d-Multiplicative Secret Sharing for Multipartite Adversary Structures

Reo Eriguchi
Graduate School of Information Science and Technology, The University of Tokyo, Japan
reo-eriguchi@g.ecc.u-tokyo.ac.jp

Noboru Kunihiro
Department of Computer Science, University of Tsukuba, Japan
kunihiro@cs.tsukuba.ac.jp

Abstract

Secret sharing schemes are said to be d-multiplicative if the i-th shares of any d secrets $s^{(j)}$, $j \in [d]$ can be converted into an additive share of the product $\prod_{j\in[d]} s^{(j)}$. d-Multiplicative secret sharing is a central building block of multiparty computation protocols with minimum number of rounds which are unconditionally secure against possibly non-threshold adversaries. It is known that d-multiplicative secret sharing is possible if and only if no d forbidden subsets covers the set of all the n players or, equivalently, it is private with respect to an adversary structure of type Q_d. However, the only known method to achieve d-multiplicativity for any adversary structure of type Q_d is based on CNF secret sharing schemes, which are not efficient in general in that the information ratios are exponential in n.

In this paper, we explicitly construct a d-multiplicative secret sharing scheme for any ℓ-partite adversary structure of type Q_d whose information ratio is $O(n^{\ell+1})$. Our schemes are applicable to the class of all the ℓ-partite adversary structures, which is much wider than that of the threshold ones. Furthermore, our schemes achieve information ratios which are polynomial in n if ℓ is constant and hence are more efficient than CNF schemes. In addition, based on the standard embedding of ℓ-partite adversary structures into $\mathbb{R}^\ell$, we introduce a class of ℓ-partite adversary structures of type Q_d with good geometric properties and show that there exist more efficient d-multiplicative secret sharing schemes for adversary structures in that family than the above general construction. The family of adversary structures is a natural generalization of that of the threshold ones and includes some adversary structures which arise in real-world scenarios.

2012 ACM Subject Classification Security and privacy → Information-theoretic techniques

Keywords and phrases Secret sharing scheme, multiplicative secret sharing scheme, multipartite adversary structure

Digital Object Identifier 10.4230/LIPIcs.ITC.2020.2

Funding This research was partially supported by JST CREST Grant Number JPMJCR14D6, Japan and JSPS KAKENHI Grant Number JP19K22838.

1 Introduction

Secret sharing is a cryptographic technique introduced in [4, 20] to protect a secret from leakage by dividing it into several shares and distributing them to n players. Let P be the set of the n players. A subset of players is called *forbidden* if it reveals no information on the secret and *authorized* if it determines the secret. In this paper, we only consider *perfect* secret sharing, in which each subset is either forbidden or authorized. For a family of subsets of players $\Delta \subseteq 2^P$, we say that a secret sharing scheme is Δ-*private* if any subset in Δ is forbidden. The efficiency of a secret sharing scheme is measured by the (total) *information ratio*, which is defined as the ratio of the total size of shares to that of a secret.

In addition to its direct application to distributed storage of secret data, secret sharing is a central buiding block of unconditionally secure multiparty computation protocols. Secure *multiparty computation* (MPC) is an important problem in cryptography, in which several players jointly compute an agreed function over their inputs without revealing no information on them to an adversary. More precisely, we assume that there are m clients holding their secret inputs $x_j \in \mathbb{F}$, $j \in [m] := \{1, 2, \ldots, m\}$ represented as elements in some finite field $\mathbb{F}$ and n servers who help the computation of the function. Furthermore, a (passive) adversary corrupts a subset of servers and learns the entire internal information of the corrupted servers. We identify the set of servers with P and let $\Delta \subseteq 2^P$ denote the family of all subsets of servers which the adversary can corrupt, which we call the *adversary structure*.

Barkol et al. [1] show that it is possible to construct a protocol with two rounds of interaction, which is the minimum number of rounds, to securely evaluate a multivariate polynomial of total degree at most d if there exists a Δ-private secret sharing scheme satisfying an additional property called *d-multiplicativity*. A secret sharing scheme is said to be *d-multiplicative* if the i-th shares of any d secrets $s^{(j)}$, $j \in [d]$ can be converted into an element c_i such that the sum $\sum_{i\in[n]} c_i$ is equal to the product $\prod_{j\in[d]} s^{(j)}$. Note that the dominant term of the communication complexity in the protocol is $m\sigma \log |\mathbb{F}|$, where m is the number of clients and σ is the information ratio of the underlying secret sharing scheme.

Barkol et al. [1] also characterize the existence of d-multiplicative secret sharing schemes: Δ-private d-multiplicative secret sharing is possible if and only if Δ is of *type* Q_d. An adversary structure Δ is called a *Q_d-adversary structure* if $A_1 \cup \cdots \cup A_d \neq P$ for any $A_1, \ldots, A_d \in \Delta$.

In particular, if we focus on the adversary who can corrupt any subset of k servers, i.e., $\Delta = \mathcal{T}_k^n := \{A \subseteq P : |A| \leq k\}$, then $\mathcal{T}_k^n$-private d-multiplicative secret sharing is possible if and only if $n > dk$. The "if" part follows from the (k, n)-*Shamir secret sharing scheme* [20], which is based on Lagrange interpolation for some polynomial over any finite field $\mathbb{F}$ with $|\mathbb{F}| > n$. It is known that Shamir's scheme achieves the optimal information ratio [16]. On the other hand, since it costs a lot to control a single server, the number of servers n should be as small as possible. The above characterization implies that we must consider non-threshold Q_d-adversary structures to design d-multiplicative secret sharing among $n \leq dk$ players.

For any (possibly non-threshold) adversary structure Δ of type Q_d, the *CNF secret sharing scheme* [15] for Δ is known to be d-multiplicative. However, the CNF scheme is inefficient in general since its information ratio is $\sum_{i\in P} |\Delta_i^+|$, which is exponential in n in the worst case. Here, Δ_i^+ denotes the set of all the maximal subsets in Δ not containing the player $i \in P$. This large information ratio of the CNF scheme leads to a large amount of communication when the scheme is used in the protocol. Therefore, it is important to devise a method to construct efficient d-multiplicative secret sharing schemes for non-threshold Q_d-adversary structures.

Besides Shamir's scheme and CNF schemes, several multiplicative secret sharing schemes have been proposed. The notion of an *arithmetic codex* is introduced in [7]. Arithmetic codices are defined as linear codes with some multiplicative property and can be used as d-multiplicative secret sharing schemes. In particular, arithmetic codices based on algebraic geometric codes [8] are important. Let d and k be any positive integers and assume that C is an algebraic curve of genus $g(C)$ defined over $\mathbb{F}$. If $dk + 2dg(C) < n < |C(\mathbb{F})|$, then there exists a $\mathcal{T}_k^n$-private d-multiplicative secret sharing scheme over $\mathbb{F}$. Here, $C(\mathbb{F})$ is the set of all $\mathbb{F}$-rational places on C. Although we need additional $2dg(C)$ players, the condition $|C(\mathbb{F})| > n$ is weaker than $|\mathbb{F}| > n$.

2-Multiplicative secret sharing schemes have received a lot of attention. For general adversary structures, one of the most significant results is that any linear secret sharing scheme for a Q_2-adversary structure can be converted into a 2-multiplicative scheme for the same adversary structure [9]. Since the information ratio of the resulting scheme is twice that of the initial scheme, it achieves $2\lambda_{\mathbb{F}}(\Delta)$, where $\lambda_{\mathbb{F}}(\Delta)$ is the minimum information ratio of Δ-private linear secret sharing schemes. In [17, 18], more efficient 2-multiplicative schemes are proposed for specific classes of Q_2-adversary structures.

1.1 Our Results

In this paper, we focus on multipartite adversary structures. The class of *multipartite adversary structures* has been well studied because they correspond to many realistic situations and can be described in a compact way. Please refer to [12] for a comprehensive survey of multipartite adversary structures. For a partition $\Pi = (P_1, \ldots, P_\ell)$ of P, Π-partite adversary structures are defined as the ones in which each player is classified into some part P_j and all players in the same part play an equivalent role. There is a useful geometric representation [11]: any Π-partite adversary structure can be embedded in $\mathbb{R}^\ell$ via the map $\Phi^\Pi : 2^P \to \mathbb{R}^\ell$, $\Phi^\Pi(X) = (|X \cap P_1|, \ldots, |X \cap P_\ell|)$. In particular, a Π-partite adversary structure Δ is uniquely determined by $\max \Phi^\Pi(\Delta)$, where $\max \Phi^\Pi(\Delta)$ is the set of all maximal elements in $\Phi^\Pi(\Delta)$ with respect to the coordinatewise order on $\mathbb{R}^\ell$.

The main contribution of this paper is twofold. First, for any ℓ-partite adversary structure Δ of type Q_d, we explicitly construct a Δ-private d-multiplicative secret sharing scheme whose information ratio is $n|\max \Phi^\Pi(\Delta)| = O(n^{\ell+1})$ (Theorem 4). The scheme can be defined over any finite field $\mathbb{F}$ with $|\mathbb{F}| > n$. It is obtained by a simple application of well-known decomposition techniques [21]. However, to our best knowledge, this is the first time to prove that the scheme satisfies d-multiplicativity if Δ is of type Q_d. As a result, we obtain d-multiplicative schemes for the class of all the ℓ-partite adversary structures of type Q_d, which is much wider than that of the threshold ones. Furthermore, our schemes achieve information ratios which are polynomial in n if ℓ is constant and hence are more efficient than CNF schemes.

Second, we show that there exists a more efficient Δ-private d-multiplicative secret sharing scheme than the scheme from the above general construction if $\Phi^\Pi(\Delta)$ has some good geometric property (Theorem 9). Specifically, let $C = \mathrm{Conv}(\Phi^\Pi(\Delta))$ be the convex hull of $\Phi^\Pi(\Delta)$ in $\mathbb{R}^\ell$ and set $\boldsymbol{p} = (1/d)\Phi^\Pi(P)$. Assume that $\boldsymbol{p} \notin C$. If $\mathrm{dist}(\boldsymbol{p}, C)$, the distance between $\boldsymbol{p}$ and C, is at least $\epsilon > 0$, then Δ is of type Q_d and it is possible to construct a Δ-private d-multiplicative scheme whose information ratio is at most $O(\ell n^2/\epsilon)$ over a finite field $\mathbb{F}$ with $|\mathbb{F}| = \Omega(\ell n^2/\epsilon)$. For example, if ϵ is a constant independent of n, then the information ratio is smaller than that of the above general construction.

The information ratio of our scheme depends only on the distance between the point $\boldsymbol{p}$ and the convex hull of $\Phi^\Pi(\Delta)$. In other words, our scheme provides the same upper bound on the minimum information ratio of Δ-private secret sharing schemes regardless of how the adversary structure Δ is represented. We demonstrate an example of adversary structures (Example 11) for which an upper bound obtained by a naive approach based on weighted threshold secret sharing would grow infinitely depending on the description of Δ.

Our construction for such Δ is a natural generalization of Shamir's scheme. Indeed, when $\Delta = \mathcal{T}_k^n$, the condition $\boldsymbol{p} \notin C$ holds if and only if $n > dk$ and then our scheme is the same as the (k, n)-Shamir secret sharing scheme.

Table 1 Comparison amongst existing d-multiplicative secret sharing schemes. The symbol "$d = *$" denotes any value of d.

Scheme	d	Adversary structure	Information ratio	Assumption on $\mathbb{F}$
Shamir [20]	$*$	$\mathcal{T}_k^n$ with $n > dk$	n	$\lvert\mathbb{F}\rvert > n$
Chen and Cramer [8]	$*$	$\mathcal{T}_k^n$ with $n > dk + 2dg(C)$	n	$\lvert C(\mathbb{F})\rvert > n$
CNF [15]	$*$	Δ of type Q_d	$\sum_{i\in P} \lvert\Delta_i^+\rvert$	–
Cramer et al. [9]	2	Δ of type Q_2	$2\lambda_{\mathbb{F}}(\Delta)$	–
Theorem 4	$*$	ℓ-partite Δ of type Q_d	$n\lvert\max \Phi^{\Pi}(\Delta)\rvert$	$\lvert\mathbb{F}\rvert > n$
Theorem 9	$*$	ℓ-partite Δ such that $\operatorname{dist}(\boldsymbol{p}, \operatorname{Conv}(\Phi^{\Pi}(\Delta))) \geq \epsilon$	$O(\ell n^2/\epsilon)$	$\lvert\mathbb{F}\rvert = \Omega(\ell n^2/\epsilon)$

1.2 Our Techniques

Let $\Pi = (P_1, \ldots, P_\ell)$ be a partition of P and Δ be any Π-partite adversary structure of type Q_d. First, we explain a high-level idea of our proposed construction of a Δ-private d-multiplicative secret sharing scheme using decomposition techniques [21].

Write $\max \Phi^{\Pi}(\Delta) = \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N\}$ and $\boldsymbol{a}_j = (\boldsymbol{a}_j(1), \ldots, \boldsymbol{a}_j(\ell))$. For each $j \in [N]$, define Δ_j as the Π-partite adversary structure such that $\Phi^{\Pi}(\Delta_j) = \{\boldsymbol{x} \in \Phi^{\Pi}(2^P) : \boldsymbol{x} \preceq \boldsymbol{a}_j\}$, where $\preceq$ is the coordinatewise order on $\mathbb{R}^\ell$. Then we can decompose Δ into N adversary structures $\Delta_1, \ldots, \Delta_N$ as $\Delta = \bigcup_{j\in[N]} \Delta_j$.

We construct a Δ-private scheme Σ as follows. Let $\mathbb{F}$ be a finite field with $\lvert\mathbb{F}\rvert > n$ and fix n distinct nonzero elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$. Let $s \in \mathbb{F}$ be a secret to be shared. We randomly split s into $s_1, \ldots, s_N$, i.e., $s = s_1 + \cdots + s_N$. For each $j \in [N]$ and $i \in [\ell]$, we run the $(\boldsymbol{a}_j(i), \lvert P_i\rvert)$-Shamir secret sharing scheme with secret s_j in parallel. In other words, we assign to each player $k \in P_i$ the evaluation of some polynomial f_{ij} with $f_{ij}(0) = s_j$ of degree at most $\boldsymbol{a}_j(i)$ at the point α_k. Then the player $k \in P_i$ receives N field elements $\{s_{i,j,k} := f_{ij}(\alpha_k) : j \in [N]\}$. As for privacy, if $A \in \Delta$, then $\Phi^{\Pi}(A) \preceq \boldsymbol{a}_j$ for some $j \in [N]$ and the players in A cannot obtain any information about s_j and hence the secret s. Since each player receives N field elements for a secret $s \in \mathbb{F}$, the information ratio of Σ is nN.

To prove the scheme Σ is d-multiplicative, let $s^{(1)}, \ldots, s^{(d)}$ be d secrets. Since we split $s^{(m)}$ into $s_1^{(m)}, \ldots, s_N^{(m)}$, the product $s^{(1)} \cdots s^{(d)}$ can be represented as the sum of N^d monomials $\{s_{j_1}^{(1)} \cdots s_{j_d}^{(d)} : j_1 \in [N], \ldots, j_d \in [N]\}$. It follows from Δ being of type Q_d that, for any tuple $(j_1, \ldots, j_d)$, there exists an index $i \in [\ell]$ such that $\boldsymbol{a}_{j_1}(i) + \cdots + \boldsymbol{a}_{j_d}(i) < \lvert P_i\rvert$. Let $(j_1, \ldots, j_d)$ be any tuple and i be such an index. From the definition of the $(\boldsymbol{a}_{j_m}(i), \lvert P_i\rvert)$-Shamir secret sharing scheme, it can be observed that $s_{j_m}^{(m)}$ is the evaluation of some polynomial of degree at most $\boldsymbol{a}_{j_m}(i)$ at the point 0. Then the monomial $s_{j_1}^{(1)} \cdots s_{j_d}^{(d)}$ is the evaluation of some polynomial f of degree at most $\boldsymbol{a}_{j_1}(i) + \cdots + \boldsymbol{a}_{j_d}(i)$ at the point 0. Each player k in P_i can obtain the evaluation of f at the point α_k by multiplying their shares $s_{i,j_1,k}^{(1)}, \ldots, s_{i,j_d,k}^{(d)}$. Since there are more than $\boldsymbol{a}_{j_m}(i) + \cdots + \boldsymbol{a}_{j_d}(i)$ players in P_i, the monomial $s_{j_1}^{(1)} \cdots s_{j_d}^{(d)}$ can be obtained from their shares by Lagrange interpolation. Finally, the product $s^{(1)} \cdots s^{(d)}$ can be obtained by doing this process for all the N^d tuple $(j_1, \ldots, j_d)$.

Next, let Δ be a Π-partite adversary structure with $\operatorname{dist}(\boldsymbol{p}, C) \geq \epsilon > 0$, where $\boldsymbol{p} = (1/d)\Phi^{\Pi}(P)$ and $C = \operatorname{Conv}(\Phi^{\Pi}(\Delta))$. We explain how to prove the existence of a Δ-private d-multiplicative secret sharing scheme whose information ratio is $O(\ell n^2/\epsilon)$. Roughly speaking, we show that Δ is contained by some weighted threshold adversary structure. For a vector

of non-negative integers $\boldsymbol{w}$ and a non-negative integer t, the *weighted threshold adversary structure* $\mathcal{W}^{\Pi}_{\boldsymbol{w},t}$ is defined as the Π-partite adversary structure such that $\Phi^{\Pi}(\mathcal{W}^{\Pi}_{\boldsymbol{w},t}) = \{\boldsymbol{x} \in \Phi^{\Pi}(2^P) : \boldsymbol{w} \cdot \boldsymbol{x} \leq t\}$, where $\boldsymbol{w} \cdot \boldsymbol{x}$ is the standard inner product in $\mathbb{R}^{\ell}$. If $\boldsymbol{w} \cdot \Phi^{\Pi}(P) > dt$, it is possible to construct a $\mathcal{W}^{\Pi}_{\boldsymbol{w},t}$-private d-multiplicative scheme whose information ratio is $\boldsymbol{w} \cdot \Phi^{\Pi}(P)$ by assigning multiple shares of Shamir's scheme to each player [20].

More precisely, let $\boldsymbol{c}^*$ be the closest point in C to $\boldsymbol{p}$ and $\boldsymbol{h}$ be the unit vector which is parallel to $\boldsymbol{p} - \boldsymbol{c}^*$. Then it can be verified that $\boldsymbol{h} \cdot (\boldsymbol{x} - \boldsymbol{p}) \leq -\epsilon$ for any $\boldsymbol{x} \in \Phi^{\Pi}(\Delta)$. Although $\boldsymbol{h}$ is not necessarily a non-negative integer vector, we can approximate it by a vector $\boldsymbol{h}'$ such that all the entries are rational numbers with common denominator $q = O(\ell n/\epsilon)$ and $\boldsymbol{h}' \cdot (\boldsymbol{x} - \boldsymbol{p}) < 0$ for any $\boldsymbol{x} \in \Phi^{\Pi}(\Delta)$. By setting $\boldsymbol{w} = q\boldsymbol{h}'$ and $t = \max_{\boldsymbol{x} \in \Phi^{\Pi}(\Delta)}\{\boldsymbol{w} \cdot \boldsymbol{x}\}$, we have that $\Delta \subseteq \mathcal{W}^{\Pi}_{\boldsymbol{w},t}$. Since $dt < \boldsymbol{w} \cdot \Phi^{\Pi}(P)$ and each entry of $\boldsymbol{w}$ can be upper bounded by $q = O(\ell n/\epsilon)$, we obtain a Δ-private d-multiplicative scheme Σ with information ratio $O(\ell n^2/\epsilon)$.

1.3 Related Work

There is another kind of MPC protocols based on secret sharing, in which the function to be computed is represented as an arithmetic circuit and servers interactively evaluate it gate by gate. In the threshold setting, the protocol in [3] is classically known and a more efficient protocol is proposed in [10]. For a non-threshold adversary, Cramer et al. [9] construct an MPC protocol based on 2-multiplicative secret sharing schemes and Maurer [19] and Hirt and Tschudi [14] construct protocols based on CNF secret sharing schemes. Their protocols are secure against an adversary whose adversary structure is of type Q_2 (or Q_3 in the setting with perfect active security) and hence they are more flexible than that of [1]. However, the servers need to interact with each other whenever they evaluate a multiplication gate.

d-Multiplicative secret sharing can also be defined in the context of *homomorphic secret sharing*. Recently, several homomorphic secret sharing schemes have been proposed in the literature (e.g. [5, 6]). However, the security of the schemes relies on some computational assumptions.

1.4 Notations

Let $\mathbb{Z}_+$ and $\mathbb{R}_+$ denote the set of all non-negative integers and the set of all non-negative real numbers, respectively. Define $[\ell] = \{1, \ldots, \ell\}$ for $\ell \in \mathbb{N}$. Let $P = \{p_1, \ldots, p_n\}$ be the set of n players. The power set of a set X is denoted by 2^X and X^m is the Cartesian product of m copies of X. Let $\mathbb{F}$ be any field. The vector $\mathbf{1} \in \mathbb{F}^m$ is the vector whose entries are all one and $\boldsymbol{e}_i \in \mathbb{F}^m$ 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 $\boldsymbol{v} \preceq \boldsymbol{w}$ if $\boldsymbol{v}(i) \leq \boldsymbol{w}(i)$ for any $i \in [m]$ and $\boldsymbol{v} \prec \boldsymbol{w}$ if $\boldsymbol{v} \preceq \boldsymbol{w}$ 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: $\|\boldsymbol{v}\| = \sqrt{\boldsymbol{v} \cdot \boldsymbol{v}}$. For two closed subsets C_1 and C_2 in $\mathbb{R}^m$, the distance between C_1 and C_2 is defined by $\mathrm{dist}(C_1, C_2) = \min\{\|\boldsymbol{c}_1 - \boldsymbol{c}_2\| : \boldsymbol{c}_1 \in C_1, \boldsymbol{c}_2 \in C_2\}$.

2 Preliminaries

2.1 Adversary Structures

A family Δ of subsets of P is *monotone decreasing* if $A \in \Delta$ and $A \supseteq B$ implies $B \in \Delta$ for any $A, B \subseteq P$. We call a monotone decreasing family of subsets of P an *adversary structure* on P.

Let Δ be an adversary structure on P and $d \geq 2$. We say that Δ is of *type* Q_d 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 the most well-known adversary structure, which is defined by $\mathcal{T}_k^n = \{A \subseteq P : |A| \leq k\}$. It can be seen that $\mathcal{T}_k^n$ is of type 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 any $j \in [\ell]$. An adversary structure Δ is called Π-*partite* if $\tau(B) \in \Delta$ for any $B \in \Delta$ and any Π-permutation τ. There is a useful geometric representation of Π-partite adversary structures. Let $\Phi^\Pi : 2^P \to \mathbb{R}^\ell$ be a map defined by $\Phi^\Pi(X) = (|X \cap P_j|)_{j \in [\ell]}$. The image of Φ^Π is the set of all integer points in the hyperrectangle determined by $\mathbf{0}$ and $\Phi^\Pi(P)$, that is, $\Phi^\Pi(2^P) = \{\boldsymbol{x} \in \mathbb{Z}^\ell : \mathbf{0} \preceq \boldsymbol{x} \preceq \Phi^\Pi(P)\}$. It follows that a Π-partite adversary structure Δ is uniquely determined by $\Phi^\Pi(\Delta)$. Note that, if $\boldsymbol{a} \in \Phi^\Pi(\Delta)$ and $\boldsymbol{a} \succeq \boldsymbol{b}$, then $\boldsymbol{b} \in \Phi^\Pi(\Delta)$ for any $\boldsymbol{a}, \boldsymbol{b} \in \Phi^\Pi(2^P)$. Thus, any Π-partite adversary structure Δ is uniquely determined only by specifying $\max \Phi^\Pi(\Delta)$, where

$$\max \Phi^\Pi(\Delta) := \{\boldsymbol{a} \in \Phi^\Pi(\Delta) : \boldsymbol{a} \prec \boldsymbol{b} \preceq \Phi^\Pi(P) \Rightarrow \boldsymbol{b} \notin \Phi^\Pi(\Delta)\}.$$

2.2 Secure Polynomial Evaluation Based on d-Multiplicative Secret Sharing

We provide the definition of d-multiplicative secret sharing and an MPC protocol proposed in [1] to securely evaluate a multivariate polynomial.

A *secret sharing scheme* [2] is a tuple $\Sigma = (\mathcal{K}, \mathcal{R}, \mathcal{S}, \varphi)$, where $\mathcal{K}$ is a domain of secrets, $\mathcal{R}$ is a set of random strings, $\mathcal{S}$ is a domain of shares, and $\varphi : \mathcal{K} \times \mathcal{R} \to \mathcal{S}^n$ is a map. For $A \subseteq P$, $\varphi(s, r)_A$ denotes the restriction of $\varphi(s, r)$ to the entries indexed by A. For each $i \in P$, we define $\mathcal{S}_i \subseteq \mathcal{S}$ as $\mathcal{S}_i = \{\varphi(s, r)_{\{i\}} : s \in \mathcal{K}, r \in \mathcal{R}\}$. The (total) *information ratio* $\sigma(\Sigma)$ is defined as $\sigma(\Sigma) = \sum_{i \in P} \log |\mathcal{S}_i| / \log |\mathcal{K}|$.

We say that a secret sharing scheme $\Sigma = (\mathcal{K}, \mathcal{R}, \mathcal{S}, \varphi)$ is *private with respect to* an adversary structure Δ on P or Δ-private for short if, for any $A \in \Delta$, any two secrets $s, t \in \mathcal{K}$, and any possible tuple of shares $(x_i)_{i \in A}$, it holds that

$$\Pr[\varphi(s, r)_A = (x_i)_{i \in A}] = \Pr[\varphi(t, r)_A = (x_i)_{i \in A}],$$

where the probabilities are taken over the random choice of $r \in \mathcal{R}$. In other words, the players in $A \in \Delta$ cannot obtain any information about a secret. Clearly, if Σ is Δ_1-private and $\Delta_1 \supseteq \Delta_2$, then Σ is also Δ_2-private.

Suppose that $\mathcal{K}$ is a finite field $\mathbb{F}$. For $d \geq 2$, a secret sharing scheme Σ is said to be d-*multiplicative* if there exists a map $\mathrm{MULT} : P \times \mathcal{S}^d \to \mathbb{F}$ such that

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

for any d secrets $s^{(1)}, \ldots, s^{(d)} \in \mathbb{F}$ and any d random strings $r^{(1)}, \ldots, r^{(d)} \in \mathcal{R}$, where $(s_i^{(j)})_{i \in P} = \varphi(s^{(j)}, r^{(j)})$ is a vector of shares for $s^{(j)}$. Furthermore, we say that a secret sharing scheme Σ is *linear* over $\mathbb{F}$ or $\mathbb{F}$-linear if $\mathcal{S}$ and $\mathcal{R}$ are vector spaces over $\mathcal{K} = \mathbb{F}$ and φ is a linear map over $\mathbb{F}$.

The most important application of d-multiplicative secret sharing is a construction of unconditionally secure MPC protocols to evaluate multivariate polynomials of total degree at most d.

Suppose that m clients C_j have secret inputs $x^{(j)} \in \mathbb{F}$ and want to evaluate a multivariate polynomial $f \in \mathbb{F}[X_1, \ldots, X_m]$ of total degree at most d. Furthermore, suppose that there are n servers indexed by P which help perform the computation. Let $\Sigma = (\mathcal{K} = \mathbb{F}, \mathcal{R}, \mathcal{S}, \varphi)$

be a d-multiplicative secret sharing scheme. Barkol et al. [1] construct an MPC protocol to obtain $f(x^{(1)}, \ldots, x^{(m)})$ by using Σ. For simplicity, we explain the protocol in the case of $m = d$ and $f = X_1 \ldots X_d$. Please refer to [1] for a general case.

- Round 1: Each client C_j generates shares $(s_i^{(j)})_{i \in P} = \varphi(x^{(j)}, r^{(j)})$ corresponding to his input $x^{(j)}$ and sends $s_i^{(j)} \in \mathcal{S}_i \subseteq \mathcal{S}$ to the server $i \in P$. In addition, C_j randomly chooses n field elements $z_i^{(j)}$, $i \in P$ conditioned on $\sum_{i \in P} z_i^{(j)} = 0$ and sends $z_i^{(j)} \in \mathbb{F}$ to the server $i \in P$.
- Round 2: Each server $i \in P$ computes $y_i = \mathrm{MULT}(i, s_i^{(1)}, \ldots, s_i^{(d)}) + \sum_{j \in [d]} z_i^{(j)}$ and sends $y_i \in \mathbb{F}$ to all clients.
- Output: Each client C_j computes $\sum_{i \in P} y_i$, which is equal to $\prod_{j \in [d]} x^{(j)}$.

Since the n servers can locally convert their shares into additive shares of the output, interaction is required only in Round 1 and the latter half of Round 2. The communication complexity of the protocol is

$$\sum_{j \in [m]} \sum_{i \in P} (\log |\mathcal{S}_i| + \log |\mathbb{F}|) + \sum_{i \in P} \sum_{j \in [m]} \log |\mathbb{F}| = m(\sigma(\Sigma) + 2n) \log |\mathbb{F}|.$$

Therefore, it is important to cut down the information ratio and the size of the base field to design a communication-efficient MPC protocol.

Let $\Delta \subseteq 2^P$ be a family of subsets of the n servers. We assume a passive adversary who can corrupt a set of servers A such that $A \in \Delta$. If the underlying secret sharing scheme Σ is Δ-private, then the adversary cannot learn anything about the inputs of the clients other than what follows from the output.

2.3 Examples of d-Multiplicative Secret Sharing Schemes

2.3.1 Shamir Secret Sharing Schemes

The (k, n)-*Shamir secret sharing scheme* [20] is a well-known $\mathcal{T}_k^n$-private linear secret sharing scheme. Let $\mathbb{F}$ be a finite field such that $|\mathbb{F}| > n$ and take n distinct nonzero elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$. Let $s \in \mathbb{F}$ be a secret to be shared. First, choose a random polynomial f over $\mathbb{F}$ of degree at most k conditioned on $f(0) = s$. Second, assign $f(\alpha_i)$ to $i \in P$ as a share. Note that the (k, n)-Shamir secret sharing scheme has the information ratio n, which is known to be optimal [16].

It can be seen that the scheme is d-multplicative if $n > dk$. Indeed, let $s^{(1)}, \ldots, s^{(d)}$ be d secrets and $f^{(1)}, \ldots, f^{(d)}$ be the corresponding d polynomials over $\mathbb{F}$ of degree at most k which are used to share $s^{(1)}, \ldots, s^{(d)}$, respectively. Since the degree of $g := \prod_{j \in [d]} f^{(j)}$ is at most $dk < n$, we can compute the product of the secrets from the shares $f^{(j)}(\alpha_i)$, $i \in \widetilde{P}$ for any subset $\widetilde{P} \subseteq P$ of size dk by Lagrange interpolation:

$$\prod_{j \in [d]} s^{(j)} = g(0) = \sum_{i \in \widetilde{P}} \lambda_i^{\widetilde{P}} g(\alpha_i) = \sum_{i \in \widetilde{P}} \lambda_i^{\widetilde{P}} \prod_{j \in [d]} f^{(j)}(\alpha_i),$$

where $\lambda_i^{\widetilde{P}}$ is a Lagrange coefficient, i.e., $\lambda_i^{\widetilde{P}} = \prod_{m \in \widetilde{P} \setminus \{i\}} \alpha_m / (\alpha_m - \alpha_i)$.

2.3.2 Weighted Threshold Secret Sharing Schemes

Weighted threshold adversary structures proposed in [20] are natural generalizations of the threshold ones to the multipartite setting. Let $\Pi = (P_1, \ldots, P_\ell)$ be a partition of P, $\boldsymbol{w} \in \mathbb{Z}_+^\ell$, and $t \in \mathbb{Z}_+$. Define $\mathcal{W}_{\boldsymbol{w},t}^{\Pi}$ as the Π-partite adversary structure such that

$$\Phi^{\Pi}(\mathcal{W}_{\boldsymbol{w},t}^{\Pi}) = \{\boldsymbol{x} \in \Phi^{\Pi}(2^P) : \boldsymbol{w} \cdot \boldsymbol{x} \leq t\}.$$

Note that, if $\boldsymbol{w} = \mathbf{1} \in \mathbb{Z}_+^\ell$, then $\mathcal{W}_{\mathbf{1},t}^\Pi$ is equal to $\mathcal{T}_t^n$.

It is possible to construct $\mathcal{W}_{\boldsymbol{w},t}^\Pi$-private linear secret sharing schemes by assigning multiple shares of Shamir's scheme to each player [20]. Let $\mathbb{F}$ be a finite field such that $|\mathbb{F}| > N := \boldsymbol{w} \cdot \Phi^\Pi(P)$ and take N distinct nonzero elements $\alpha_{ijk} \in \mathbb{F}$ for $i \in [\ell]$, $j \in P_i$ and $k \in [\boldsymbol{w}(i)]$. Let $s \in \mathbb{F}$ be a secret to be shared. First, choose a random polynomial f over $\mathbb{F}$ of degree at most t with $f(0) = s$. Second, assign $\boldsymbol{w}(i)$ shares $(f(\alpha_{ijk}))_{k \in [\boldsymbol{w}(i)]}$ to the player $j \in P$, where i is the unique index such that $j \in P_i$. Note that the information ratio of the scheme is $N = \boldsymbol{w} \cdot \Phi^\Pi(P)$. It can be shown that the scheme is d-multiplicative if $N > dt$ in the same manner as Shamir's scheme. In summary, the following proposition holds.

▶ **Proposition 1** ([20]). *Let $\Pi = (P_1, \dots, P_\ell)$ be a partition of P and $\mathcal{W}_{\boldsymbol{w},t}^\Pi$ be the Π-partite weighted threshold adversary structure with weight $\boldsymbol{w} \in \mathbb{Z}_+^\ell$ and threshold $t \in \mathbb{Z}_+$. Let $\mathbb{F}$ be a finite field such that $|\mathbb{F}| > \boldsymbol{w} \cdot \Phi^\Pi(P)$. Then there exists a $\mathcal{W}_{\boldsymbol{w},t}^\Pi$-private $\mathbb{F}$-linear secret sharing scheme Σ with information ratio $\sigma(\Sigma) = \boldsymbol{w} \cdot \Phi^\Pi(P)$. Furthermore, if $\boldsymbol{w} \cdot \Phi^\Pi(P) > dt$, then Σ is d-multiplicative.*

2.3.3 CNF Secret Sharing Schemes

For any adversary structure Δ of type Q_d, it is possible to construct a Δ-private d-multiplicative secret sharing scheme [15]. Let Δ^+ be the set of all maximal subsets in Δ. Let s be a secret to be shared. First, choose $|\Delta^+|$ random field elements r_A, $A \in \Delta^+$ such that $s = \sum_{A \in \Delta^+} r_A$. Second, assign $(r_A)_{A \in \Delta_i^+}$ to each $i \in P$, where $\Delta_i^+ = \{A \in \Delta^+ : i \notin A\}$. The information ratio of the scheme is $\sum_{i \in P} |\Delta_i^+|$. It can be seen that the scheme is d-multiplicative as long as Δ is of type Q_d.

3 d-Multiplicative Secret Sharing for Any Multipartite Q_d-Adversary Structure

In this section, we propose an explicit construction of a Δ-private d-multiplicative secret sharing scheme for any ℓ-partite adversary structure Δ of type Q_d. Our scheme achieves an information ratio $n|\max \Phi^\Pi(\Delta)| = O(n^{\ell+1})$. First, we restate the definition of Q_d-adversary structures in the multipartite setting.

▶ **Proposition 2.** *Let $\Pi = (P_1, \dots, P_\ell)$ be a partition of P and Δ be a Π-partite adversary structure on P. Then Δ is of type Q_d if and only if $\boldsymbol{x}_1 + \cdots + \boldsymbol{x}_d \not\succeq \Phi^\Pi(P)$ for any (not necessarily distinct) d points $\boldsymbol{x}_1, \dots, \boldsymbol{x}_d \in \Phi^\Pi(\Delta)$.*

Proof. First, assume that P is covered by d subsets $B_1, \dots, B_d \in \Delta$. Since Δ is monotone decreasing, we may assume that the B_i's are pairwise distinct. Then it holds that $\Phi^\Pi(B_i) \in \Phi^\Pi(\Delta)$ and $\Phi^\Pi(B_1) + \cdots + \Phi^\Pi(B_d) = \Phi^\Pi(P)$.

Second, assume that there exists d points $\boldsymbol{x}_1, \dots, \boldsymbol{x}_d \in \Phi^\Pi(\Delta)$ such that $\boldsymbol{x}_1 + \cdots + \boldsymbol{x}_d \succeq \Phi^\Pi(P)$. Since $\boldsymbol{c}' \in \Phi^\Pi(\Delta)$ if $\boldsymbol{c} \in \Phi^\Pi(\Delta)$ and $\mathbf{0} \preceq \boldsymbol{c}' \preceq \boldsymbol{c}$, we can replace the $\boldsymbol{x}_i$'s with d points $\boldsymbol{b}_1, \dots, \boldsymbol{b}_d \in \Phi^\Pi(\Delta)$ such that $\boldsymbol{b}_i \preceq \boldsymbol{x}_i$ and $\boldsymbol{b}_1 + \cdots + \boldsymbol{b}_d = \Phi^\Pi(P)$. Then there exist pairwise disjoint d subsets $B_1, \dots, B_d$ in Δ such that $\boldsymbol{x}_i = \Phi^\Pi(B_i)$. We have that $B_1 \cup \cdots \cup B_d = P$. ◀

Next, we explain the well-known decomposition technique [21], which is fundamental to our construction of d-multiplicative schemes. Roughly speaking, if an adversary structure Δ is decomposed into several adversary structures Δ_i, then a Δ-private secret sharing scheme can be obtained from secret sharing schemes each of which is Δ_i-private. Specifically, let

$\Delta_1, \ldots, \Delta_N$ be N adversary structures on P and set $\Delta^\forall = \bigcap_{i\in[N]} \Delta_i$ and $\Delta^\exists = \bigcup_{i\in[N]} \Delta_i$. Suppose that, for each $i \in [N]$, we are given a Δ_i-private secret sharing scheme $\Sigma_i = (\mathcal{K}_i, \mathcal{R}_i, \mathcal{S}_i, \varphi_i)$. We assume that all domains of secrets $\mathcal{K}_i$ are identical to a finite field $\mathbb{F}$.

In the following, we construct two secret sharing schemes $\Sigma^\forall$ and $\Sigma^\exists$ with domain of secrets $\mathbb{F}$ which are private with respect to $\Delta^\forall$ and $\Delta^\exists$, respectively. Set $\mathcal{R} = \mathcal{R}_1 \times \cdots \times \mathcal{R}_N$ and $\mathcal{S} = \mathcal{S}_1 \times \cdots \times \mathcal{S}_N$. Let $s \in \mathbb{F}$ be a secret to be shared. First, $\Sigma^\forall$ randomly chooses $r = (r_1, \ldots, r_N)$ from $\mathcal{R}$ and sets a vector of shares as $\varphi(s, r) = (\varphi_1(s, r_1), \ldots, \varphi_N(s, r_N)) \in \mathcal{S}^n$. Equivalently, $\Sigma^\forall$ runs N secret sharing schemes Σ_i in parallel with secret s. Second, $\Sigma^\exists$ randomly chooses $r = (r_1, \ldots, r_N)$ from $\mathcal{R}$ and $N-1$ elements $s_1, \ldots, s_{N-1}$ from $\mathbb{F}$. Then it sets $s_N = s - \sum_{i\in[N-1]} s_i$ and a vector of shares as $\varphi(s, (r, s_1, \ldots, s_{N-1})) = (\varphi_1(s_1, r_1), \ldots, \varphi_N(s_N, r_N)) \in \mathcal{S}^n$. In other words, $\Sigma^\exists$ randomly splits s into $s_1, \ldots, s_N$ and runs Σ_i in parallel with secret s_i for each $i \in [N]$. Then the following proposition holds.

▶ **Proposition 3** ([21]). *Let $\mathbb{F}$ be a finite field. Let $\Delta_1, \ldots, \Delta_N$ be N adversary structures on P and set $\Delta^\forall = \bigcap_{i\in[N]} \Delta_i$ and $\Delta^\exists = \bigcup_{i\in[N]} \Delta_i$. Suppose that, for each $i \in [N]$, a Δ_i-private secret sharing scheme $\Sigma_i = (\mathbb{F}, \mathcal{R}_i, \mathcal{S}_i, \varphi_i)$ is given. Then there exist a $\Delta^\forall$-private secret sharing scheme $\Sigma^\forall$ and a $\Delta^\exists$-private secret sharing scheme $\Sigma^\exists$ both of which have information ratios at most $\sum_{i\in[N]} \sigma(\Sigma_i)$.*

Now, we are ready to provide our construction of d-multiplicative schemes. Let $\Pi = (P_1, \ldots, P_\ell)$ be a partition of P and Δ be a Π-partite adversary structure. Write $\max \Phi^\Pi(\Delta) = \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N\}$. We decompose Δ into N adversary structures $\Delta_1, \ldots, \Delta_N$ as $\Delta = \bigcup_{j\in[N]} \Delta_j$, where Δ_j is the Π-partite adversary structure such that $\Phi^\Pi(\Delta_j) = \{\boldsymbol{x} \in \Phi^\Pi(2^P) : \boldsymbol{x} \preceq \boldsymbol{a}_j\}$. Furthermore, we decompose each Δ_j into ℓ adversary structures $\Delta_{j1}, \ldots, \Delta_{j\ell}$ as $\Delta_j = \bigcap_{k\in[\ell]} \Delta_{jk}$, where Δ_{jk} is the Π-partite adversary structure such that $\Phi^\Pi(\Delta_{jk}) = \{\boldsymbol{x} \in \Phi^\Pi(2^P) : \boldsymbol{x}(k) \le \boldsymbol{a}_j(k)\}$.

For each Δ_{jk}, we can construct a Δ_{jk}-private scheme Σ_{jk} based on the $(\boldsymbol{a}_j(k), |P_k|)$-Shamir secret sharing scheme. Indeed, let $\mathbb{F}$ be a finite field with $|\mathbb{F}| > n$ and fix n distinct nonzero elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$. For a secret $s \in \mathbb{F}$, choose a random polynomial f_{jk} of degree at most $\boldsymbol{a}_j(k)$ conditioned on $f_{jk}(0) = s$ and assign $f_{jk}(\alpha_i) \in \mathbb{F}$ to each player $i \in P_k$.

In view of Proposition 3, we obtain a Δ_j-private secret sharing scheme Σ_j from $\Sigma_{j1}, \ldots, \Sigma_{j\ell}$. Since Σ_{jk} does not assign any share to players in $P_{k'}$ for $k' \neq k$, the information ratio of Σ_j is n. Again, from Proposition 3, we obtain a Δ-private secret sharing scheme Σ with information ratio nN from $\Sigma_1, \ldots, \Sigma_N$.

We show that the scheme Σ constructed in this way is d-multiplicative if Δ is of type Q_d.

▶ **Theorem 4.** *Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| > n$. Let $\Pi = (P_1, \ldots, P_\ell)$ be a partition of P and Δ be a Π-partite Q_d-adversary structure on P. Write $\max \Phi^\Pi(\Delta) = \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N\}$. Then there exists a Δ-private d-multiplicative $\mathbb{F}$-linear secret sharing scheme Σ such that $\sigma(\Sigma) = nN$.*

Proof. First, we define some notations. For each $i \in P$, let $\ell_i \in [\ell]$ be the unique index such that $i \in P_{\ell_i}$. Since Δ is of type Q_d, it holds that $\boldsymbol{a}_{j_1} + \cdots + \boldsymbol{a}_{j_d} \not\succeq \Phi^\Pi(P)$ for any $\boldsymbol{j} = (j_1, \ldots, j_d) \in [N]^d$. In particular, there exists an index k such that $\boldsymbol{a}_{j_1}(k) + \cdots + \boldsymbol{a}_{j_d}(k) < |P_k|$. Thus, we can define 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 any $\boldsymbol{j} = (j_1, \ldots, j_d) \in [N]^d$. For each $\boldsymbol{j} = (j_1, \ldots, j_d) \in [N]^d$, we fix a subset $\widetilde{P}_{\boldsymbol{j}} \subseteq P_{\psi(\boldsymbol{j})}$ of size $\boldsymbol{a}_{j_1}(\psi(\boldsymbol{j})) + \cdots + \boldsymbol{a}_{j_d}(\psi(\boldsymbol{j})) + 1$. Note that $\ell_i = \psi(\boldsymbol{j})$ if $i \in \widetilde{P}_{\boldsymbol{j}}$. Furthermore, we define $J_i := \{\boldsymbol{j} \in [N]^d : i \in \widetilde{P}_{\boldsymbol{j}}\}$ for $i \in P$.

Let Σ be the above secret sharing scheme. From the construction of Σ, any share assigned to $i \in P$ for a secret s has the form of $(f_{1\ell_i}(\alpha_i), \ldots, f_{N\ell_i}(\alpha_i))$, where each $f_{j\ell_i}$ is a polynomial of degree at most $\boldsymbol{a}_j(\ell_i)$ and $s = f_{1\ell_i}(0) + \cdots + f_{N\ell_i}(0)$. For any $k \neq k' \in [\ell]$, the schemes Σ_{jk} and $\Sigma_{jk'}$ have the same secret as inputs and hence it holds that $f_{jk}(0) = f_{jk'}(0)$.

Let $s^{(1)}, \dots, s^{(d)}$ be any d secrets. For $m \in [d]$, let $(f^{(m)}_{1\ell_i}(\alpha_i), \dots, f^{(m)}_{N\ell_i}(\alpha_i))$ be a share assigned to $i \in P$ for the secret $s^{(m)}$. Since $f^{(m)}_{jk}(0)$ have the same value for all $k \in [\ell]$, we denote the common value by $s^{(m)}_j$. Then it holds that $s^{(m)} = s^{(m)}_1 + \cdots + s^{(m)}_N$.

Note that, for any $\boldsymbol{j} = (j_1, \dots, j_d) \in [N]^d$ and $k = \psi(\boldsymbol{j})$, the product $\prod_{m\in[d]} f^{(m)}_{j_m k}$ is a polynomial of degree at most $\sum_{m\in[d]} \boldsymbol{a}_{j_m}(k)$ and $\widetilde{P}_{\boldsymbol{j}}$ is a subset of size $\sum_{m\in[d]} \boldsymbol{a}_{j_m}(k) + 1$. Thus, by Lagrange interpolation, for any $\boldsymbol{j} = (j_1, \dots, j_d) \in [N]^d$, it holds that

$$s^{(1)}_{j_1} \cdots s^{(d)}_{j_d} = f^{(1)}_{j_1,\psi(\boldsymbol{j})}(0) \cdots f^{(d)}_{j_d,\psi(\boldsymbol{j})}(0) = \sum_{i\in\widetilde{P}_{\boldsymbol{j}}} \lambda_i^{\widetilde{P}_{\boldsymbol{j}}} f^{(1)}_{j_1\ell_i}(\alpha_i) \cdots f^{(d)}_{j_d\ell_i}(\alpha_i),$$

where $\lambda_i^{\widetilde{P}_{\boldsymbol{j}}}$ is a lagrange coefficient, i.e., $\lambda_i^{\widetilde{P}_{\boldsymbol{j}}} = \prod_{k\in\widetilde{P}_{\boldsymbol{j}}\setminus\{i\}} \alpha_k/(\alpha_k - \alpha_i)$.

Now we have

$$\begin{aligned} s^{(1)} \cdots s^{(d)} &= \sum_{\boldsymbol{j}=(j_1,\dots,j_d)\in[N]^d} s^{(1)}_{j_1} \cdots s^{(d)}_{j_d} \\ &= \sum_{\boldsymbol{j}\in[N]^d} \sum_{i\in\widetilde{P}_{\boldsymbol{j}}} \lambda_i^{\widetilde{P}_{\boldsymbol{j}}} f^{(1)}_{j_1\ell_i}(\alpha_i) \cdots f^{(d)}_{j_d\ell_i}(\alpha_i) \\ &= \sum_{i\in P} \sum_{\boldsymbol{j}\in J_i} \lambda_i^{\widetilde{P}_{\boldsymbol{j}}} f^{(1)}_{j_1\ell_i}(\alpha_i) \cdots f^{(d)}_{j_d\ell_i}(\alpha_i). \end{aligned}$$

For $i \in P$ with $J_i = \emptyset$, the corresponding sum is assumed to be 0. Therefore, the d-multiplicativity follows by defining $\mathrm{MULT} : P \times \mathcal{S}^d \to \mathbb{F}$ as

$$\mathrm{MULT}(i, (\gamma^{(1)}_1, \dots, \gamma^{(1)}_N), \dots, (\gamma^{(d)}_1, \dots, \gamma^{(d)}_N)) = \sum_{\boldsymbol{j}=(j_1,\dots,j_d)\in J_i} \lambda_i^{\widetilde{P}_{\boldsymbol{j}}} \gamma^{(1)}_{j_1} \cdots \gamma^{(d)}_{j_d}. \qquad \blacktriangleleft$$

Since $N = |\max \Phi^{\Pi}(\Delta)|$ is clearly at most $|\Phi^{\Pi}(2^P)| = O(n^\ell)$, we can obtain a Δ-private d-multiplicative secret sharing schemes with information ratio $O(n^{\ell+1})$ for any ℓ-partite Q_d-adversary structure Δ. Although the CNF scheme for Δ is also d-multiplicative, the information ratio $\sum_{i\in P} |\Delta_i^+|$ is exponential in n. Indeed, the set of all maximal subsets Δ^+ contains at least all subsets A such that $\Phi^{\Pi}(A) = \boldsymbol{a}_1$. Therefore, we have

$$|\Delta_i^+| \geq \binom{|P_{\ell_i}| - 1}{\boldsymbol{a}_1(\ell_i)} \prod_{k\in[\ell]\setminus\{\ell_i\}} \binom{|P_k|}{\boldsymbol{a}_1(k)}.$$

▶ **Example 5.** We apply Theorem 4 to a family of bipartite adversary structures. Suppose that the number of servers an adversary can corrupt is at most k. Equivalently, suppose that the adversary structure Δ corresponding to the adversary satisfies $\Delta \subseteq \mathcal{T}^n_k$. If $n > dk$, Shamir's scheme can tolerate the maximal adversary $\Delta = \mathcal{T}^n_k$. In the case of $d(k-1) < n \leq dk$, it is no longer possible to make d-multiplicative schemes secure against an adversary who can corrupt *any* k servers since $\mathcal{T}^n_k$ is not of type Q_d. On the other hand, d-multiplicative secret sharing can still tolerate any $k-1$ corrupted servers. It is natural to ask how many subsets of size k we can add to Δ under the condition that $\Delta \supseteq \mathcal{T}^n_{k-1}$. Then, for $n = dk - r$ with $0 \leq r < d-1$,[1] we define the following $(S, P\setminus S)$-partite adversary structure $\mathcal{B}^n_k(S)$ for a subset $S \subseteq P$ of size $(d-r)k - 1$:

$$\mathcal{B}^n_k(S) = \mathcal{T}^n_{k-1} \cup \{A \subseteq P : |A| = k \text{ and } A \subseteq S\}.$$

[1] When $r = d-1$ and $n = d(k-1)+1$, $\mathcal{T}^n_{k-1} \cup \{B\}$ is not of type Q_d for any subset B of size k. In other words, $\mathcal{T}^n_{k-1}$ is the only Q_d-adversary structure Δ such that $\Delta \supseteq \mathcal{T}^n_{k-1}$.

This adversary structure corresponds to the situation in which the adversary can corrupt any $k-1$ servers in P and any k servers in S. It can be shown that $\mathcal{B}_k^n(S)$ is actually of type Q_d and is maximal in the sense that $\mathcal{B}_k^n(S) \cup \{B\}$ is not of type Q_d for any subset $B \notin \mathcal{B}_k^n(S)$ of size k (see Appendix A).

It can be seen that $\max \Phi^{\Pi}(\mathcal{B}_k^n(S)) = \{(k,0)\} \cup \{(x, k-1-x) : x = 0, 1, \ldots, k-2\}$ if $0 < r < d-1$ and $\max \Phi^{\Pi}(\mathcal{B}_k^n(S)) = \{(k,0), (k-2,1)\}$ if $r = 0$. From Theorem 4, we obtain a $\mathcal{B}_k^n(S)$-private d-multiplicative secret sharing scheme whose information ratio is kn if $d(k-1)+1 < n < dk$ and $2n$ if $n = dk$. The scheme can be defined over any finite field $\mathbb{F}$ with $|\mathbb{F}| > n$.

4 d-Multiplicative Secret Sharing for ℓ-Partite Adversary Structures with Good Geometric Properties

Let Δ be a Π-partite adversary structure. We show that there exists a more efficient Δ-private d-multiplicative scheme than the above general construction if the associated set of integer points $\Phi^{\Pi}(\Delta)$ has some good geometric property.

Let $C = \mathrm{Conv}(\Phi^{\Pi}(\Delta))$ be the *convex hull* of $\Phi^{\Pi}(\Delta)$ in $\mathbb{R}^{\ell}$. The convex hull of a finite set $S = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N\}$ is defined by

$$\mathrm{Conv}(S) = \left\{ \sum_{j=1}^{N} \alpha_j \boldsymbol{x}_j : \forall j \in [N],\ \alpha_j \geq 0 \text{ and } \sum_{j=1}^{N} \alpha_j = 1 \right\}.$$

Set $\boldsymbol{p} := (1/d)\Phi^{\Pi}(P)$. Assume that $\boldsymbol{p} \notin C$. The hyperplane separation theorem [13, Theorem 4.4] states that there exists a vector $\boldsymbol{h}$ such that $\boldsymbol{h} \cdot (\boldsymbol{c} - \boldsymbol{p}) < 0$ for any $\boldsymbol{c} \in C$. Then there do not exist $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_d \in \Phi^{\Pi}(\Delta)$ such that $\boldsymbol{x}_1 + \cdots + \boldsymbol{x}_d = \Phi^{\Pi}(P)$ since, otherwise, it would hold $\sum_{i \in [d]} \boldsymbol{h} \cdot (\boldsymbol{x}_i - \boldsymbol{p}) = 0$. In short, an adversary structure Δ is of type Q_d if $\boldsymbol{p} \notin \mathrm{Conv}(\Phi^{\Pi}(\Delta))$. Furthermore, since C is closed, there exists some $\epsilon > 0$ such that $\|\boldsymbol{p} - \boldsymbol{c}\| \geq \epsilon$ for any $\boldsymbol{c} \in C$.

For an adversary structure Δ with $\mathrm{dist}(\boldsymbol{p}, C) \geq \epsilon > 0$, we construct a Δ-private d-multiplicative secret sharing scheme whose information ratio is at most $O(\ell n^2/\epsilon)$ based on weighted threshold secret sharing. For example, if ϵ is a constant independent of n, the information ratio is much smaller than those of the schemes from the above general construction, which is $O(n^{\ell+1})$.

To begin with, we show that the convex hull C is also monotone decreasing. Specifically, for any $\boldsymbol{c} \in C$, the hyperrectangle determined by $\boldsymbol{0}$ and $\boldsymbol{c}$ is included in C.

▶ **Lemma 6.** *Let $\Pi = (P_1, \ldots, P_{\ell})$ be a partition of P and Δ be a Π-partite adversary structure. Let $C = \mathrm{Conv}(\Phi^{\Pi}(\Delta))$ be the convex hull of $\Phi^{\Pi}(\Delta)$ in $\mathbb{R}^{\ell}$. If $\boldsymbol{c} \in C$ and $\boldsymbol{0} \preceq \boldsymbol{c}' \preceq \boldsymbol{c}$, then $\boldsymbol{c}' \in C$.*

Proof. Let $\boldsymbol{c} \in C$ and represent it as a convex combination of some points of $\Phi^{\Pi}(\Delta)$: $\boldsymbol{c} = \sum_i \alpha_i \boldsymbol{x}_i$, where $\sum_i \alpha_i = 1$ and $\alpha_i \geq 0$. Then, for any $A \subseteq [\ell]$, $\boldsymbol{c}(A) = \sum_i \alpha_i \boldsymbol{x}_i(A)$ and hence $\boldsymbol{c}(A) \in C$. Here, for a vector $\boldsymbol{v} \in \mathbb{R}^{\ell}$ and $A \subseteq [\ell]$, $\boldsymbol{v}(A)$ denotes the vector whose entries indexed by A are the same as those of $\boldsymbol{v}$ and 0 otherwise. If we set $X := \{\boldsymbol{c}(A) : A \in 2^{[\ell]}\}$, it holds that $\mathrm{Conv}(X) \subseteq C$ since C is convex.

We finish the proof by showing that $\mathrm{Conv}(X) = \{\boldsymbol{x} \in \mathbb{R}^{\ell} : \boldsymbol{0} \preceq \boldsymbol{x} \preceq \boldsymbol{c}\}$. Let $\boldsymbol{x} \in \mathbb{R}^{\ell}$ with $\boldsymbol{0} \preceq \boldsymbol{x} \preceq \boldsymbol{c}$. Set $Z = \{i \in [\ell] : \boldsymbol{c}(i) \neq 0\}$ and write $\{\boldsymbol{x}(i)/\boldsymbol{c}(i) : i \in Z\} = \{v_1, \ldots, v_m\}$, where $v_0 := 0 \leq v_1 < \cdots < v_m \leq 1$. Furthermore, for $j \in [m]$, set $I_j = \{i \in Z : \boldsymbol{x}(i)/\boldsymbol{c}(i) = v_j\}$ and $A_j = I_j \cup I_{j+1} \cup \cdots \cup I_m$. Let $\boldsymbol{y}$ be a vector such that $\boldsymbol{y}(i) = \boldsymbol{x}(i)/\boldsymbol{c}(i)$ for $i \in Z$ and otherwise $\boldsymbol{y}(i) = 0$. Then we have $\boldsymbol{y} = \sum_{j=1}^{m} (v_j - v_{j-1}) \boldsymbol{1}(A_j)$, from which we obtain $\boldsymbol{x} = \sum_{j=1}^{m} (v_j - v_{j-1}) \boldsymbol{c}(A_j) + (1 - v_m)\boldsymbol{c}(\emptyset)$. Thus, $\boldsymbol{x} \in \mathrm{Conv}(X)$. The other inclusion clearly holds. ◀

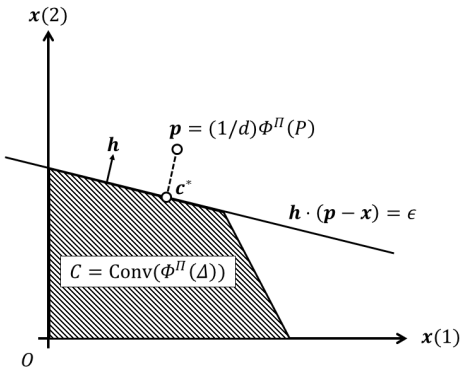

Figure 1 The convex hull of $\Phi^{\Pi}(\Delta)$ in $\mathbb{R}^{\ell}$.

Next, we show that if we set $\boldsymbol{h}$ as the unit vector parallel to $\boldsymbol{p}-\boldsymbol{c}^*$ for the closest point $\boldsymbol{c}^* \in C$ to $\boldsymbol{p}$, then $\boldsymbol{h}\cdot(\boldsymbol{p}-\boldsymbol{x}) \geq \mathrm{dist}(\boldsymbol{p}, C)$ for any $\boldsymbol{x} \in \Phi^{\Pi}(\Delta)$. Although the existence of $\boldsymbol{h}$ easily follows from the hyperplane separation theorem, we additionally show that $\boldsymbol{h} \in \mathbb{R}^{\ell}_{+}$ using the fact that C is monotone decreasing. The vector $\boldsymbol{h}$ is used to find a weight vector $\boldsymbol{w}$ such that $\Delta \subseteq \mathcal{W}^{\Pi}_{\boldsymbol{w},t}$.

▶ **Lemma 7.** *Let $\Pi = (P_1, \ldots, P_\ell)$ be a partition of P and Δ be a Π-partite adversary structure. 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 $\mathrm{dist}(\boldsymbol{p}, C) \geq \epsilon > 0$, i.e., $\|\boldsymbol{c}-\boldsymbol{p}\| \geq \epsilon$ for any $\boldsymbol{c} \in C$. 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 $\boldsymbol{c}^* \not\preceq \boldsymbol{p}$. 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 $\boldsymbol{0} \preceq \boldsymbol{c}' \preceq \boldsymbol{c}^*$, $\boldsymbol{c}'$ 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 $\boldsymbol{x} \in \Phi^{\Pi}(\Delta) \subseteq C$. ◀

To obtain a weight vector $\boldsymbol{w}$, we approximate $\boldsymbol{h}$ by a vector of rational numbers $\boldsymbol{h}+\boldsymbol{\delta}$ for a small vector $\boldsymbol{\delta}$ and set $\boldsymbol{w} = q(\boldsymbol{h}+\boldsymbol{\delta})$ for some integer q. 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 q to be $q = O(\ell n/\epsilon)$.

▶ **Lemma 8.** *In the setting of Lemma 7, 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 any $\boldsymbol{x} \in \Phi^{\Pi}(\Delta)$ and $0 \leq \boldsymbol{w}(j) \leq (\ell n/\epsilon) + 1$ for any $j \in [\ell]$.*

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 q be the smallest positive integer satisfying $q > \ell n/\epsilon$. Set $p_j = \lceil q\boldsymbol{h}(j) \rceil$ for each $j \in [\ell]$. Since $\|\boldsymbol{h}\| = 1$, we have $0 \leq q\boldsymbol{h}(j) \leq q$ and hence $0 \leq p_j \leq q$.

Let $\boldsymbol{\delta} \in \mathbb{R}^\ell$ be a vector such that

$$0 \leq \boldsymbol{\delta}(j) = \frac{p_j}{q} - \boldsymbol{h}(j) \leq \frac{1}{q}.$$

Then $\|\boldsymbol{\delta}\| \leq \|q^{-1}\mathbf{1}\| < \epsilon/(\sqrt{\ell} n)$. Set $\boldsymbol{w} = q(\boldsymbol{h} + \boldsymbol{\delta}) = (p_1, \ldots, p_\ell) \in \mathbb{Z}_+^\ell$. It holds that $f_j(\boldsymbol{w}) = q f_j(\boldsymbol{h} + \boldsymbol{\delta}) < 0$ for any $j \in [N]$ and $0 \leq \boldsymbol{w}(j) \leq q \leq (\ell n/\epsilon) + 1$. ◀

Now, we construct a d-multiplicative scheme using the weight vector $\boldsymbol{w}$ in Lemma 8.

▶ **Theorem 9.** *Let $\Pi = (P_1, \ldots, P_\ell)$ be a partition of P and Δ be a Π-partite adversary structure. Let C be the convex hull of $\Phi^{\Pi}(\Delta)$ in $\mathbb{R}^\ell$. Set $\boldsymbol{p} = (1/d)\Phi^{\Pi}(P)$. Suppose that $\mathrm{dist}(\boldsymbol{p}, C) \geq \epsilon > 0$. If $\mathbb{F}$ is a finite field with $|\mathbb{F}| > (\ell n^2/\epsilon) + n$, then there exists a Δ-private d-multiplicative $\mathbb{F}$-linear secret sharing scheme whose information ratio is at most $(\ell n^2/\epsilon) + n$.*

Proof. From Lemma 8, 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 $\boldsymbol{x} \in \Phi^{\Pi}(\Delta)$. Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| > \boldsymbol{w} \cdot \Phi^{\Pi}(P)$. Then, applying Proposition 1 to the weighted threshold adversary structure $\mathcal{W}^{\Pi}_{\boldsymbol{w},t}$, we obtain Δ-private d-multiplicative secret sharing scheme over $\mathbb{F}$ whose information ratio is $\boldsymbol{w} \cdot \Phi^{\Pi}(P) \leq (\ell n^2/\epsilon) + n$. ◀

The construction of Theorem 9 is a natural generalization of Shamir's threshold schemes. Indeed, the convex hull $C = \mathrm{Conv}(\Phi^{\Pi}(\Delta))$ for $\Delta = \mathcal{T}_k^n$ is $\{\boldsymbol{x} \in \mathbb{R}^\ell : \mathbf{1} \cdot \boldsymbol{x} \leq k\}$. Thus, the condition $\boldsymbol{p} \notin C$ holds if and only if $n > dk$. Then we can set $\boldsymbol{w} \in \mathbb{Z}_+^\ell$ in the proof of Theorem 9 as $\mathbf{1} \in \mathbb{Z}_+^\ell$ and $t = \max_{\boldsymbol{x} \in \Phi^{\Pi}(\mathcal{T}_k^n)}\{\boldsymbol{w} \cdot \boldsymbol{x}\} = k$. The weighted threshold secret sharing for $\mathcal{W}^{\Pi}_{\boldsymbol{w},t} = \mathcal{W}^{\Pi}_{\mathbf{1},k}$ obtained from Proposition 1 is nothing but the (k, n)-Shamir secret sharing scheme.

▶ **Example 10.** We consider the bipartite adversary structure $\mathcal{B}_k^n(S)$ in Example 5 again.

If $n = dk - r$ and $0 < r < d - 1$, then the convex hull $C = \mathrm{Conv}(\Phi^{\Pi}(\mathcal{B}_k^n(S)))$ is

$$C = \{(x, y) \in \mathbb{R}^2 : x \geq 0,\ y \geq 0,\ (k-1)x + ky \leq k(k-1)\}.$$

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 9 as $(k-1, k)$. If we set $t = \max_{\boldsymbol{x} \in \Phi^{\Pi}(\mathcal{B}_k^n(S))}\{\boldsymbol{w} \cdot \boldsymbol{x}\} = k(k-1)$, then $\mathcal{B}_k^n(S) = \mathcal{W}^{\Pi}_{\boldsymbol{w},t}$. As a result, we obtain a $\mathcal{B}_k^n(S)$-private d-multiplicative secret sharing scheme whose information ratio is $\boldsymbol{w} \cdot \Phi^{\Pi}(P) = dk^2 - dk + 1$. The scheme can be defined over any finite field $\mathbb{F}$ with $|\mathbb{F}| > dk^2 - dk + 1$.

If $n = dk$, then the convex hull $C = \mathrm{Conv}(\Phi^{\Pi}(\mathcal{B}_k^n(S)))$ is

$$C = \{(x, y) \in \mathbb{R}^2 : x \geq 0,\ 0 \leq y \leq 1,\ x + 2y \leq k\}.$$

Now, we can set $\boldsymbol{w} \in \mathbb{Z}_+^2$ as $(1, 2)$ and $t = \max_{\boldsymbol{x} \in \Phi^{\Pi}(\mathcal{B}_k^n(S))}\{\boldsymbol{w} \cdot \boldsymbol{x}\} = k$. Therefore, we obtain a $\mathcal{B}_k^n(S)$-private d-multiplicative secret sharing scheme whose information ratio is $\boldsymbol{w} \cdot \Phi^{\Pi}(P) = dk + 1 = n + 1$. The scheme can be defined over any finite field $\mathbb{F}$ with $|\mathbb{F}| > n + 1$.

In both cases, the information ratios are smaller than those of the d-multiplicative schemes in Example 5, which are $kn = dk^2 - rk$ if $0 < r < d-1$ and $2n$ if $r = 0$. However, the schemes in Example 5 can be defined over a smaller field $\mathbb{F}$ such that $|\mathbb{F}| > n$.

Moreover, we provide another example of adversary structures which arise in real-world scenarios and apply Theorem 9 to them. In a naive approach based on weighted threshold secret sharing, the obtained information ratio would grow infinitely depending on the description of an adversary structure.

▶ **Example 11.** Suppose that a Π-partite adversary structure Δ is described as $\Phi^{\Pi}(\Delta) = \{\boldsymbol{x} \in \Phi^{\Pi}(2^P) : \boldsymbol{a} \cdot \boldsymbol{x} \leq b\}$ for some $\boldsymbol{a}$ and b and that $\boldsymbol{a} \cdot \boldsymbol{p} > b$. In a real-world setting, such Δ corresponds to a situation in which each value $\boldsymbol{a}(j)$ is the cost required to corrupt a single server in the j-th part and b specifies the maximum tolerable cost. Note that there are infinitely many pairs $(\boldsymbol{a}', b')$ such that $\Phi^{\Pi}(\Delta) = \{\boldsymbol{x} \in \Phi^{\Pi}(2^P) : \boldsymbol{a}' \cdot \boldsymbol{x} \leq b'\}$ since $\Phi^{\Pi}(\Delta)$ is a finite subset in $\mathbb{R}^{\ell}$.

If $\boldsymbol{a} \in \mathbb{Z}_+^{\ell}$, then we have $\Delta \subseteq \mathcal{W}^{\Pi}_{\boldsymbol{a},t}$ and $dt < \boldsymbol{a} \cdot \Phi^{\Pi}(P)$ for $t = \max_{\boldsymbol{x} \in \Phi^{\Pi}(\Delta)}\{\boldsymbol{a} \cdot \boldsymbol{x}\}$. Hence, we immediately obtain a Δ-private d-multiplicative scheme whose information ratio is $\boldsymbol{a} \cdot \Phi^{\Pi}(P)$. However, $\boldsymbol{a}$ is not necessarily a vector of non-negative integers. One may have a good rational approximation $\widetilde{\boldsymbol{a}}$ of $\boldsymbol{a}$ and set $\boldsymbol{w} = N\widetilde{\boldsymbol{a}} \in \mathbb{Z}_+^{\ell}$ for some N. Nevertheless, as the complexity of $\boldsymbol{a}$ increases, N would grow infinitely, which results in a large information ratio.

From Theorem 9, we can construct a Δ-private d-multiplicative scheme whose information ratio depends on the distance between the point $\boldsymbol{p}$ and the hyperplane $H = \{\boldsymbol{x} \in \mathbb{R}^{\ell} : \boldsymbol{a} \cdot \boldsymbol{x} = b\}$ rather than the complexity of the coefficient vector $\boldsymbol{a}$. Let $C = \{\boldsymbol{x} \in \mathbb{R}^{\ell} : \boldsymbol{a} \cdot \boldsymbol{x} \leq b\}$. Since C is convex, C includes $\mathrm{Conv}(\Phi^{\Pi}(\Delta))$. Thus, the distance between $\boldsymbol{p}$ and $\mathrm{Conv}(\Phi^{\Pi}(\Delta))$ is lower bounded by $\mathrm{dist}(\boldsymbol{p}, H)$. In other words, for any $\boldsymbol{c} \in \mathrm{Conv}(\Phi^{\Pi}(\Delta))$, it holds that $\|\boldsymbol{c} - \boldsymbol{p}\| \geq \mathrm{dist}(\boldsymbol{p}, H) = (\boldsymbol{a} \cdot \boldsymbol{p} - b)/\|\boldsymbol{a}\|$. From Theorem 9, we have a Δ-private d-multiplicative secret sharing scheme Σ such that

$$\sigma(\Sigma) \leq \frac{\ell n^2}{\mathrm{dist}(\boldsymbol{p}, H)} + n = \frac{\ell n^2 \|\boldsymbol{a}\|}{\boldsymbol{a} \cdot \boldsymbol{p} - b} + n.$$

To explicitly obtain secret sharing schemes from Theorem 9, we have to find the vector $\boldsymbol{h} = (\boldsymbol{p} - \boldsymbol{c}^*)/\|\boldsymbol{p} - \boldsymbol{c}^*\|$ in Lemma 7, where $\boldsymbol{c}^*$ is the closest point in $C = \mathrm{Conv}(\Phi^{\Pi}(\Delta))$ to $\boldsymbol{p}$. For that purpose, we can make use of (hard margin) *support vector machine* [22]. Note that, since C is convex, the vector $\boldsymbol{h}$ is characterized by the condition $\boldsymbol{h} \cdot (\boldsymbol{p} - \boldsymbol{x}) \geq \epsilon$, $\forall \boldsymbol{x} \in C$, where $\epsilon = \mathrm{dist}(\boldsymbol{p}, C)$. Set a training data set $\mathcal{D}$ as $\mathcal{D} = \{(\boldsymbol{x}, -1) : \boldsymbol{x} \in \Phi^{\Pi}(\Delta)\} \cup \{(\boldsymbol{p}, 1)\}$. Consider the following quadratic programming problem with respect to $\boldsymbol{w} \in \mathbb{R}^{\ell}$ and $b \in \mathbb{R}$:

$$\begin{array}{ll} \text{minimize} & \|\boldsymbol{w}\|^2 \\ \text{subject to} & y(\boldsymbol{w} \cdot \boldsymbol{x} - b) \geq 1, \qquad \forall (\boldsymbol{x}, y) \in \mathcal{D}. \end{array}$$

It holds that $\boldsymbol{h} \cdot \boldsymbol{x} - (\boldsymbol{h} \cdot \boldsymbol{p} - \epsilon/2) \leq -\epsilon/2$ for any $\boldsymbol{x} \in \Phi^{\Pi}(\Delta)$, which means that $((2/\epsilon)\boldsymbol{h}, (2/\epsilon)\boldsymbol{h} \cdot \boldsymbol{p} - 1)$ is a feasible solution to the problem. On the other hand, for any feasible solution $(\boldsymbol{w}, b)$, we have $C \subseteq \{\boldsymbol{x} \in \mathbb{R}^{\ell} : \boldsymbol{w} \cdot \boldsymbol{x} - b \leq -1\}$ and hence $\epsilon \geq 2/\|\boldsymbol{w}\|$, that is, $\|\boldsymbol{w}\| \geq \|(2/\epsilon)\boldsymbol{h}\|$. Therefore, the optimal solution $(\boldsymbol{w}^*, b^*)$ is given by $((2/\epsilon)\boldsymbol{h}, (2/\epsilon)\boldsymbol{h} \cdot \boldsymbol{p} - 1)$. Then we obtain the vector $\boldsymbol{h}$ by computing $\boldsymbol{h} = \boldsymbol{w}^*/\|\boldsymbol{w}^*\|$.

References

1 Omer Barkol, Yuval Ishai, and Enav Weinreb. On d-multiplicative secret sharing. *Journal of cryptology*, 23(4):580–593, 2010.

2 Amos Beimel. Secret-sharing schemes: A survey. In *Coding and Cryptology*, pages 11–46, 2011.

3 Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 1–10, 1988.

4 G. R. Blakley. Safeguarding cryptographic keys. In *1979 International Workshop on Managing Requirements Knowledge (MARK)*, pages 313–318, 1979.

5 Elette Boyle, Niv Gilboa, and Yuval Ishai. Breaking the circuit size barrier for secure computation under ddh. In *Advances in Cryptology — CRYPTO 2016*, pages 509–539, 2016.

6 Elette Boyle, Lisa Kohl, and Peter Scholl. Homomorphic secret sharing from lattices without fhe. In *Advances in Cryptology — EUROCRYPT 2019*, pages 3–33, 2019.

7 I. Cascudo, R. Cramer, and C. Xing. The arithmetic codex. In *2012 IEEE Information Theory Workshop*, pages 75–79, 2012.

8 Hao Chen and Ronald Cramer. Algebraic geometric secret sharing schemes and secure multi-party computations over small fields. In *Advances in Cryptology — CRYPTO 2006*, pages 521–536, 2006.

9 Ronald Cramer, Ivan Damgård, and Ueli Maurer. General secure multi-party computation from any linear secret-sharing scheme. In *Advances in Cryptology — EUROCRYPT 2000*, pages 316–334, 2000.

10 Ivan Damgård and Jesper Buus Nielsen. Scalable and unconditionally secure multiparty computation. In *Advances in Cryptology — CRYPTO 2007*, pages 572–590, 2007.

11 Oriol Farràs, Jaume Martí-Farré, and Carles Padró. Ideal multipartite secret sharing schemes. *Journal of cryptology*, 25(3):434–463, 2012.

12 Oriol Farràs and Carles Padró. Ideal secret sharing schemes for useful multipartite access structures. In *Coding and Cryptology*, pages 99–108, 2011.

13 P. M. Gruber. *Convex and Discrete Geometry*. Springer-Verlag, 2007.

14 Martin Hirt and Daniel Tschudi. Efficient general-adversary multi-party computation. In *Advances in Cryptology — ASIACRYPT 2013*, pages 181–200, 2013.

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

16 E. Karnin, J. Greene, and M. Hellman. On secret sharing systems. *IEEE Transactions on Information Theory*, 29(1):35–41, 1983.

17 Emilia Käsper, Ventzislav Nikov, and Svetla Nikova. Strongly multiplicative hierarchical threshold secret sharing. In *International Conference on Information Theoretic Security*, pages 148–168, 2007.

18 M. Liu, L. Xiao, and Z. Zhang. Multiplicative linear secret sharing schemes based on connectivity of graphs. *IEEE Transactions on Information Theory*, 53(11):3973–3978, 2007.

19 Ueli Maurer. Secure multi-party computation made simple. *Discrete Applied Mathematics*, 154(2):370–381, 2006.

20 A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

21 D. R. Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Transactions on Information Theory*, 40(1):118–125, 1994.

22 Vladimir Vapnik. Pattern recognition using generalized portrait method. *Automation and remote control*, 24:774–780, 1963.

A The Bipartite Adversary Structure $\mathcal{B}_k^n(S)$

▶ **Proposition 12.** *Let k, d, r be integers such that $k \geq 1$, $d \geq 2$, and $0 \leq r < d-1$, respectively. Set $n = dk - r$. For any subset $S \subseteq P$ of size $(d-r)k-1$, the bipartite adversary structure $\mathcal{B}_k^n(S)$ is of type Q_d.*

Proof. Assume that P is covered by some pairwise disjoint d subsets $A_1, \ldots, A_d$ in $\mathcal{B}_k^n(S)$. Since $n = (d-r)k + r(k-1)$ and $|A_i| \leq k$ for any $i \in [d]$, we may assume that the first $d-r$ subsets $A_1, \ldots, A_{d-r}$ are of size k and the other subsets $A_{d-r+1}, \ldots, A_d$ are of size $k-1$. From the definition of $\mathcal{B}_k^n(S)$, $A_1, \ldots, A_{d-r}$ are pairwise disjoint subsets of S and, in particular, $|S| \geq |A_1| + \cdots + |A_{d-r}|$. However, S is a set of size $(d-r)k-1$, which is a contradiction. ◀

▶ **Proposition 13.** *Continuing the notation of Proposition 12, $\mathcal{B}_k^n(S) \cup \{B\}$ is not of type Q_d for any subset $B \notin \mathcal{B}_k^n(S)$ of size k.*

Proof. If B is a subset of size k such that $B \notin \mathcal{B}_k^n(S)$, then $|S \setminus B| \geq (d-r-1)k$. Then we can partition $S \setminus B$ into pairwise disjoint $d-r-1$ subsets $B_2, \ldots, B_{d-r}$ of size k. By partitioning $P \setminus (B \cup B_2 \cup \cdots \cup B_{d-r})$ into r subsets $B_{d-r+1}, \ldots, B_d$ each of size $k-1$, we obtain $B \cup B_2 \cup \cdots \cup B_d = P$, which means $\mathcal{B}_k^n(S) \cup \{B\}$ is not Q_d. ◀