m \in \mathbb{N}$ be a number satisfying Eq. (3). Then it holds that $n < (\sqrt{q} - 1)\sqrt{q}^m - 1 \leq |\mathbb{P}_q^{(1)}(F_m)| - 1$ and

$$g(F_m) \leq \sqrt{q}^m \leq \frac{\sqrt{q}^m \kappa\mu(\sqrt{q} - 2)}{2d} \leq \frac{\kappa\mu n}{2d} \leq \frac{\kappa \min_{k \in [\ell]} |P_k|}{2d}.$$

Apply Proposition 5. □

Example 1 Let $n \in \mathbb{N}$ be an even number, $\Pi = (P_1, P_2)$ be a 2-partition such that $|P_1| = |P_2| = n/2$, and $\tau, \sigma \in \mathbb{R}_+$ such that $\sigma \leq \tau$. Define a Π-partite adversary structure $\mathcal{D}^{\Pi}_{\tau,\sigma} = \{X \subseteq P : |X| \leq \tau n \wedge (|X \cap P_1| \leq \sigma n \vee |X \cap P_2| \leq \sigma n)\}$. The motivation behind $\mathcal{D}^{\Pi}_{\tau,\sigma}$ is modification of $\mathcal{T}^n_k$ so that it takes into account a real-world situation. Suppose that the players are classified to two organizations P_1, P_2 and an adversary $\mathcal{A}$ is one of the players. If $\mathcal{A}$ belongs to P_1, then it would be more difficult for $\mathcal{A}$ to corrupt players in the other organization P_2 than players in P_1. We therefore add the constraint $|X \cap P_2| \leq \sigma n$ to the threshold constraint $|X| \leq \tau n$. Similarly, we require $|X \cap P_1| \leq \sigma n$. To tolerate $\mathcal{D}^{\Pi}_{\tau,\sigma}$, the threshold schemes [23,7,5] must tolerate $\mathcal{T}^n_k$ for $k \geq \tau n$ and hence is inapplicable to $\mathcal{D}^{\Pi}_{\tau,\sigma}$ for $\tau \geq 1/d$.

On the other hand, for an odd number d, our multipartite schemes can tolerate $\mathcal{D}^{\Pi}_{\tau,\sigma}$ for a wider range of τ and σ. Consider a larger Π-partite adversary structure $\mathcal{U}^{\Pi}_{\tau,\sigma}$ defined as $\max \Phi^{\Pi}(\mathcal{U}^{\Pi}_{\tau,\sigma}) = \{(\tau n, \sigma n), (\sigma n, \tau n)\}$. Then, it can be seen that $\mathcal{U}^{\Pi}_{\tau,\sigma}$ is Q_d with margin κ if and only if

$$\frac{d-1}{2d}\tau + \frac{d+1}{2d}\sigma < \frac{1}{2d}(1-\kappa). \tag{4}$$

Therefore, our multipartite schemes are applicable to $\mathcal{D}^{\Pi}_{\tau,\sigma}$ for $\tau < 1/(d-1)$ by appropriately choosing σ and κ. Our scheme in Theorem 1 can work for any τ and σ satisfying the condition (4) with $\kappa = 0$ while requiring the field size q to be greater than n. To apply Theorem 2, assume $q = 2^{12}$ and $d = 3$, for example. Since $\mu = \min\{|P_1|, |P_2|\}/n = 1/2$, we can choose $\kappa = 1/5$. Then, our scheme in Theorem 2 can work for any τ and σ such that $\tau + 2\sigma < 2/5$ and hence be applicable to $\mathcal{D}^{\Pi}_{\tau,\sigma}$ such that $(1/d =)1/3 \leq \tau < 2/5$. Although the range of applicable parameters is strictly smaller than that of Theorem 1, the field size q is now independent of n. We emphasize that when applied to MPC, point-to-point communication complexity is constant for arbitrary n.

4 d-MSS for Weighted Threshold Adversary Structures

In this section, we show another construction of a Δ-private d-MSS scheme that is more efficient than Theorem 1 for Δ such that players in each part have the same weight and a set of players is in Δ if and only if the sum of their weights is at most a threshold. Specifically, let $C = \mathrm{Conv}(\Phi^{\Pi}(\Delta))$ be the convex hull of $\Phi^{\Pi}(\Delta)$ in $\mathbb{R}^{\ell}$. Here, the convex hull of a finite set $S = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N\}$ is defined by the set of all points of the form $\sum_{j=1}^{N} \alpha_j \boldsymbol{x}_j$, where $\alpha_j \geq 0$ and $\sum_{j=1}^{N} \alpha_j = 1$. Set $\boldsymbol{p} = (1/d)\Phi^{\Pi}(P)$. We can construct a Δ-private d-MSS scheme if $\mathrm{dist}(\boldsymbol{p}, C) > 0$. It achieves a smaller information ratio than Theorem 1 for some class of adversary structures (Example 2).

If Δ is contained in a threshold adversary structure $\mathcal{T}^n_k$ with $dk < n$, it is more efficient to use the (k, n)-Shamir scheme, which is d-multiplicative. We note that our condition $\mathrm{dist}(\boldsymbol{p}, C) > 0$ is strictly weaker than $\Delta \subseteq \mathcal{T}^n_k$. Indeed, we also show in Example 2 that our construction works for a class of

non-threshold adversary structures to which the previous threshold schemes cannot be applied.

4.1 Technical Overview

We first show that if $\epsilon := \mathrm{dist}(\boldsymbol{p}, C) > 0$, there exist a hyperplane H passing through $\boldsymbol{p}$ such that C and hence $\Phi^{\Pi}(\Delta)$ is contained in one of its open half-spaces (Lemma 2). By clearing of fractions of its normal vector $\boldsymbol{h}$, we can find a weight vector $\boldsymbol{w} \in \mathbb{Z}_+^{\ell}$ and a threshold $t \in \mathbb{Z}_+$ such that $\Delta \subseteq \mathcal{W}^{\Pi}_{\boldsymbol{w},t}$ and $\boldsymbol{w} \cdot \Phi^{\Pi}(P) > dt$. Then we can obtain a d-MSS scheme for Δ from Proposition 1.

However, the choice of such a hyperplane H is not unique. The obtained scheme has a large information ratio if one chooses a hyperplane whose normal vector has high complexity. Our key observation is that since $\Phi^{\Pi}(\Delta)$ has finitely many points, if we continuously change $\boldsymbol{h}$ to $\boldsymbol{h}'$, the hyperplane H' determined by $\boldsymbol{h}'$ still satisfies the requirements, i.e., its open half-space still contains $\Phi^{\Pi}(\Delta)$. We show that there is $\boldsymbol{h}' \in \mathbb{Q}^{\ell}$ in a neighborhood of $\boldsymbol{h}$ such that each entry of $\boldsymbol{w}' = u\boldsymbol{h}'$ is $O(\ell n/\epsilon)$, where u is the least common multiple of the denominators of $\boldsymbol{h}'$ (Lemma 3). Based on the new hyperplane H', we obtain a d-MSS scheme for Δ with information ratio $O(\ell n/\epsilon)$ (Theorem 3).

4.2 Formal Description

To begin with, we show the following lemma.

Lemma 2 *Set $\boldsymbol{p} = (1/d)\Phi^{\Pi}(P)$. Let $C = \mathrm{Conv}(\Phi^{\Pi}(\Delta))$ be the convex hull of $\Phi^{\Pi}(\Delta)$ in $\mathbb{R}^{\ell}$. Suppose that $\mathrm{dist}(\boldsymbol{p}, C) \geq \epsilon > 0$. Then there exists a vector $\boldsymbol{h} \in \mathbb{R}_+^{\ell}$ with $\|\boldsymbol{h}\| = 1$ such that $\boldsymbol{h} \cdot (\boldsymbol{p} - \boldsymbol{x}) \geq \epsilon$ for any $\boldsymbol{x} \in \Phi^{\Pi}(\Delta)$.*

Proof Let $\boldsymbol{c}^* = \mathrm{argmin}_{\boldsymbol{c} \in C} \|\boldsymbol{p} - \boldsymbol{c}\|$ and set $\boldsymbol{h}_0 = \boldsymbol{p} - \boldsymbol{c}^*$. Note that $\|\boldsymbol{h}_0\| \geq \epsilon$. Then $\boldsymbol{h}_0 \cdot (\boldsymbol{p} - \boldsymbol{c}) \geq \|\boldsymbol{h}_0\|^2$ for any $\boldsymbol{c} \in C$. Indeed, let $\boldsymbol{c}$ be any point in C. For λ with $0 < \lambda < 1$, we define a point $\boldsymbol{c}_\lambda$ as $\boldsymbol{c}_\lambda = \lambda \boldsymbol{c} + (1 - \lambda)\boldsymbol{c}^*$. It follows from the definition of $\boldsymbol{c}^*$ that $\|\boldsymbol{c}_\lambda - \boldsymbol{p}\|^2 \geq \|\boldsymbol{c}^* - \boldsymbol{p}\|^2$. This implies that $0 \geq -\lambda \|\boldsymbol{c} - \boldsymbol{c}^*\|^2 + 2(\boldsymbol{c}^* - \boldsymbol{p}) \cdot (\boldsymbol{c}^* - \boldsymbol{c})$. By making λ approach to 0, we obtain $\boldsymbol{h}_0 \cdot (\boldsymbol{c}^* - \boldsymbol{c}) \geq 0$, which implies that $\boldsymbol{h}_0 \cdot (\boldsymbol{p} - \boldsymbol{c}) = \boldsymbol{h}_0 \cdot (\boldsymbol{p} - \boldsymbol{c}^*) + \boldsymbol{h}_0 \cdot (\boldsymbol{c}^* - \boldsymbol{c}) \geq \|\boldsymbol{h}_0\|^2$. We show that $\boldsymbol{h}_0 \in \mathbb{R}_+^{\ell}$. Assume that $\boldsymbol{c}^* \not\leq \boldsymbol{p}$. Then there is an index $j \in [\ell]$ with $\boldsymbol{c}^*(j) > \boldsymbol{p}(j)$. Set $\boldsymbol{c}' = \boldsymbol{c}^* - (\boldsymbol{c}^*(j) - \boldsymbol{p}(j))\boldsymbol{e}_j$. Since $\boldsymbol{0} \leq \boldsymbol{c}' \leq \boldsymbol{c}^*$, $\boldsymbol{c}'$ is in C. However, it holds that $\|\boldsymbol{c}' - \boldsymbol{p}\|^2 - \|\boldsymbol{c}^* - \boldsymbol{p}\|^2 = -(\boldsymbol{c}^*(j) - \boldsymbol{p}(j))^2 < 0$, which contradicts the definition of $\boldsymbol{c}^*$. Set $\boldsymbol{h} = \boldsymbol{h}_0 / \|\boldsymbol{h}_0\| \in \mathbb{R}_+^{\ell}$. Then $\|\boldsymbol{h}\| = 1$ and $\boldsymbol{h} \cdot (\boldsymbol{p} - \boldsymbol{x}) \geq \|\boldsymbol{h}_0\| \geq \epsilon$ for any $\boldsymbol{x} \in \Phi^{\Pi}(\Delta) \subseteq C$. □

We approximate $\boldsymbol{h}$ by a vector of rational numbers $\boldsymbol{h} + \boldsymbol{\delta}$ for a small vector $\boldsymbol{\delta}$ and set $\boldsymbol{w} = u(\boldsymbol{h} + \boldsymbol{\delta})$ for some integer u. Since $\boldsymbol{h} \cdot (\boldsymbol{p} - \boldsymbol{x}) \geq \epsilon$ for a finite number of vectors $\boldsymbol{x} \in \Phi^{\Pi}(\Delta)$, we can choose u to be $u = O(\ell n/\epsilon)$.

Lemma 3 *In the setting of Lemma 2, let* $\boldsymbol{h}$ *be a vector of* $\mathbb{R}^\ell_+$ *with* $\|\boldsymbol{h}\| = 1$ *such that* $\boldsymbol{h}\cdot(\boldsymbol{p}-\boldsymbol{x}) \geq \epsilon$ *for any* $\boldsymbol{x} \in \Phi^{\Pi}(\Delta)$*. Then there exists a vector* $\boldsymbol{w} \in \mathbb{Z}^\ell_+$ *such that* $\boldsymbol{w}\cdot(\boldsymbol{x}-\boldsymbol{p}) < 0$ *for every* $\boldsymbol{x} \in \Phi^{\Pi}(\Delta)$ *and* $0 \leq \boldsymbol{w}(j) \leq (\ell n/\epsilon) + 1$ *for every* $j \in [\ell]$*.*

Proof Write $\Phi^{\Pi}(\Delta) = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N\}$. Define a continuous function $f_j : \mathbb{R}^\ell \to \mathbb{R}$ as $f_j(\boldsymbol{w}) = \boldsymbol{w}\cdot(\boldsymbol{x}_j - \boldsymbol{p})$ for $j \in [N]$. Observe that $f_j(\boldsymbol{h}) \leq -\epsilon$ and that for any $\boldsymbol{\delta} \in \mathbb{R}^\ell$, $|f_j(\boldsymbol{h}+\boldsymbol{\delta}) - f_j(\boldsymbol{h})| \leq \|\boldsymbol{x}_j - \boldsymbol{p}\| \cdot \|\boldsymbol{\delta}\| \leq \sqrt{\ell}n\|\boldsymbol{\delta}\|$. Thus, $f_j(\boldsymbol{h}+\boldsymbol{\delta}) < 0$ for any $\boldsymbol{\delta} \in \mathbb{R}^\ell$ with $\|\boldsymbol{\delta}\| < \epsilon/(\sqrt{\ell}n)$. Let u be the smallest positive integer satisfying $u > \ell n/\epsilon$. Set $v_j = \lceil u\boldsymbol{h}(j) \rceil$ for each $j \in [\ell]$. Since $\|\boldsymbol{h}\| = 1$, we have $0 \leq u\boldsymbol{h}(j) \leq u$ and hence $0 \leq v_j \leq u$. Let $\boldsymbol{\delta} \in \mathbb{R}^\ell$ be a vector such that $0 \leq \boldsymbol{\delta}(j) = (v_j/u) - \boldsymbol{h}(j) \leq 1/u$. Then $\|\boldsymbol{\delta}\| \leq \|u^{-1}\mathbf{1}\| < \epsilon/(\sqrt{\ell}n)$. Set $\boldsymbol{w} = u(\boldsymbol{h}+\boldsymbol{\delta}) = (v_1, \ldots, v_\ell) \in \mathbb{Z}^\ell_+$. It holds that $f_j(\boldsymbol{w}) = uf_j(\boldsymbol{h}+\boldsymbol{\delta}) < 0$ for any $j \in [N]$ and $0 \leq \boldsymbol{w}(j) \leq u \leq (\ell n/\epsilon) + 1$. □

Now, we construct a d-MSS scheme using the weight vector $\boldsymbol{w}$.

Theorem 3 *Let* C *be the convex hull of* $\Phi^{\Pi}(\Delta)$ *in* $\mathbb{R}^\ell$*. Set* $\boldsymbol{p} = (1/d)\Phi^{\Pi}(P)$ *and suppose that* $\mathrm{dist}(\boldsymbol{p}, C) \geq \epsilon > 0$*. If* $\mathbb{F}_q$ *is a finite field with* $q > (\ell n^2/\epsilon) + n$*, then there exists a* Δ*-private* d*-multiplicative* $\mathbb{F}_q$*-linear secret sharing scheme whose information ratio is at most* $(\ell n/\epsilon) + 1$*.*

Proof From Lemma 3, we have $\boldsymbol{w} \in \mathbb{Z}^\ell_+$ such that $\boldsymbol{w}\cdot(\boldsymbol{x}-\boldsymbol{p}) < 0$ for any $\boldsymbol{x} \in \Phi^{\Pi}(\Delta)$ and $0 \leq \boldsymbol{w}(j) \leq (\ell n/\epsilon)+1$ for any $j \in [\ell]$. Set $t = \max_{\boldsymbol{x}\in\Phi^{\Pi}(\Delta)}\{\boldsymbol{w}\cdot\boldsymbol{x}\}$. Clearly, $\boldsymbol{w}\cdot\boldsymbol{x} \leq t$ for any $\boldsymbol{x} \in \Phi^{\Pi}(\Delta)$. Furthermore, $dt < \boldsymbol{w}\cdot\Phi^{\Pi}(P)$ since $\boldsymbol{w}\cdot\boldsymbol{x} < \boldsymbol{w}\cdot\boldsymbol{p}$ for any $\boldsymbol{x} \in \Phi^{\Pi}(\Delta)$. Since $q > n((\ell n/\epsilon) + 1)$, it holds that $q > \sum_{j\in[\ell]} |P_j| \max_{j\in[\ell]}\{\boldsymbol{w}(j)\} \geq \boldsymbol{w}\cdot\Phi^{\Pi}(P)$. Then, by applying Proposition 1, we obtain a Δ-private d-MSS scheme over $\mathbb{F}_q$ whose information ratio is $\boldsymbol{w}\cdot\Phi^{\Pi}(P)/n \leq (\ell n/\epsilon) + 1$. □

Example 2 Let d, k be positive integers and assume $n = dk - r$ for $0 \leq r < d-1$. For $S \subseteq P$, we consider the following $(S, P\setminus S)$-partite adversary structure $\mathcal{B}^n_k(S) = \mathcal{T}^n_{k-1} \cup \{A \subseteq P : |A| = k \wedge A \subseteq S\}$. It corresponds to a situation in which an adversary can corrupt any $k-1$ players in P and any k players in S. Since $n \leq dk$, the threshold schemes [23,7,5] are not d-multiplicative. It can be seen that $\mathcal{B}^n_k(S)$ is Q_d if $|S| < (d-r)k$. Consider the case of $|S| = (d-r)k-1$. Theorem 1 provides a $\mathcal{B}^n_k(S)$-private d-MSS scheme with information ratio k if $r > 0$ and 2 if $r = 0$. On the other hand, if $r > 0$, the convex hull $C = \mathrm{Conv}(\Phi^{\Pi}(\mathcal{B}^n_k(S)))$ is

$$C = \{(x, y) \in \mathbb{R}^2_+ : (k-1)x + ky \leq k(k-1)\}.$$

The closest point $\boldsymbol{c}^* \in C$ to $\boldsymbol{p}$ is on the line $(k-1)x + ky = k(k-1)$. In particular, $\boldsymbol{c}^* - \boldsymbol{p}$ is parallel to $(k-1, k)$. Therefore, we can set $\boldsymbol{w} \in \mathbb{Z}^2_+$ in the proof of Theorem 3 as $(k-1, k)$. We have $\mathcal{B}^n_k(S) \subseteq \mathcal{W}^{\Pi}_{\boldsymbol{w},t}$ for $t = k(k-1)$. As a result, we obtain a $\mathcal{B}^n_k(S)$-private d-MSS scheme whose information ratio is $\boldsymbol{w}\cdot\Phi^{\Pi}(P)/n = (dk^2 - dk + 1)/n < k - (d-r-1)/d$. Similarly, if $r = 0$, we obtain a d-MSS scheme with information ratio $(dk+1)/n = 1 + 1/n$. In both cases, the information ratios are smaller than the scheme from Theorem 1.

5 $(0, d)$-VMSS for Multipartite Q_{d+1}-Adversary Structures

In this section, we prove that the scheme Σ in Theorem 1 is a $(0, d)$-VMSS scheme if the adversary structure Δ is Q_{d+1}.

5.1 Technical Overview

Let $T \in \Delta$ be a set of all corrupted players. We present PROOF and VER for Σ assuming (for now) that T is known in advance. The problem is still non-trivial since we have to tell whether players in T actually modify their shares or they honestly behave.

Let $\boldsymbol{a}_m \in \max \Phi^{\Pi}(\Delta)$ be such that $\Phi^{\Pi}(T) \leq \boldsymbol{a}_m$. We first deal with the case of verifying the computation of a monomial $s^{(1)} \cdots s^{(d)}$. Recall that the product can be written as the sum of N^d monomials as shown in Eq. (1). Since Δ is Q_{d+1}, for every $(i_1, \ldots, i_d) \in [N]^d$, there exists $k \in [\ell]$ such that $\boldsymbol{a}_{i_1}(k) + \cdots + \boldsymbol{a}_{i_d}(k) < |P_k| - \boldsymbol{a}_m(k)$. Then, we have a partition $(J_1, \ldots, J_k)$ of $[N]^d$ such that if $(i_1, \ldots, i_d) \in J_k$, then $\boldsymbol{a}_{i_1}(k) + \cdots + \boldsymbol{a}_{i_d}(k) < |P_k| - \boldsymbol{a}_m(k)$. Following the partition, we can decompose the sum of N^d monomials into k parts:

$$s^{(1)} \cdots s^{(d)} = \sum_{k \in [\ell]} \sum_{(i_1, \ldots, i_d) \in J_k} s_{i_1}^{(1)} \cdots s_{i_d}^{(d)} \tag{5}$$

Our high-level idea of PROOF is that we let players in each P_k submit Shamir shares of $t_k := \sum_{(i_1, \ldots, i_d) \in J_k} s_{i_1}^{(1)} \cdots s_{i_d}^{(d)}$. Specifically, since each $s_v^{(j)}$ is shared via the $(\boldsymbol{a}_v(k), |P_k|)$-Shamir scheme, every player $i \in P_k$ can locally compute $g_k(\alpha_i)$ for a common polynomial g_k such that $g_k(0) = t_k$ and $\deg g_k < \max_{(i_1, \ldots, i_d) \in J_k} \{\boldsymbol{a}_{i_1}(k) + \cdots + \boldsymbol{a}_{i_d}(k)\} < |P_k| - \boldsymbol{a}_m(k)$. PROOF outputs $g_k(\alpha_i)$ as a proof for $i \in P_k$.

We then use the MDS property of a Reed-Solomon code to check the consistency of the Shamir shares. Our decoder Dec first reconstructs $g_k(0)$ from $(g_k(\alpha_i))_{i \in P_k}$ for each $k \in [\ell]$ and computes the sum $\eta = \sum_{k \in [\ell]} g_k(0)$, which can be done by Lagrange interpolation since $\deg g_k < |P_k|$. Note that η is equal to $s^{(1)} \cdots s^{(d)}$ unless proofs are modified. To verify that their proofs are Shamir shares, Dec also computes the syndrome ρ_k of $(g_k(\alpha_i))_{i \in P_k}$ viewed as a codeword of the Reed-Solomon code of length $|P_k|$ and dimension $|P_k| - \boldsymbol{a}_m(k)$. The syndrome ρ_k can be computed by multiplying the parity-check matrix to the vector of proofs. Note that $\rho_k = 0$ if and only if the vector is a codeword.

Now our verification algorithm VER checks if the following hold:

- The sum η is equal to the sum of additive shares outputted by MULT;
- All syndromes are equal to 0, i.e., $\rho_k = 0$ for all $k \in [\ell]$.

If corrupted players modify their proofs, the Hamming distance between the vector of proofs and the original codeword $(g_k(\alpha_i))_{i \in P_k}$ is at most $|T \cap P_k| \leq \boldsymbol{a}_m(k)$. Since the minimum Hamming distance of the Reed-Solomon code is

$|P_k|-(|P_k|-\boldsymbol{a}_m(k))+1 = \boldsymbol{a}_m(k)+1$, the vector of proofs cannot be a codeword and hence it holds that $\rho_k \neq 0$, which tells us the inconsistency.

When T is not known in advance, we perform the above procedures for all $\boldsymbol{a}_m \in \max \Phi^{\Pi}(\Delta)$ in parallel, which increases the share and proof sizes by N times. We can then detect inconsistency in at least one instance corresponding to $\boldsymbol{a}_m$ such that $\Phi^{\Pi}(T) \leq \boldsymbol{a}_m$. Thanks to the linearity of Dec and the underlying secret sharing schemes, it is straightforward to extend the above procedures to the case of verifying the computation of a polynomial.

5.2 Formal Description

Now, we present the formal descriptions of PROOF, Dec and VER for the MSS scheme in Theorem 1.

Theorem 4 *Let $\mathbb{F}_q$ be a finite field with $q > n$. Assume that Δ satisfies the Q_{d+1} property. Then, the scheme Σ described in Fig. 2 is a Δ-private, $(0,d)$-verifiably multiplicative (with respect to a linear decoder Dec), and $\mathbb{F}_q$-linear secret sharing scheme with domain of secrets $\mathbb{F}_q$, domain of shares $\mathbb{F}_q^N$, and domain of proofs $\mathbb{F}_q^N$, where $N = |\max \Phi^{\Pi}(\Delta)|$.*

Proof Since Δ is Q_{d+1}, for each $m \in [N]$, there is a map $\psi_m : [N]^d \to [\ell]$ such that for every $(j_1, \ldots, j_d) \in [N]^d$, it holds that $\boldsymbol{a}_{j_1}(k) + \cdots + \boldsymbol{a}_{j_d}(k) < |P_k| - \boldsymbol{a}_m(k)$, where $k = \psi_m(j_1, \ldots, j_d)$. For $k \in [\ell]$, let $(\lambda_{ki})_{i \in P_k}$ be a tuple of constants such that $g(0) = \sum_{i \in P_k} \lambda_{ki} g(\alpha_i)$ for any polynomial g of degree less than $|P_k|$, whose existence is guaranteed by Lagrange interpolation. To show that Σ is $(0,d)$-VMSS, we define PROOF, Dec and VER for Σ as shown in Fig. 4.

Let $x^{(i)} \in \mathbb{F}_q$ be an input of $i \in P$ and $h = \sum_{\boldsymbol{u} \in [n]^d} c_{\boldsymbol{u}} X_{u_1} \cdots X_{u_d}$ be a degree-d polynomial to compute, where $c_{\boldsymbol{u}} \in \mathbb{F}_q$. Let T be a set of players corrupted by an adversary Adv and $m \in [N]$ be such that $\Phi^{\Pi}(T) \leq \boldsymbol{a}_m$. We prove that the experiment $\mathrm{Exp}(x^{(1)}, \ldots, x^{(n)}, h, T, \mathsf{Adv})$ in Fig. 1 never outputs 1.

Let $X_{u_1} \cdots X_{u_d}$ be any monomial appearing in h. Note that each $x^{(i)}$ is split into N elements $s_1^{(i)}, \ldots, s_N^{(i)}$ when being shared by Σ. Also, $[N]^d$ is partitioned as $[N]^d = \psi_m^{-1}(1) \cup \cdots \cup \psi_m^{-1}(\ell)$. We therefore have that

$$\begin{aligned} x^{(u_1)} \cdots x^{(u_d)} &= \sum_{(i_1,\ldots,i_d) \in [N]^d} s_{i_1}^{(u_1)} \cdots s_{i_d}^{(u_d)} \\ &= \sum_{k \in [\ell]} \sum_{(i_1,\ldots,i_d) \in \psi_m^{-1}(k)} s_{i_1}^{(u_1)} \cdots s_{i_d}^{(u_d)} \\ &= \sum_{k \in [\ell]} t_k^{(\boldsymbol{u})}, \end{aligned}$$

Notations.

- Let $\alpha_1, \ldots, \alpha_n$ be n distinct non-zero elements $\mathbb{F}_q$.
- For $m \in [N]$, let $\psi_m : [N]^d \to [\ell]$ be a map such that for every $(j_1, \ldots, j_d) \in [N]^d$, it holds that $\boldsymbol{a}_{j_1}(k) + \cdots + \boldsymbol{a}_{j_d}(k) < |P_k| - \boldsymbol{a}_m(k)$, where $k = \psi_m(j_1, \ldots, j_d)$.
- For $k \in [\ell]$, let $(\lambda_{ki})_{i \in P_k}$ be constants such that $g(0) = \sum_{i \in P_k} \lambda_{ki} g(\alpha_i)$ for any polynomial g of degree less than $|P_k|$.
- Let $c'_m = \sum_{k \in [\ell]} \boldsymbol{a}_m(k) + 1$ for $m \in [N]$ and $c' = \sum_{m \in [N]} c'_m$.
- For $m \in [N]$ and $k \in [\ell]$, let $\boldsymbol{H}_{mk} \in \mathbb{F}_q^{\boldsymbol{a}_m(k) \times |P_k|}$ be a parity-check matrix of the Reed-Solomon code of length $|P_k|$ and dimension $|P_k| - \boldsymbol{a}_m(k)$.

PROOF. Given $i \in P$, a degree-d polynomial h, and n shares $\gamma_i^{(1)}, \ldots, \gamma_i^{(n)} \in \mathbb{F}_q^N$ of Σ:

1. Write h as $h = \sum_{\boldsymbol{u} \in [n]^d} c_{\boldsymbol{u}} X_{u_1} \cdots X_{u_d}$, where $c_{\boldsymbol{u}} \in \mathbb{F}_q$.
2. For each $j \in [n]$, parse $\gamma_i^{(j)}$ as $\gamma_i^{(j)} = (\beta_1^{(j)}, \ldots, \beta_N^{(j)})$, where $\beta_m^{(j)} \in \mathbb{F}_q$.
3. Let $k \in [\ell]$ be such that $i \in P_k$.
4. For each $m \in [N]$, do the following:
   (a) For each $\boldsymbol{u} \in [n]^d$, let $\delta_i^{(\boldsymbol{u})} = \sum_{(i_1, \ldots, i_d) \in \psi_m^{-1}(k)} \beta_{i_1}^{(u_1)} \cdots \beta_{i_d}^{(u_d)}$.
   (b) Let $\eta_{im} = \sum_{\boldsymbol{u} \in [n]^d} c_{\boldsymbol{u}} \delta_i^{(\boldsymbol{u})}$.
5. Output $\sigma_i = (\eta_{i1}, \ldots, \eta_{iN}) \in \mathbb{F}_q^N$.

Dec. Given $\sigma_i \in \mathbb{F}_q^N$ for $i \in P$:

1. For each $i \in P$, parse σ_i as $\sigma_i = (\eta_{i1}, \ldots, \eta_{iN})$, where $\sigma_{mi} \in \mathbb{F}_q$.
2. For each $m \in [N]$, do the following:
   (a) Let
   $$\rho_0 = \sum_{k \in [\ell]} \sum_{i \in P_k} \lambda_{ki} \eta_{im} \in \mathbb{F}_q.$$
   (b) For each $k \in [\ell]$, let
   $$\boldsymbol{\rho}_k = \boldsymbol{H}_{mk}(\eta_{im})_{i \in P_k} \in \mathbb{F}_q^{\boldsymbol{a}_m(k)}.$$
   (c) Let $\boldsymbol{\tau}_m = (\rho_0, \boldsymbol{\rho}_1, \ldots, \boldsymbol{\rho}_\ell) \in \mathbb{F}_q^{c'_m}$.
3. Output $\sigma = (\boldsymbol{\tau}_1, \ldots, \boldsymbol{\tau}_N) \in \mathbb{F}_q^{c'}$.

VER. Given $\zeta \in \mathbb{F}_q$ and $\sigma \in \mathbb{F}_q^{c'}$:

1. Parse σ as $\sigma = (\boldsymbol{\tau}_1, \ldots, \boldsymbol{\tau}_N)$, where $\boldsymbol{\tau}_m \in \mathbb{F}_q^{c'_m}$.
2. Output 1 if and only if $\boldsymbol{\tau}_m = (\zeta, 0, \ldots, 0)$ for all $m \in [N]$.

Fig. 4 PROOF, Dec and VER for the MSS scheme in Theorem 1

where $t_k^{(\boldsymbol{u})} = \sum_{(i_1, \ldots, i_d) \in \psi_m^{-1}(k)} s_{i_1}^{(u_1)} \cdots s_{i_d}^{(u_d)}$. Players in P_k have Shamir shares of each $s_\mu^{(j)}$ with threshold $\boldsymbol{a}_\mu(k)$ and hence they can locally compute Shamir shares of $s_{i_1}^{(u_1)} \cdots s_{i_d}^{(u_d)}$ with threshold $\boldsymbol{a}_{i_1}(k) + \cdots + \boldsymbol{a}_{i_d}(k)$. Therefore, the player $i \in P_k$ can obtain a Shamir share $\delta_i^{(\boldsymbol{u})}$ of $t_k^{(\boldsymbol{u})}$ with threshold

$$\max_{(i_1, \ldots, i_d) \in \psi_m^{-1}(k)} \{\boldsymbol{a}_{i_1}(k) + \cdots + \boldsymbol{a}_{i_d}(k)\} < |P_k| - \boldsymbol{a}_m(k),$$

which is done at Step 4(a) of PROOF.

By computing a linear combination of the above Shamir shares, every player $i \in P_k$ can obtain a Shamir share of $\sum_{\boldsymbol{u}\in[n]^d} c_{\boldsymbol{u}} t_k^{(\boldsymbol{u})}$ with threshold $< |P_k| - \boldsymbol{a}_m(k)$, which is denoted by η_{im} at Step 4(b) of PROOF. In other words, let $\sigma_i = (\eta_{i1}, \dots, \eta_{iN})$ denote the output of $\mathsf{PROOF}(i, h, \gamma_i^{(1)}, \dots, \gamma_i^{(n)})$. Then there exist polynomials $g_1, \dots, g_\ell$ such that

$$((g_1(\alpha_i))_{i\in P_1}, \dots, (g_\ell(\alpha_i))_{i\in P_\ell}) = (\eta_{1m}, \dots, \eta_{nm}),$$
$$g_1(0) + \cdots + g_\ell(0) = h(x^{(1)}, \dots, x^{(n)})$$

and $\deg g_k < |P_k| - \boldsymbol{a}_m(k)$ for all $k \in [\ell]$.

If Dec takes as input a tuple $(\sigma_i)_{i\in P}$ of correct proofs, ρ_0 computed by Dec at Step 2(a) is equal to

$$\sum_{k\in[\ell]} \sum_{i\in P_k} \lambda_{ki} g_k(\alpha_i) = \sum_{k\in[\ell]} g_k(0) = h(x^{(1)}, \dots, x^{(n)}).$$

Since $\boldsymbol{H}_{mk}$ is a parity-check matrix of the Reed-Solomon code of length $|P_k|$ and dimension $|P_k| - \boldsymbol{a}_m(k)$, we have that $\boldsymbol{\rho}_k = 0$ if and only if $(\eta_{im})_{i\in P_k}$ is a tuple of consistent Shamir shares with threshold $|P_k| - \boldsymbol{a}_m(k)$.

Therefore, if players in T honestly behave, it holds at Step 2 of VER that $\boldsymbol{\tau}_\mu = (h(x^{(1)}, \dots, x^{(n)}), 0, \dots, 0)$ for all $\mu \in [N]$ and then VER outputs 1, from which we see the correctness. Suppose that players in T modify their shares and proofs. The adversary wins only if $\boldsymbol{\tau}_m = (\zeta, 0, \dots, 0)$ for some $\zeta \neq h(x^{(1)}, \dots, x^{(n)})$. Then, players in T should have modified their proofs $(\eta_{im})_{i\in T}$ so that $\rho_0 = \zeta$ at Step 2(a) of Dec. However, this would imply that $(\eta_{im})_{i\in P_k}$ is different from a codeword $(g_k(\alpha_i))_{i\in P_k}$ for some $k \in [\ell]$. Since their Hamming distance is at most $|T \cap P_k| \leq \boldsymbol{a}_m(k)$, it follows from the MDS property of the Reed-Solomon code that the syndrome of $(\eta_{im})_{i\in P_k}$ is non-zero, i.e., $\boldsymbol{\rho}_k \neq 0$. We thus conclude that VER never outputs 1 in this case, which implies the error-free verifiability of Σ. □

5.3 Application to MPC

Based on our $(0, d)$-VMSS scheme, it is possible to construct an MPC protocol in which the output player outputs $h(x^{(1)}, \dots, x^{(n)})$ or $\perp$ (with probability 1) even if some corrupted players send incorrect messages.

In the protocol of [25], every player $i \in P$ shares their input $x^{(i)}$ among the other players. Then, every player $i \in P$ locally computes an additive share ζ_i of $h(x^{(1)}, \dots, x^{(n)})$ using MULT, and also computes a proof σ_i using PROOF. The output player collects all shares ζ_i and proofs σ_i, and computes $\zeta = \sum_{i\in P} \zeta_i$ and $\sigma = \mathsf{Dec}(\sigma_1, \dots, \sigma_n)$. He outputs ζ if $\mathsf{VER}(\zeta, \sigma) = 1$ and otherwise, outputs $\perp$. It is necessary to re-randomize the additive shares $(\zeta_i)_{i\in P}$ and the proofs $(\sigma_i)_{i\in P}$ since they may give the output player additional information beyond $h(x^{(1)}, \dots, x^{(n)})$. If Dec is additive, it can be done by letting all players generate fresh additive shares of 0 and send them along with their input shares at the first round. However, since the decoder of our scheme is not additive, we need a more complicated re-randomizing technique than [25].

Design. We modify the above protocol in such a way that proofs collected by the output player are uniformly distributed over the set of all possible proofs for $h(x^{(1)}, \ldots, x^{(n)})$. Observe that our decoder Dec is linear and that every vector of correct proofs $(\sigma_i)_{i \in P}$ satisfies $\mathsf{Dec}((\sigma_i)_{i \in P}) = (h(x^{(1)}, \ldots, x^{(n)}), 0, \ldots, 0) =: \sigma^*$. Thus, the set of all vectors of proofs is a coset $u^* + \mathcal{V}$, where $\mathcal{V}$ is the kernel of a linear map Dec and u^* is a vector such that $\mathsf{Dec}(u^*) = \sigma^*$. We let players choose a vector from $\mathcal{V}$ at random instead of fresh additive shares of 0. Specifically, each player $i \in P$ chooses $(w_j^{(i)})_{j \in P} \leftarrow\!\!\$\, \mathcal{V}$ and sends $w_j^{(i)}$ to $j \in P$ at the first round. At the second round, each player $i \in P$ sends $v_i = \sigma_i + \sum_{j \in P} w_i^{(j)}$ to the output player instead of σ_i.

We see that $(v_i)_{i \in P}$ leaks nothing beyond $h(x^{(1)}, \ldots, x^{(n)})$. Let T be a set of corrupted players. It is sufficient to show that the output player's views are indistinguishable between the cases where the honest players' input are $(x^{(i)})_{i \notin T}$ or $(\widetilde{x}^{(i)})_{i \notin T}$, if the value of h on them are the same. Assume that honest players $j \notin T$ have different inputs $\widetilde{x}^{(j)}$ such that $h((x^{(i)})_{i \in T}, (\widetilde{x}^{(i)})_{i \notin T}) = h((x^{(i)})_{i \in T}, (x^{(i)})_{i \notin T})$. Honest players proofs $(\sigma_i)_{i \notin T}$ based on the x_i's may change to different ones $(\widetilde{\sigma}_i)_{i \notin T}$ based on the $\widetilde{x}_i$'s. Nevertheless, the distribution of $(v_i)_{i \in P}$ is independent of whether honest players have inputs $(x_i)_{i \notin T}$ or $(\widetilde{x}_i)_{i \notin T}$. Indeed, $\mathsf{Dec}((\sigma_i)_{i \in T}, (\widetilde{\sigma}_i)_{i \notin T}) = \mathsf{Dec}((\sigma_i)_{i \in T}, (\sigma_i)_{i \notin T}) = \sigma^*$ since both vectors of proofs are for $h((x^{(i)})_{i \in T}, (\widetilde{x}^{(i)})_{i \notin T}) = h((x^{(i)})_{i \in T}, (x^{(i)})_{i \notin T})$. Then the difference between $((\sigma_i)_{i \in T}, (\widetilde{\sigma}_i)_{i \notin T})$ and $((\sigma_i)_{i \in T}, (\sigma_i)_{i \notin T})$ is in V. Since $(\sum_{j \in P} w_i^{(j)})_{i \in P}$ is uniformly distributed over $\mathcal{V}$, $(v_i)_{i \in P}$ is uniformly distributed over $u^* + \mathcal{V}$ regardless of the inputs of honest players.

Formal Description. Using the notations in the proof of Theorem 4, let $\mathcal{V} = \{(w_i)_{i \in P} \in (\mathbb{F}_q^N)^n : \mathsf{Dec}(w_1, \ldots, w_n) = 0\}$ be a linear subspace of $(\mathbb{F}_q^N)^n$. Based on our $(0, d)$-VMSS scheme Σ, we consider the following protocol for computing a degree-d polynomial $h = \sum_{\boldsymbol{u}} c_{\boldsymbol{u}} X_{u_1} \cdots X_{u_d}$.

Round 1

Each player $j \in P$ generates shares $(\gamma_i^{(j)})_{i \in P} = \mathsf{SHARE}(x^{(j)}, r^{(j)})$ of his input $x^{(j)}$ and sends $\gamma_i^{(j)}$ to $i \in P$. In addition, he randomly chooses n vectors $(z_i^{(j)}, w_i^{(j)}) \in \mathbb{F}_q^{1+N}$ for $i \in P$ conditioned on $\sum_{i \in P} z_i^{(j)} = 0$ and $(w_i^{(j)})_{i \in P} \in \mathcal{V}$, and sends $(z_i^{(j)}, w_i^{(j)})$ to $i \in P$.

Round 2

Each player $i \in P$ computes

$$\begin{aligned} \zeta_i &= \sum_{\boldsymbol{u} \in [n]^d} c_{\boldsymbol{u}} \mathsf{MULT}(i, \gamma_i^{(u_1)}, \ldots, \gamma_i^{(u_d)}), \\ \sigma_i &= \mathsf{PROOF}(i, h, \gamma_i^{(1)}, \ldots, \gamma_i^{(n)}), \text{ and} \\ (y_i, v_i) &= (\zeta_i, \sigma_i) + \sum_{j \in P} (z_i^{(j)}, w_i^{(j)}), \end{aligned}$$

and sends $(y_i, v_i) \in \mathbb{F}_q^{1+N}$ to an output player.

Output

The output player computes $\zeta = \sum_{i \in P} y_i$ and $\sigma = \mathsf{Dec}(v_1, \ldots, v_n)$, and outputs ζ if $\mathsf{VER}(\zeta, \sigma) = 1$ and otherwise $\perp$.

It clearly follows from Theorem 4 and the definition of $\mathcal{V}$ that the output player indeed receives $h(x^{(1)}, \ldots, x^{(n)})$ if all players submit correct messages and that he outputs $h(x^{(1)}, \ldots, x^{(n)})$ or $\perp$ (with probability 1) even if some subset of players in Δ send incorrect messages. The communication complexity is given by $(n^2\rho(\Sigma) + n^2(N+1) + n(N+1)) \log q = O(n^2 N \log q)$.

Note that the proofs σ_i may contain information on $(x^{(j)})_{j \notin T}$ beyond $(x^{(j)})_{j \in T}$ and $h(x^{(1)}, \ldots, x^{(n)})$. It is not trivial that an adversary colluding with the output player and a subset $T \in \Delta$ of input players learns additional information. Nevertheless, we can prove it thanks to masking with random vectors $(w_i^{(j)})_{i \in P}$ as follows.

Proposition 6 *Using the above notations, for any inputs $x^{(1)}, \ldots, x^{(n)}$ and any degree-d polynomial h, the view of the adversary corrupting the output player and a set of input players $T \in \Delta$ reveals no information on $(x^{(j)})_{j \notin T}$ beyond $h(x^{(1)}, \ldots, x^{(n)})$.*

Proof Here we only prove the privacy against part of the adversary's view regarding re-randomized proofs v_i's since the privacy against y_i's follows from the same argument as [1]. Observe that the randomness of the protocol unknown to the adversary is $R = (R_1, R_2)$, where

$$R_1 = (r^{(j)})_{j \notin T} \text{ and } R_2 = (w_i^{(j)})_{i \notin T, j \notin T}.$$

We fix the other randomness, which is known to her. We only need to take into account pieces in the adversary's view depending on honest players' inputs, that is, shares $(\gamma_i^{(j)})_{i \in T}$ sent by a player $j \notin T$ and re-randomized proofs $(v_i)_{i \in P}$. Also, observe that $(\gamma_i^{(j)})_{i \in T}$ is determined by inputs $x^{(j)}$ and randomness R_1, and $(v_i)_{i \in P}$ depends on inputs $\boldsymbol{x}$ and randomness $R = (R_1, R_2)$. We then use a notation

$$A(\boldsymbol{x}, R_1) = \{(\gamma_i^{(j)})_{i \in T} : j \notin T\} \text{ and } B(\boldsymbol{x}, R) = (v_i)_{i \in P}.$$

Let $(x^{(j)})_{j \notin T}$ be a tuple of different inputs for honest players such that $\zeta := h(\widetilde{\boldsymbol{x}}) = h(\boldsymbol{x})$, where $\widetilde{\boldsymbol{x}} = ((x^{(i)})_{i \in T}, (\widetilde{x}^{(i)})_{i \notin T})$. The statements follow if we show that the part of the adversary's view $A(\boldsymbol{x}, R_1), B(\boldsymbol{x}, R)$ on input $\boldsymbol{x}$ has the same distribution as $A(\widetilde{\boldsymbol{x}}, R_1), B(\widetilde{\boldsymbol{x}}, R)$ on input $\widetilde{\boldsymbol{x}}$. It is sufficient to show that there exists a one-to-one transformation θ on the randomness space of the protocol such that $A(\boldsymbol{x}, R_1) = A(\widetilde{\boldsymbol{x}}, \theta_1(R))$ and $B(\boldsymbol{x}, R) = B(\widetilde{\boldsymbol{x}}, \theta(R))$, where $\theta(R) = (\theta_1(R), \theta_2(R))$.

First, due to the Δ-privacy of Σ, shares held by T reveal no information on the underlying secret. We thus have a one-to-one transformation φ on the set of all R_1's such that $A(\boldsymbol{x}, R_1) = A(\widetilde{\boldsymbol{x}}, \varphi(R_1))$.

Let σ_i be a proof for ζ constructed by the player $i \in P$ in the case where the inputs are $\boldsymbol{x}$ and the randomness is $R_1 = (r^{(j)})_{j \in P}$. Here, it does not

depend on the other randomness R_2 since it is a function of shares only. Also, let $\widetilde{\sigma}_i$ be a proof for ζ constructed by $i \in P$ in the case where the inputs are $\widetilde{\boldsymbol{x}}$ and the randomness is $\varphi(R_1)$. Since $A(\boldsymbol{x}, R_1) = A(\widetilde{\boldsymbol{x}}, \varphi(R_1))$, we have that $\sigma_i = \widetilde{\sigma}_i$ for all $i \in T$. Since $h(\boldsymbol{x}) = \zeta = h(\widetilde{\boldsymbol{x}})$, it also holds that

$$\mathsf{Dec}(\sigma_1, \ldots, \sigma_n) = (\zeta, 0, \ldots, 0) = \mathsf{Dec}(\widetilde{\sigma}_1, \ldots, \widetilde{\sigma}_n)$$

and hence that $(\sigma_i)_{i \in P} - (\widetilde{\sigma}_i)_{i \in P} \in \mathcal{V}$.

Without loss of generality, we assume that $1 \notin T$. We define $\theta_1(R_1, R_2) = \varphi(R_1)$ and $\theta_2(R) = (\widetilde{w}_i^{(j)})_{i \notin T, j \notin T}$ as

$$\widetilde{w}_i^{(j)} = \begin{cases} w_i^{(1)} + \sigma_i - \widetilde{\sigma}_i, & \text{if } i \notin T \text{ and } j = 1, \\ w_i^{(j)}, & \text{otherwise.} \end{cases}$$

The image of R via $\theta = (\theta_1, \theta_2)$ is indeed in the domain since $(\sigma_i)_{i \in P} - (\widetilde{\sigma}_i)_{i \in P} \in \mathcal{V}$ implies $((w_i^{(j)})_{i \in T}, (\widetilde{w}_i^{(j)})_{i \notin T}) \in \mathcal{V}$. Clearly θ is one-to-one. We have seen above that $A(\boldsymbol{x}, R_1) = A(\widetilde{\boldsymbol{x}}, \theta_1(R))$. We see that $B(\boldsymbol{x}, R) = B(\widetilde{\boldsymbol{x}}, \theta(R))$ in the following. Let $B(\widetilde{\boldsymbol{x}}, \theta(R)) = (\widetilde{v}_i)_{i \in P}$. If $i \notin T$, then $\widetilde{v}_i = v_i$ since we have seen above that $\widetilde{\sigma}_i = \sigma_i$ for $i \notin T$. If $i \in T$, we also have $\widetilde{v}_i = v_i$ since

$$\begin{aligned} \widetilde{v}_i &= \widetilde{\sigma}_i + \sum_{j \notin T} \widetilde{w}_i^{(j)} + \sum_{j \in T} \widetilde{w}_i^{(j)} \\ &= \widetilde{\sigma}_i + (w_i^{(1)} + \sigma_i - \widetilde{\sigma}_i) + \sum_{j \notin T \cup \{1\}} \widetilde{w}_i^{(j)} + \sum_{j \in T} \widetilde{w}_i^{(j)} \\ &= \sigma_i + w_i^{(j)} + \sum_{j \in P} w_i^{(j)} \\ &= v_i. \end{aligned}$$

□

6 (δ, d)-VMSS for Multipartite Q_{d+1}-Adversary Structures with Margin κ

In this section, we show a (δ, d)-VMSS scheme whose proof size can be smaller than that of Theorem 4 while it requires $\delta > 0$ and the adversary structure satisfies the Q_{d+1}-property with margin $\kappa > 0$.

6.1 Technical Overview

Our construction is similar to the one in [25], in which players share a codeword of a certain AMD code [4,10] so that any tampering by an adversary will be detected. A difference is that our scheme shares the codeword, which is a vector, *simultaneously* while each entry of the codeword is shared *individually* in [25].

To deal with multiple secrets, we first construct a variant of the MSS scheme in Theorem 1 by replacing Shamir's schemes with packed secret sharing schemes [8]. A packed secret sharing scheme shares multiple secrets simultaneously without increasing the share size at the price of decreasing corruption tolerance. As a result, if a multipartite adversary structure Δ' satisfies the $Q_{d'}$ property with some margin $\kappa' > 0$, we obtain a d'-MSS scheme for Δ' which supports the element-wise product of d' vectors. Thanks to the packed secret sharing, the share size is the same as that of Theorem 1.

Let Δ be a Q_{d+1}-adversary structure with some margin $\kappa > 0$. We have a scheme Σ_0 for Δ which supports the product of $d+1$ vectors in $\mathbb{A} := \mathbb{F}_q^3$, from the above construction with $d' = d+1$. Given a secret $s \in \mathbb{F}_q$, our VMSS scheme Σ first chooses a random element $r \in \mathbb{F}_q$ and then shares two secrets using Σ_0: one is $\mathsf{E}(s, 1)$ and the other is $\mathsf{E}(1, r)$. Here, $\mathsf{E}(s, r)$ is an AMD codeword defined as $\mathsf{E}(s, r) = (s, r, sr) \in \mathbb{A}$. It is easy to see that Σ is d-multiplicative (with respect to $\mathbb{F}_q$) since players can compute additive shares of $\mathsf{E}(s^{(1)}, 1) * \cdots * \mathsf{E}(s^{(d)}, 1) = (s^{(1)} \cdots s^{(d)}, 1, s^{(1)} \cdots s^{(d)})$, where $*$ denotes the element-wise product.

We now see that Σ is (δ, d)-VMSS for $\delta = q^{-1}$. We first deal with a simple case of verifying the computation of a monomial $s^{(1)} \cdots s^{(d)}$. Then players receive shares generated by Σ_0 for secrets $\mathsf{E}(s^{(j)}, 1)$ and $\mathsf{E}(1, r^{(j)})$, $j \in [d]$. Since Σ_0 is $(d+1)$-multiplicative with respect to $\mathbb{A}$, they can compute additive shares for $\mathsf{E}(1, r^{(1)}) * \mathsf{E}(s^{(1)}, 1) * \cdots * \mathsf{E}(s^{(d)}, 1) = \mathsf{E}(s^{(1)} \cdots s^{(d)}, r^{(1)})$. We define these additive shares as their proofs. To verify a result, an output player reconstructs $\mathsf{E}(s^{(1)} \cdots s^{(d)}, r^{(1)})$ and checks if an adversary has tampered with shares. Since $r^{(1)}$ is uniformly distributed over $\mathbb{F}_q$ and unknown to the adversary due to Δ-privacy, the AMD code detects any tampering with probability $1 - q^{-1}$.

We then consider the general case where n players have inputs $x^{(i)}$, $i \in P$ and want to compute a polynomial $h(x^{(1)}, \ldots, x^{(n)})$ of degree d. Players receive shares generated by Σ_0 for secrets $\mathsf{E}(x^{(j)}, 1)$ and $\mathsf{E}(1, r^{(j)})$, $j \in [n]$. Since Σ_0 is linear, they can compute a share of Σ_0 for $\mathsf{E}(1, r^{(0)})$ by taking an average of $\mathsf{E}(1, r^{(j)})$'s, where $r^{(0)} = \sum_{j \in [d]} r^{(j)}/n$.[2] Then, for each monomial $x^{(i_1)} \cdots x^{(i_d)}$ appearing in h, they compute additive shares for $\mathsf{E}(1, r^{(0)}) * \mathsf{E}(x^{(i_1)}, 1) * \cdots * \mathsf{E}(x^{(i_d)}, 1) = \mathsf{E}(1, r^{(0)}) * \mathsf{E}(x^{(i_1)} \cdots x^{(i_d)}, 1)$. By computing a linear combination of them, they obtain additive shares for $\mathsf{E}(1, r^{(0)}) * \mathsf{E}(h(x^{(1)}, \ldots, x^{(n)}), h(1, \ldots, 1))$, which results in $\mathsf{E}(h(x^{(1)}, \ldots, x^{(n)}), r^{(0)})$ if we normalize h in advance so that $h(1, \ldots, 1) = 1$ holds. Similarly to the above, the probability that players output an incorrect value $\zeta \notin \{h(x^{(1)}, \ldots, x^{(n)}), \perp\}$ is at most q^{-1}. Note that it is possible to make the probability of failure q^{-m} by choosing each $r^{(j)}$ from an extension field $\mathbb{F}_{q^m}$.

[2] We here assume that n is coprime with q.

6.2 Formal Description

To begin with, we define a more general notion of d-MSS, which generalizes the previous definition in Section 2.2 in that it supports the product of d secrets from the *extension ring* $\mathbb{A}$ instead of those from $\mathbb{F}_q$. In particular, if we set $\mathbb{A} = \mathbb{F}_q$, this notion collapses to the previous one.

Definition 3 Let $\mathbb{A}$ be a finite-dimensional algebra over $\mathbb{F}_q$. For $d \geq 2$, a secret sharing scheme $\Sigma = (\mathbb{A}, \mathcal{R}, \mathcal{S}, \mathsf{SHARE})$ is said to be d-multiplicative with respect to $\mathbb{A}$ if there exists a map $\mathsf{MULT} : P \times \mathcal{S}^d \to \mathbb{A}$ such that

$$\prod_{j \in [d]} s^{(j)} = \sum_{i \in P} \mathsf{MULT}(i, \gamma_i^{(1)}, \ldots, \gamma_i^{(d)}), \tag{6}$$

for any $s^{(1)}, \ldots, s^{(d)} \in \mathbb{A}$ and any $r^{(1)}, \ldots, r^{(d)} \in \mathcal{R}$, where $(\gamma_i^{(j)})_{i \in P} = \mathsf{SHARE}(s^{(j)}, r^{(j)})$ is a tuple of shares for $s^{(j)}$. The product and summation in Eq. (6) are performed in the ring $\mathbb{A}$.

We use this generalized notion of d-MSS to share codewords of the AMD code given by Proposition 2. We set $\mathbb{A}$ as the set of all AMD codewords, i.e., $\mathbb{A} = \mathbb{F}_q \times \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$. Formally, we fix the following notations throughout this section:

- m is a prime and $L = 2m + 1$.
- $\alpha_1, \ldots, \alpha_n, \beta_1, \beta_2, \beta_3$ are $n + 3$ elements of $\overline{\mathbb{F}}_q$ such that there is no pair which are Galois-conjugates over $\mathbb{F}_q$, $\mathbb{F}_q(\alpha_i) = \mathbb{F}_q$ for $i \in P$, $\mathbb{F}_q(\beta_1) = \mathbb{F}_q$, and $\mathbb{F}_q(\beta_u) \simeq \mathbb{F}_{q^m}$ for $u = 2, 3$.
- $\mathbb{A}$ is the product ring $\mathbb{A} = \mathbb{F}_q(\beta_1) \times \mathbb{F}_q(\beta_2) \times \mathbb{F}_q(\beta_3)$.

We impose the condition on $\alpha_1, \ldots, \alpha_n, \beta_1, \beta_2, \beta_3$ to use the following generalized Lagrange interpolation.

Lemma 4 ([8]) *Let $\gamma_1, \ldots, \gamma_t \in \overline{\mathbb{F}}_q$ be such that there is no pair γ_i, γ_j, $i \neq j$ which are Galois-conjugates over $\mathbb{F}_q$. Let d_u be the degree of $\mathbb{F}_q(\gamma_u)/\mathbb{F}_q$ for $u \in [t]$ and set $M = \sum_{u \in [t]} d_u$. Then, for each $\xi_1, \ldots, \xi_t$ with $\xi_u \in \mathbb{F}_q(\gamma_u)$ ($u \in [t]$), there exists a unique polynomial $f(X) \in \mathbb{F}_q[X]$ such that $\deg f < M$ and $f(\gamma_u) = \xi_u$ for all $u \in [t]$.*

We note that there indeed exist such α_i's and β_i's. For a positive integer u, define the number $\nu(u, q)$ as $\nu(u, q) = (1/u) \sum_{x|u} \mu(x) q^{u/x}$, where x ranges over all divisors of u and $\mu(x)$ is the Möbius function, i.e., $\mu(x) = 1$ if x is a square-free integer with an even number of prime factors, $\mu(x) = -1$ if x is a square-free integer with an odd number of prime factors, and otherwise $\mu(x) = 0$. This number $\nu(u, q)$ is known to be the number of all irreducible polynomials of degree u over $\mathbb{F}_q$ [19, Section 4.13]. Therefore, a sufficient condition is that $\nu(1, q) \geq n+1$ and $\nu(m, q) \geq 2m$ since every $\gamma \in \mathbb{F}_{q^m}$ has at most m conjugates over $\mathbb{F}_q$. In particular, it is equivalent to $q \geq n + 1$ and $q^m - q \geq 2m$ if m is a prime. Since $q(q^{m-1} - 1) > q^{m-1} - 1$, it is sufficient to choose $q > \max\{n, (2m + 1)^{1/(m-1)}\}$.

Now, we show a variant of Theorem 1 that is d-MSS over $\mathbb{A}$.

SHARE. Given a secret $s \in \mathbb{A}$:

1. Choose $s_j \in \mathbb{A}$, $j \in [N]$ at random such that $s = \sum_{j\in[N]} s_j$.
2. For each $j \in [N]$, parse $s_j = (\xi_{j1}, \xi_{j2}, \xi_{j3})$, where $\xi_{ju} \in \mathbb{F}_q(\beta_u)$ for $u \in \{1,2,3\}$.
3. For each $j \in [N]$ and $k \in [\ell]$, choose $f_{jk} \in \mathbb{F}_q[X]$ at random such that $s_j = (f_{jk}(\beta_u))_{u\in\{1,2,3\}}$ and $\deg(f_{jk}) \le \boldsymbol{a}_j(k) + L - 1$.
4. Output $(f_{jk}(\alpha_i))_{j\in[N]}$ as a share for $i \in P_k$.

Fig. 5 A secret sharing scheme over $\mathbb{A}$ for an ℓ-partite adversary structure

Proposition 7 *Assume that Δ satisfies the Q_d property with margin κ and that $q > \max\{n, (2m+1)^{1/(m-1)}\}$. If $\kappa \ge d(L-1)/\min_{k\in[\ell]} |P_k|$, then the scheme Σ described in Fig. 5 is a Δ-private, d-multiplicative with respect to $\mathbb{A}$, and $\mathbb{F}_q$-linear secret sharing scheme with domain of secrets $\mathbb{A}$ and domain of shares $\mathbb{F}_q^N$, where $N = |\max \Phi^{\Pi}(\Delta)|$.*

Proof Using the notations in Fig. 5, let $(f_{1k}(\alpha_i), \ldots, f_{Nk}(\alpha_i))$ be a share assigned to $i \in P_k$ for a secret s. To prove Δ-privacy, let $A \in \Delta$ such that $\Phi^{\Pi}(A) = \boldsymbol{a}_j$ for some $j \in [N]$. We show that for each $k \in [\ell]$, the players in $A \cap P_k$ have no information on s_j. Indeed, in view of Lemma 4, for any $s' \in \mathbb{A}$, there is a unique polynomial $g \in \mathbb{F}_q[X]$ of degree at most $\boldsymbol{a}_j(k) + L - 1$ such that $(g(\beta_u))_{u\in\{1,2,3\}} = s'$ and $g(\alpha_i) = f_{jk}(\alpha_i)$ for all $i \in A \cap P_k$. That is, players in $A \cap P_k$ cannot distinguish between the cases where the underlying secret of their Shamir shares $(f_{jk}(\alpha_i))_{i\in A\cap P_k}$ is s' or s_j. Thus, players in A have no information on s_j and hence on s.

The d-multiplicativity follows from a similar argument in the proof of Theorem 1. Let $s^{(1)}, \ldots, s^{(d)} \in \mathbb{A}$ be any d secrets. Note that $s^{(\iota)}$ is split as $s^{(\iota)} = s_1^{(\iota)} + \cdots + s_N^{(\iota)}$. It is sufficient to show that players can compute additive shares of each summand $s_{j_1}^{(1)} \cdots s_{j_d}^{(d)}$. It follows from an argument similar to the proof of Proposition 5 that there is $k \in [\ell]$ such that $\boldsymbol{a}_{j_1}(k) + \cdots + \boldsymbol{a}_{j_d}(k) + d(L-1) < |P_k|$. From the construction, players in P_k have points of polynomials $f_{j_1k}^{(1)}, \ldots, f_{j_dk}^{(d)}$ such that for all $\iota \in [d]$, $(f_{j_\iota k}(\beta_u))_{u\in\{1,2,3\}} = s_{j_\iota}^{(\iota)}$ and $\deg f_{j_\iota k} \le \boldsymbol{a}_{j_\iota}(k) + L - 1$. Therefore, they can obtain points of a polynomial f such that $(f(\beta_u))_{u\in\{1,2,3\}} = s_{j_1}^{(1)} \cdots s_{j_d}^{(d)}$ and $\deg f \le \sum_{\iota\in[d]} \boldsymbol{a}_{j_\iota}(k) + d(L-1) < |P_k|$. It follows from Lemma 4 that f is uniquely determined. In particular, players in P_k can compute additive shares (over $\mathbb{A}$) for $(f(\beta_u))_{u\in\{1,2,3\}} = s_{j_1}^{(1)} \cdots s_{j_d}^{(d)}$. □

From the above proposition, we obtain an MSS scheme which can simultaneously share a codeword of the AMD code in Proposition 2. The scheme is shown to be (δ, d)-verifiably multiplicative for $\delta > 0$. Furthermore, due to its linearity, it works for degree-d *polynomials* while the previous scheme [25] only works for *monomials*. Since the decoder is additive, it is straightforward to apply it to MPC as in [25].

Theorem 5 *Assume that Δ satisfies the Q_{d+1} property with margin κ. Also, assume that q is coprime with n and $q > \max\{n, (2m+1)^{1/(m-1)}\}$. If $\kappa \ge$*

Notations.
- Let (E, D) be the δ-AMD code with $\mathcal{R} = \mathbb{F}_{q^m}$ and $\delta = q^{-m}$ in Proposition 2.
- Let $\Sigma_0 = (\mathbb{A}, \mathcal{R}_0, \mathcal{S}_0, \mathsf{SHARE}_0)$ a Δ-private secret sharing scheme that is $(d+1)$-multiplicative with respect to $\mathbb{A}$, and $\mathsf{MULT}_0 : P \times \mathcal{S}_0^{d+1} \to \mathbb{A}$ be the map associated with the $(d+1)$-multiplicativity of Σ_0.
- Fix a vector of shares $(1_i)_{i\in P}$ of Σ_0 for a secret $\mathsf{E}(1,1)$, that is, $(1_i)_{i\in P}$ is a possible output of $\mathsf{SHARE}_0(\mathsf{E}(1,1))$.

SHARE. Given a secret $s \in \mathbb{F}_q(\beta_1)$:
1. Choose $r \in \mathbb{F}_q(\beta_2)$ at random.
2. Let $(\eta_i)_{i\in P} = \mathsf{SHARE}(\mathsf{E}(s,1))$ and $(\xi_i)_{i\in P} = \mathsf{SHARE}(\mathsf{E}(1,r))$.
3. Output $\gamma_i = (\eta_i, \xi_i)$ as a share for $i \in P$.

MULT. Given $i \in P$ and d shares $\gamma_i^{(1)}, \ldots, \gamma_i^{(d)} \in \mathcal{S}$:
1. For each $j \in [d]$, parse $\gamma_i^{(j)}$ as $\gamma_i^{(j)} = (\eta_i^{(j)}, \xi_i^{(j)})$, where $\eta_i^{(j)}, \xi_i^{(j)} \in \mathcal{S}_0$.
2. Let $\widetilde{\zeta_i} = (\zeta_{i1}, \zeta_{i2}, \zeta_{i3}) = \mathsf{MULT}_0(i, 1_i, \eta_i^{(1)}, \ldots, \eta_i^{(d)}) \in \mathbb{A}$.
3. Output $\zeta_i = \zeta_{i1} \in \mathbb{F}_q(\beta_1)$.

PROOF. Given $i \in P$, a degree-d polynomial h with $h(1,\ldots,1) = 1$, and n shares $\gamma_i^{(1)}, \ldots, \gamma_i^{(n)} \in \mathcal{S}$:
1. Write h as $h = \sum_{\boldsymbol{u}\in[n]^d} c_{\boldsymbol{u}} X_{u_1} \cdots X_{u_d}$, where $c_{\boldsymbol{u}} \in \mathbb{F}_q$.
2. For each $j \in [n]$, parse $\gamma_i^{(j)}$ as $\gamma_i^{(j)} = (\eta_i^{(j)}, \xi_i^{(j)})$, where $\eta_i^{(j)}, \xi_i^{(j)} \in \mathcal{S}_0$.
3. Let $\xi_i^{(0)} = n^{-1} \sum_{j\in P} \xi_i^{(j)}$.
4. Let
$$\widetilde{\sigma_i} = (\sigma_{i1}, \sigma_{i2}, \sigma_{i3}) = \sum_{\boldsymbol{u}\in[n]^d} c_{\boldsymbol{u}} \mathsf{MULT}_0(i, \xi_i^{(0)}, \eta_i^{(u_1)}, \ldots, \eta_i^{(u_d)}) \in \mathbb{A}.$$
5. Output $\sigma_i = (\sigma_{i2}, \sigma_{i3}) \in \mathbb{F}_q(\beta_2) \times \mathbb{F}_q(\beta_3)$.

VER. Given $\zeta \in \mathbb{F}_q$ and $\sigma = (r, r') \in \mathbb{F}_q(\beta_2) \times \mathbb{F}_q(\beta_3)$, output 0 if and only if $\mathsf{D}(\zeta, r, r') = \perp$.

Fig. 6 A (δ, d)-VMSS scheme for an ℓ-partite adversary structure

$2(d+1)m/\min_{k\in[\ell]} |P_k|$, *then there exists a* Δ*-private,* (q^{-m}, d)*-verifiably multiplicative (with respect to the additive decoder), and* $\mathbb{F}_q$*-linear secret sharing scheme* Σ *with domain of secrets* $\mathbb{F}_q$*, domain of shares* $\mathbb{F}_q^{2N}$ *and domain of proofs* $\mathbb{F}_q^{2m}$.

Proof To simplify notations, we omit random strings used by sharing algorithms. From Proposition 7, we have a Δ-private secret sharing scheme $\Sigma_0 = (\mathbb{A}, \mathcal{R}_0, \mathcal{S}_0, \mathsf{SHARE}_0)$ that is $(d+1)$-multiplicative with respect to $\mathbb{A}$. Let $\mathsf{MULT}_0 : P \times \mathcal{S}_0^{d+1} \to \mathbb{A}$ be the map associated with the $(d+1)$-multiplicativity of Σ_0.

We construct a verifiably multiplicative scheme Σ based on Σ_0. The domain of secrets is $\mathbb{F}_q(\beta_1) = \mathbb{F}_q$. Let (E, D) be the δ-AMD code with $\mathcal{R} = \mathbb{F}_{q^m}$ and $\delta = q^{-m}$ in Proposition 2. Define SHARE, MULT, PROOF and VER for Σ as shown in Fig. 6. The domain of shares is $\mathcal{S}_0^2 = \mathbb{F}_q^{2N}$ and that of proofs is $\mathbb{F}_q(\beta_2) \times \mathbb{F}_q(\beta_3) \simeq \mathbb{F}_q^{2m}$. The Δ-privacy directly follows from that of Σ_0.

For $j \in [d]$, let $(\gamma_i^{(j)})_{i\in P}$ be a vector of shares for a secret $s^{(j)} \in \mathbb{F}_q(\beta_1)$. Then, $\eta_i^{(j)}$ obtained at Step 1 of MULT is a consistent share for $i \in P$ with a secret $\mathsf{E}(s^{(j)}, 1)$ (under Σ_0). The $(d+1)$-multiplicativity of Σ_0 implies that $(\widetilde{\zeta}_i)_{i\in P}$ is additive sharing of $\mathsf{E}(1,1) * \mathsf{E}(s^{(1)},1) * \cdots * \mathsf{E}(s^{(d)},1) = (s^{(1)} \cdots s^{(d)}, 1, s^{(1)} \cdots s^{(d)})$, where $*$ denotes the element-wise product. We therefore have that $(\zeta_i)_{i\in P}$ is additive sharing of $s^{(1)} \cdots s^{(d)}$, which shows the d-multiplicativity of Σ.

We see that Σ is (q^{-m}, d)-verifiably multiplicative in the following. Let $x^{(j)} \in \mathbb{F}_q$ be an input of a player $j \in P$ and $h = \sum_{\boldsymbol{u}\in[n]^d} c_{\boldsymbol{u}} X_{u_1} \cdots X_{u_d}$ be a degree-d polynomial with $h(1,\ldots,1) = 1$. Let $(\gamma_i^{(j)})_{i\in P} = (\eta_i^{(j)}, \xi_i^{(j)})_{i\in P}$ be a vector of shares for $x^{(j)}$. Let $r^{(j)} \in \mathbb{F}_q(\beta_2)$ be a random element sampled at Step 1 of $\mathsf{SHARE}(x^{(j)})$. It can be seen that $(\eta_i^{(j)})_{i\in P}$ and $(\xi_i^{(j)})_{i\in P}$ are vectors of shares for $\mathsf{E}(x^{(j)}, 1)$ and $\mathsf{E}(1, r^{(j)})$ under Σ_0, respectively. First, due to the linearity of Σ_0, $\xi_i^{(0)}$ at Step 3 of PROOF is a consistent share for $i \in P$ with a secret $n^{-1}\sum_{j\in P} \mathsf{E}(1, r^{(j)}) = \mathsf{SHARE}_0(\mathsf{E}(1, r^{(0)}))$, where $r^{(0)} = n^{-1}\sum_{j\in P} r^{(j)}$. The $(d+1)$-multiplicativity of Σ_0 implies that

$$\begin{aligned}\sum_{i\in P} \widetilde{\sigma}_i &= \sum_{\boldsymbol{u}\in[n]^d} c_{\boldsymbol{u}} \mathsf{E}(1, r^{(0)}) * \mathsf{E}(x^{(u_1)}, 1) * \cdots * \mathsf{E}(x^{(u_d)}, 1) \\ &= \mathsf{E}(1, r^{(0)}) * \mathsf{E}(h(x^{(1)}, \ldots, x^{(n)}), h(1, \ldots, 1)) \\ &= \mathsf{E}(h(x^{(1)}, \ldots, x^{(n)}), r^{(0)}).\end{aligned}$$

If we let σ_i be a proof outputted by $\mathsf{PROOF}(i, h, \gamma_i^{(1)}, \ldots, \gamma_i^{(n)})$, it holds that $\mathsf{VER}(h(x^{(1)}, \ldots, x^{(n)}), \sum_{i\in P} \sigma_i) = 1$, from which the correctness of PROOF and VER follows.

To see verifiability, consider the experiment $\mathrm{Exp}(x^{(1)}, \ldots, x^{(n)}, h, T, \mathsf{Adv})$ in Fig. 1 for an adversary Adv corrupting players in $T \in \Delta$. We obtain (ζ', σ') at Step 4 of the experiment and let $c = (\zeta', \sigma') - \mathsf{E}(h(x^{(1)}, \ldots, x^{(n)}), r^{(0)})$. Adv can choose c arbitrarily by modifying ζ'_i and σ'_i for $i \in T$. However, the probability that (ζ', σ') passes verification and $\zeta' \neq h(x^{(1)}, \ldots, x^{(n)})$ is at most $|\mathbb{F}_{q^m}|^{-1} = q^{-m}$. It follows from the verifiability of the AMD code (E, D) and the fact that $r^{(0)}$ is uniformly distributed over $\mathbb{F}_{q^m}$ even conditioned on Adv's view due to contribution by honest players. □

The proof size of the (δ, d)-VMSS scheme in Theorem 5 is $O(\log \delta^{-1})$, which can be smaller than the proof size $O(N \log n)$ of Theorem 4 depending on the number N of maximal points of Δ. A price to pay for the efficiency gain is that δ must be non-zero and Δ must satisfy the Q_{d+1} property with margin $\kappa > 0$.

In the case of monomials, we just let $\mathsf{SHARE}(s)$ output $\mathsf{SHARE}_0(\mathsf{E}(s, r))$ for $r \leftarrow\!\!\$\, \mathbb{F}_{q^m}^*$ instead of $(\mathsf{SHARE}_0(\mathsf{E}(s,1)), \mathsf{SHARE}_0(\mathsf{E}(1,r)))$, where $\mathbb{F}_{q^m}^*$ is the multiplicative group of $\mathbb{F}_{q^m}$. Let MULT and PROOF output additive shares of $\mathsf{E}(x^{(1)}, r^{(1)}) * \cdots * \mathsf{E}(x^{(d)}, r^{(d)})$ using MULT_0. Then, MULT_0 is only required to be d-multiplicative with respect to $\mathbb{A}$. Accordingly, we can weaken the condition on adversary structures and also cut down the share size.

Corollary 1 *Assume that Δ satisfies the Q_d property with margin κ and that $q > \max\{n, (2m+1)^{1/(m-1)}\}$. If $\kappa \geq 2dm/\min_{k\in[\ell]}|P_k|$, then there exists a Δ-private, $((q^m-1)^{-1}, d)$-verifiably multiplicative for the monomial $h = X_1 \cdots X_d$, and $\mathbb{F}_q$-linear secret sharing scheme Σ with domain of secrets $\mathbb{F}_q$, domain of shares $\mathbb{F}_q^N$, and domain of proofs $\mathbb{F}_q^{2m}$, where $N = |\max \Phi^{\Pi}(\Delta)|$.*

The authors in [25] propose a method to transform any d-MSS scheme into a (δ, d)-VMSS scheme for computing degree-d monomials for any $\delta > 0$. Specifically, a secret $s \in \mathbb{F}_q$ is encoded into $\mathsf{E}(s, r) \in \mathcal{C}$ for $r \leftarrow_{\$} \mathbb{F}_{q^m}^*$ using the AMD code in Proposition 2 and $\mathsf{E}(s, r)$ is shared among the players in parallel. Then, the scheme is (δ, d)-verifiably multiplicative with $\delta = (q^m - 1)^{-1}$. However, their transformation does not work for degree-d polynomials since $\mathsf{E}(s, r)+\mathsf{E}(s', r')$ is not a codeword of the AMD code in general. Moreover, the information ratio of the resulting scheme is $2m + 1 = O(\log_q \delta^{-1})$ times larger than the initial d-MSS scheme since $\mathcal{C} \simeq \mathbb{F}_q^{2m+1}$ as $\mathbb{F}_q$-linear spaces.

Example 3 To demonstrate the importance of Theorem 5, we show a parameter setting for the 2-partite adversary structure $\mathcal{U}_{\tau,\sigma}^{\Pi}$ in Example 1. Assume that $n = 1000$, $d = 2$, and $\delta = 2^{-60}$. Let q be the smallest prime such that $q > n$. We choose $m = 7$ to make the error probability less than δ. Then, we can choose $\kappa = 1/10 > 2(d+1)m/\min_{k\in[\ell]}|P_k|$. Our scheme in Theorem 5 can tolerate τ, σ satisfying $\tau + 2\sigma < (1-\kappa)/2 = 0.45$. In particular, it can tolerate a bounded number of subsets of at most $\tau n < 0.45n$ players. Since $N = 2$, a share consists of 4 field elements and a proof consists of 14 field elements. In the particular case of computing monomials, our scheme in Corollary 1 can compute degree-3 monomials with the same tolerable adversary structure. The share size is now $2\log q$ bits while the proof size is the same as above. However, if one applies the generic transformation [25] to the scheme in Theorem 1, the share size of the resulting scheme is $2(2m+1)\log q$ bits, which is $2m+1 = 15$ times larger than ours.

References

1. Barkol, O., Ishai, Y., Weinreb, E.: On d-multiplicative secret sharing. Journal of Cryptology **23**(4), 580–593 (2010)
2. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, pp. 1–10 (1988)
3. Blakley, G.R.: Safeguarding cryptographic keys. In: 1979 International Workshop on Managing Requirements Knowledge (MARK), pp. 313–318 (1979)
4. Cabello, S., Padró, C., Sáez, G.: Secret sharing schemes with detection of cheaters for a general access structure. Designs, Codes and Cryptography **25**(2), 175–188 (2002)
5. Cascudo, I., Cramer, R., Xing, C.: The arithmetic codex. In: 2012 IEEE Information Theory Workshop, pp. 75–79 (2012)
6. Chaum, D., Crépeau, C., Damgard, I.: Multiparty unconditionally secure protocols. In: Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, STOC '88, pp. 11–19 (1988)
7. Chen, H., Cramer, R.: Algebraic geometric secret sharing schemes and secure multiparty computations over small fields. In: Advances in Cryptology – CRYPTO 2006, pp. 521–536 (2006)

8. Chen, H., Cramer, R., de Haan, R., Pueyo, I.C.: Strongly multiplicative ramp schemes from high degree rational points on curves. In: Advances in Cryptology – EUROCRYPT 2008, pp. 451–470 (2008)
9. Cramer, R., Damgård, I., Maurer, U.: General secure multi-party computation from any linear secret-sharing scheme. In: Advances in Cryptology – EUROCRYPT 2000, pp. 316–334 (2000)
10. Cramer, R., Fehr, S., Padró, C.: Algebraic manipulation detection codes. Science China Mathematics **56**(7), 1349–1358 (2013)
11. Damgård, I., Nielsen, J.B.: Scalable and unconditionally secure multiparty computation. In: Advances in Cryptology – CRYPTO 2007, pp. 572–590 (2007)
12. Eriguchi, R., Kunihiro, N.: d-Multiplicative secret sharing for multipartite adversary structures. In: 1st Conference on Information-Theoretic Cryptography (ITC 2020), vol. 163, pp. 2:1–2:16 (2020)
13. Farràs, O., Martí-Farré, J., Padró, C.: Ideal multipartite secret sharing schemes. Journal of Cryptology **25**(3), 434–463 (2012)
14. Farràs, O., Padró, C.: Ideal secret sharing schemes for useful multipartite access structures. In: Coding and Cryptology, pp. 99–108 (2011)
15. Garcia, A., Stichtenoth, H.: On the asymptotic behaviour of some towers of function fields over finite fields. Journal of Number Theory **61**(2), 248 – 273 (1996)
16. Hirt, M., Maurer, U.: Complete characterization of adversaries tolerable in secure multi-party computation (extended abstract). In: Proceedings of the Sixteenth Annual ACM Symposium on Principles of Distributed Computing, PODC '97, pp. 25–34 (1997)
17. Hirt, M., Tschudi, D.: Efficient general-adversary multi-party computation. In: Advances in Cryptology – ASIACRYPT 2013, Part II, pp. 181–200 (2013)
18. Ito, M., Saito, A., Nishizeki, T.: Secret sharing scheme realizing general access structure. Electronics and Communications in Japan (Part III: Fundamental Electronic Science) **72**(9), 56–64 (1989)
19. Jacobson, N.: Basic algebra I. Courier Corporation (2012)
20. Käsper, E., Nikov, V., Nikova, S.: Strongly multiplicative hierarchical threshold secret sharing. In: International Conference on Information Theoretic Security, pp. 148–168 (2007)
21. Liu, M., Xiao, L., Zhang, Z.: Multiplicative linear secret sharing schemes based on connectivity of graphs. IEEE Transactions on Information Theory **53**(11), 3973–3978 (2007)
22. Maurer, U.: Secure multi-party computation made simple. Discrete Applied Mathematics **154**(2), 370–381 (2006)
23. Shamir, A.: How to share a secret. Communications of the ACM **22**(11), 612–613 (1979)
24. Stichtenoth, H.: Algebraic Function Fields and Codes. Springer-Verlag (2009)
25. Yoshida, M., Obana, S.: Verifiably multiplicative secret sharing. IEEE Transactions on Information Theory **65**(5), 3233–3245 (2019)