# Guarding Multiple Secrets: Enhanced Summary Statistic Privacy for Data Sharing

**Shuaiqi Wang**[*]        **Rongzhe Wei**[†]

**Mohsen Ghassemi**[◇]    **Eleonora Kreačić**[◇]    **Vamsi K. Potluru**[◇]

[*]*ECE, Carnegie Mellon University*                *shuaiqiw@andrew.cmu.edu*
[†]*ECE, Georgia Institute of Technology*          *rongzhe.wei@gatech.edu*
[◇]*J.P. Morgan AI Research*    *{mohsen.ghassemi, eleonora.kreacic, vamsi.k.potluru}@jpmchase.com*

## Abstract

Data sharing enables critical advances in many research areas and business applications, but it may lead to inadvertent disclosure of sensitive summary statistics (e.g., means or quantiles). Existing literature only focuses on protecting a single confidential quantity, while in practice, data sharing involves multiple sensitive statistics. We propose a novel framework to define, analyze, and protect *multi-secret summary statistics privacy* in data sharing. Specifically, we measure the privacy risk of any data release mechanism by the worst-case probability of an attacker successfully inferring summary statistic secrets. Given an attacker's objective spanning from inferring a subset to the entirety of summary statistic secrets, we systematically design and analyze tailored privacy metrics. Defining the distortion as the worst-case distance between the original and released data distribution, we analyze the tradeoff between privacy and distortion. Our contribution also includes designing and analyzing data release mechanisms tailored for different data distributions and secret types. Evaluations on real-world data demonstrate the effectiveness of our mechanisms in practical applications.

## 1   Introduction

Data sharing has become integral to collaborative research and industrial applications [23, 43, 29]. However, in many domains such as finance and healthcare, as well as in industrial settings, the sensitive nature of data is cause for great concern regarding data privacy and leakage of sensitive information. If appropriate measures are not adopted, data sharing may reveal sensitive information not only about particular individuals [1], but also aggregate information at dataset level [19, 39, 25]. Summary statistics of the data (e.g., mean, standard deviation, histograms, etc.) may contain sensitive or proprietary information that the data holder needs to protect due to legal or competitive risks.

In recent years, protecting the privacy of individuals has garnered significant attention, leading to the continued development of prominent frameworks such as differential privacy and its many variants [8, 20]. In contrast, there remains a noticeable lack of research on quantifying the summary statistics leakage of shared datasets. Protecting sensitive summary statistics is especially crucial in industrial settings due to the proprietary nature of such information. Companies, when publishing data on their performance, customer base, or equipment expenditure, are often concerned with leaking sensitive summary statistics that may reveal the firm's typical client characteristics, market segments the firm is most active in, or future business plans. Despite these risks, in many scenarios it is in the data owner's interest, as well as the public interest, to "liberate" data to be shared safely with other entities. One prominent example is when a financial company shares data publicly (e.g. for academic collaborations and furthering potential technological advances in areas such as financial fraud detection and anti-money laundering). Similar scenarios exist for companies in many other industries that can benefit from publishing their data for research purposes or sharing their data with consulting firms. In many cases, the data holder may only deem certain (and not all) summary

statistics as sensitive. Moreover, as with notions of individual privacy, data holders are often comfortable with tolerating a "sufficiently low" leakage risk. This highlights the need for a privacy framework to quantify the risks of revealing summary statistics and allow for designing data release mechanisms that meet the data holder's requirements.

Recently, [25] proposed a novel privacy framework designed to identify and analyze concerns related to summary statistics privacy. They focus solely on the scenario where only one summary statistic is deemed confidential by the data owner. In real-world scenarios, however, one often deals with high-dimensional data where potentially multiple summary statistics may contain sensitive information or be regarded as proprietary information. Hence, there is a compelling need to expand the current framework, ensuring it encompasses cases with multiple confidential statistics.

The privacy metric and analysis in [25] cannot be trivially extended to address the multi-secret case. Given the varied data sharing contexts and the intricacies of summary statistics secrets, data holders' privacy requirements can differ. Some scenarios require *none of the secrets* being disclosed, while others may only demand *not all secrets* being revealed simultaneously. To this end, we propose a framework to quantify, analyze and protect *multi-secret summary statistics privacy* under different protection scenarios.

Our proposed framework includes *interpretable* privacy metrics that have clear operational meaning: the probability that an attacker successfully (i.e. within certain error tolerance range) guesses the secrets. It also includes a utility metric to evaluate the usefulness of the released data. Based on these metrics, we provide privacy-utility trade-off analyses to obtain the fundamental limits of what is achievable for any release mechanism in terms of utility for a given privacy budget, or vice versa. Understanding these limits informs mechanism design as it provides a benchmark to evaluate the "optimality" of any release mechanism.

## 1.1 Main contributions

**Metric Design (§3, §5)** We introduce and analyze several novel interpretable metrics to measure the privacy risks of data release mechanisms for multi-secret protection. In §3.1, we tackle the strictest scenario by defining the privacy metric as the worst-case probability of an attacker correctly guessing any single secret within a specified tolerance range. Subsequently, in §5, we explore relaxed scenarios wherein the data holder aims to thwart the attacker from correctly guessing either a group of or the entirety of secrets simultaneously, establishing the appropriate privacy metric for each.

**Privacy-Distortion Tradeoff Analysis (§4, §5)** We provide the general lower bounds on the distortion given a certain constraint on the privacy corresponding to various privacy metrics. Those lower bounds are non-trivial extensions of the tradeoff analysis in [25]. The analysis of the lower bound is general, but its value depends on data distributions and secret types. The bound also reveals how the number of secrets affect the privacy-distortion tradeoffs under different privacy metrics. We then specify the lower bound under several specific data distributions and secret types.

**Mechanism Design and Empirical Evaluation (§6, §7)** Our privacy framework is applicable to any data release mechanism, and can be used to guide designing mechanisms that effectively protect against summary statistics attacks. To this end, we develop mechanisms tailored to various data distributions and secret types and subsequently assess their performance. At a high level, these mechanisms function by quantizing the distribution parameters into bins and then randomly releasing points within the respective bins into which the parameters fit. Such mechanisms are straightforward to implement and have near-optimal privacy-distortion performance. We employ real-world datasets to demonstrate the effectiveness of our designed data release mechanisms and to illustrate the variations in privacy-distortion tradeoffs across different privacy metrics.

## 2 Related Work

In this section, we provide a brief overview of related work and highlight the main distinctions between our work and prior works in Table 1. A more detailed discussion can be found in App. A.
**Heuristics** Although commonly adopted in many industries for data sharing [16], heuristic methods often lack rigorous privacy guarantees and can be vulnerable in real-world scenarios [10]. Particularly, methods such

Table 1: Comparison with prior privacy frameworks

| | secret to protect | privacy-distortion analysis | suitable to data sharing |
|---|---|---|---|
| Differential Privacy [8] | individual/group information | ✓ | ✓ |
| Distribution Privacy [19] | overall distribution | ✗ | ✓ |
| Attribute Privacy [42] | single summary statistic | ✗ | ✗ |
| Summary Statistic Privacy [25] | single summary statistic | ✓ | ✓ |
| Our Framework | multiple summary statistics | ✓ | ✓ |

as subsetting [32], culling [32], and de-identification [12] are susceptible to re-identification or unintentional data property leakage [28, 38].

**Differential Privacy (DP) [8]**  This notion of privacy ensures indistinguishability between neighboring datasets. Several works have applied DP to release summary statistics [5, 30]. However, as a metric, DP is concerned with privacy guarantees in terms of protecting individual record contributions rather than overarching distributional statistical properties. In other words, it provides no metric to quantify risks of leaking aggregate dataset-level information. Moreover, certain DP mechanisms like the Laplacian [8] introduce zero-mean noise to samples but often leave certain integral statistics (e.g. means) less affected, rendering them unsuitable for directly protecting summary statistic privacy.

**Other Indistinguishability Approaches**  Another relevant line of work is *attribute privacy* [42] which aims to safeguard specific dataset properties. However, their applications do not always align with data sharing scenarios as those methods only output certain statistical queries. Moreover, paradigms like *distribution privacy* [19] and *distribution inference* [36, 37] prioritize preserving the confidentiality of statistical secrets (e.g., mean). Their robust nature, ensuring indistinguishability across a broad range of distributions (e.g., a Dirac delta distribution and a Gaussian distribution with the same mean), may result in adding excessive amount of noise, leading to reduced data utility.

**Leakage-Based Methods**  Many works utilize information-theoretic methods to delineate and safeguard statistical privacy, typically balancing between limiting the disclosure of private data and promoting the release of non-sensitive data. They often characterize the exposure of confidential information through the concept of leakage [2].Various measures, including Shannon entropy [31], min-entropy [3], and gain function [27] have been employed to define leakage. A notable advancement in this area is the concept of *maximal leakage* [17], which quantifies the increased likelihood of correctly inferring secrets post-data release. In contrast to our setting, maximal leakage and its generalizations, such as [14], assume that the secrets are not known to the data holder in advance.

**Summary Statistic Privacy**  The recently introduced summary statistic privacy [25] aligns closely with our objective, emphasizing the protection of the dataset's summary statistics during data sharing. In their approach, privacy is measured by the worst-case likelihood of an adversary accurately discerning the secret within a defined range. However, their framework focuses on safeguarding a singular secret under one-shot attack and confines the data analysis to one dimension, which may not cater comprehensively to many practical applications. Our work is a non-trivial extension of the framework in [25] to guard multiple secrets (see §1.1 for details).

## 3  Problem Formulation

**Notation**  Let $X$ denote any random variable. Its distribution measure is represented by $\omega_X$. When $X$ is part of a parametric family, represented by a parameter $\theta$ that lies in $\mathbb{R}^q$ ($q \geq 1$), our notation becomes more specific: $X_\theta$ for the random variable and $\omega_{X_\theta}$ for its distribution. Additionally, when considering $\theta$ not as a fixed value but as a realization of another random variable, denoted by $\Theta$, its distribution is captured by $\omega_\Theta$. Note that $\omega_\Theta$ acts as the prior distribution of parameter $\theta$.

**Original Data and Summary Statistic Secrets to Protect**  Consider a data holder in possession of a dataset, denoted as $\mathcal{X} = \{x_1, x_2, \ldots, x_m\}$, comprising $m$ i.i.d. samples drawn from a certain distribution. Given the ability to represent diverse datasets using parametric generative models, we posit that this distribution belongs to a parametric family characterized by a parameter $\theta \in \mathbb{R}^q$. The data holder aims to hide $d$

summary statistic secrets from the original data distribution $\omega_{X_\theta}$. We can express the secrets as $d$ functions $\boldsymbol{g} = [g_1, g_2, \cdots, g_d]$, where $g_i(\theta) : \mathbb{R}^q \to \mathbb{R}$ for each function $g_i$.

**Data Release Mechanism** To release data, the data holder passes the original distribution parameter $\theta$ through the data release mechanism $\mathcal{M}_g$. The released data distribution parameter $\theta'$ satisfies $\theta' \sim \mathcal{M}_g(\theta)$.

**Threat Model** We assume the attacker knows the parametric family to which the data generating distribution belongs, but does not know the distribution parameter $\theta$. The attacker also knows the released parameter $\theta'$ and the mechanism $\mathcal{M}_g$, but does not know the realization of the internal randomness of the mechanism. Based on the released parameter $\theta'$, the attacker guesses the secrets $\boldsymbol{g}(\theta) = [g_1(\theta), g_2(\theta), \cdots, g_d(\theta)]$ by strategies $\hat{\boldsymbol{g}}(\theta') = [\hat{g}_1(\theta'), \hat{g}_2(\theta'), \cdots, \hat{g}_d(\theta')]$

## 3.1 Metrics for Preserving Multiple Secrets

We define the privacy and distortion metrics and formulate the data holder's objective as follows.

**Privacy Metric** Consider the case where the data holder aims to prevent attackers from guessing *any* secret correctly. We define the *union privacy* metric $\Pi_{\epsilon,\omega_\Theta}^{\text{union}}$ as the probability of the attacker guessing any secret within a *tolerance range*, $\epsilon_i$ for secret $g_i$, employing the best attack strategy:

$$\Pi_{\epsilon,\omega_\Theta}^{\text{union}} \triangleq \sup_{\hat{\boldsymbol{g}}} \; \mathbb{P}\Big( \bigcup_{i \in [d]} |\hat{g}_i(\theta') - g_i(\theta)| \le \epsilon_i \Big) , \tag{1}$$

where the probability is taken over the randomness of the original data distribution parameter $\theta$, the data release mechanism $\mathcal{M}_g$, and the attacker strategy $\hat{\boldsymbol{g}}$.

Union privacy is the *strictest* privacy metric for the data holder, as the attacker guessing any secret successfully will result in protection failure. In §5, we introduce alternative privacy metrics.

Union privacy also accommodates *multi-shot attack* scenario where the attacker guesses the secret multiple times, and the data holder aims to prevent success in any guess. In this scenario, $g_1 = g_2 = \cdots = g_d$ and $\hat{\boldsymbol{g}}$ represents sequential strategies guessing the secret.

**Distortion Metric** Since the goal of data sharing is to maintain high utility of the disseminated data, it is important to discern the extent to which the released data diverges from the original. In this context, we introduce the concept of *distortion*, denoted as $\Delta_{\mathcal{M}_g}$. Specifically, the distortion of a mechanism is characterized by the worst-case discrepancy between the original distribution and the released distribution:

$$\Delta_{\mathcal{M}_g} \triangleq \sup_{\substack{\theta \in \text{Supp}(\omega_\Theta), \\ \theta' \in \text{Supp}(\mathcal{M}_g(\theta))}} \mathfrak{D}\left(\omega_{X_\theta} \| \omega_{X_{\theta'}}\right), \tag{2}$$

where $\text{Supp}(\cdot)$ is the support of the distribution and $\mathfrak{D}$ can be any general distance metric defined over distributions. In this paper, we specify the distance metric as Wasserstein-2 distance, as it is widely adopted in data quality estimation (e.g., [21]).

**Objective** The data holder's objective is to choose a data release mechanism that minimizes distortion metric $\Delta_{\mathcal{M}_g}$ subject to a privacy budget constraint on $\Pi_{\epsilon,\omega_\Theta}^{\text{union}}$:

$$\min_{\mathcal{M}_g} \quad \Delta_{\mathcal{M}_g} \qquad \text{subject to} \quad \Pi_{\epsilon,\omega_\Theta}^{\text{union}} \le T. \tag{3}$$

# 4 General Lower Bound on Privacy-Distortion Tradeoffs

Given the metrics defined in §3.1 and a privacy budget $T$, we present a lower bound on distortion that applies to any data distribution and any secret $\boldsymbol{g} = [g_1, g_2, \cdots, g_d]$.

**Theorem 4.1** (Lower bound of privacy-distortion tradeoff). *Let* $D(X_{\theta_1}, X_{\theta_2}) = \frac{1}{2}\mathfrak{D}\left(\omega_{X_{\theta_1}} \| \omega_{X_{\theta_2}}\right)$. *Further, let* $R^{union}(X_{\theta_1}, X_{\theta_2}) = \prod_{i \in [d]} |g_i(\theta_1) - g_i(\theta_2)|^{1/d}$ *and*

$$\gamma^{union} = \inf_{\theta_1, \theta_2 \in Supp(\omega_\Theta)} \frac{D(X_{\theta_1}, X_{\theta_2})}{R^{union}(X_{\theta_1}, X_{\theta_2})}. \tag{4}$$

4

Then, for tolerance ranges $\{\epsilon_i\}$ as defined in Eq. (1) and for any mechanism $\mathcal{M}_g$ subject to privacy budget $\Pi^{union}_{\epsilon,\omega_\Theta} \leq T < 1$, we have

$$\Delta_{\mathcal{M}_g} > 2\gamma^{union}\left\lceil \frac{1}{1 - (1-T)^{1/d}} - 1 \right\rceil \left(\prod\nolimits_{i\in[d]} \epsilon_i\right)^{1/d}. \tag{5}$$

The proof is shown in App. B.1, and we provide the proof sketch as below. Thm. 4.1 shows that the lower bound is proportional to the geometric mean of the tolerance ranges $\epsilon_1, \cdots, \epsilon_d$, and is *inversely* proportional to the privacy budget $T$. The ratio $\gamma^{union}$ acts as a conversion parameter that bridges the difficulty of guessing the secrets and the distributional disparity, and its value depends on secret types and data distribution. The impact of the secret number $d$ on the lower bound depends on the characteristics of secrets (i.e., $\gamma^{union}$) and their tolerance ranges (i.e., the geometric mean of tolerance ranges). However, as the ceiling term in Eq. (5) increases with the growth of secret number, achieving a lower value for the lower bound becomes much more challenging with a larger number of secrets. This aligns with intuition: with more secrets, the attacker can more easily succeed in guessing at least one secret. For the multi-shot attack scenario, where $g_1 = \cdots = g_d$ and $\epsilon_1 = \cdots = \epsilon_d$, the lower bound increases as the attacker's trial count $d$ grows.
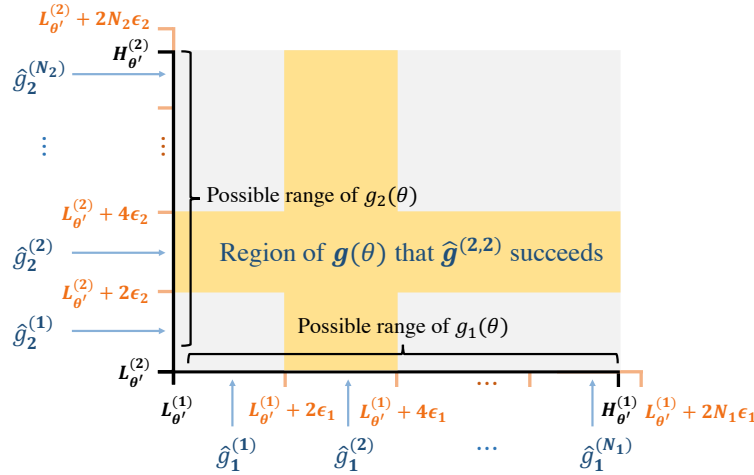


Figure 1: Attacker construction for proof of Thm. 4.1 under the 2-secret case. The true value of secret vector lies in the intersection of the highlighted bands.

**Proof Sketch** We prove the tradeoff lower bound Eq. (5) by constructing a sequence of attackers (agnostic of data distribution and release mechanism), such that some of them can successfully guess at least one secret. We take the 2-secret case (i.e., $d = 2$) as an example, as illustrated in Fig. 1. For each secret $g_i(\theta)$, we partition the range of possible secret values into $N_i$ segments of length $2\epsilon_i$ and design $N_i$ individual-secret attack strategies $\hat{g}_i^{(j)}$ ($j \in [N_i]$), each guessing the midpoint of a segment. We subsequently formulate multi-secret attack strategies $\hat{\boldsymbol{g}}^{(j,k)}$ ($j \in [N_1], k \in [N_2]$) by combining individual-secret strategy $\hat{g}_1^{(j)}$ for secret $g_1(\theta)$ and $\hat{g}_2^{(k)}$ for secret $g_2(\theta)$. Note that none of these attacks depends on a released parameter $\theta'$: the sequence is solely determined by the range of the secret. The yellow $\boldsymbol{g}(\theta)$ region in Fig. 1 represents where the attacker $\hat{\boldsymbol{g}}^{(2,2)}$ correctly guesses at least one secret within the tolerance range. We then establish the distortion lower bound based on the privacy constraint that the attack success rate is at most $T$ and by utilizing the conversion parameter $\gamma^{union}$, which serves as a linkage between the distributional distance and possible ranges of secrets.

## 5   Alternative Privacy Metrics and Analysis

In §3.1, we define the privacy metric for the worst case: attacker guessing any of the secrets within the tolerance range will result in the failure of secret protection. In practice, sensitive information is sometimes significantly compromised only when the attacker successfully guesses all or a group of secrets. Consider, e.g., a dataset containing the ingredients purchase logs belonging to a pharmaceutical (or food product) company. The company may be concerned about its trade secrets (e.g. drug formula or recipe) being leaked based on the average monthly purchase amounts for the ingredients. However, in this case the company may consider its trade secret revealed only if all (or most) of the ingredient ratios are disclosed, rather than the absolute values for one or a few ingredients. In this section, we propose alternative privacy metrics that apply to such scenarios. We discuss a further variant metric ($l_p$ privacy metric) in App. D.

## 5.1 Intersection Summary Statistic Privacy

We first consider the scenario where secrets are considered compromised only when the attacker successfully guesses *all* of them simultaneously. We define the *intersection privacy* metric as the probability of attacker guessing all secrets within their respective tolerance ranges, $\epsilon_i$ for secret $g_i$, employing the best attacker strategy:

$$\Pi_{\epsilon,\omega_\Theta}^{\text{inter}} \triangleq \sup_{\hat{\boldsymbol{g}}} \ \mathbb{P}\left(\bigcap_{i\in[d]} |\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i\right). \tag{6}$$

The following theorem presents a lower bound on distortion, given intersection privacy budget $T$.

**Theorem 5.1** (Lower bound of privacy-distortion tradeoff for intersection privacy). *Let* $D(X_{\theta_1}, X_{\theta_2}) = \frac{1}{2}\mathfrak{D}\left(\omega_{X_{\theta_1}} \| \omega_{X_{\theta_2}}\right)$. *Further, let* $R^{inter}(X_{\theta_1}, X_{\theta_2}) = \frac{1}{d}\sum_{i\in[d]}|g_i(\theta_1) - g_i(\theta_2)|$ *and*

$$\gamma^{inter} = \inf_{\theta_1,\theta_2\in Supp(\omega_\Theta)} \frac{D(X_{\theta_1}, X_{\theta_2})}{R^{inter}(X_{\theta_1}, X_{\theta_2})}. \tag{7}$$

*Then, for tolerance ranges* $\{\epsilon_i\}$ *as defined in Eq. (6) and for any mechanism* $\mathcal{M}_g$ *subject to privacy budget* $\Pi_{\epsilon,\omega_\Theta}^{inter} \leq T < 1$, *we have*

$$\Delta_{\mathcal{M}_g} > 2\gamma^{inter}\left(\left\lceil \frac{1}{T}\right\rceil^{1/d}\Big(\prod_{i\in[d]}\epsilon_i\Big)^{1/d} - \frac{1}{d}\sum_{i\in[d]}\epsilon_i\right). \tag{8}$$

(Proof in App. B.2.) As the secret number $d$ increases, Thm. 5.1 shows that achieving a lower value for the distortion lower bound becomes easier, which aligns with intuition: with more secrets, it becomes increasingly challenging for the attacker to succeed in guessing all secrets. Since intersection privacy is the least strict privacy metric for the data holder, its least achievable distortion is no greater than that for union privacy, as demonstrated in Prop. 5.2 (proof in App. B.3).

**Proposition 5.2.** *Given a privacy budget $T$ and tolerance ranges* $\epsilon_1, \cdots, \epsilon_d$, *we have* $\Delta^{union} \geq \Delta^{inter}$, *where* $\Delta^{union}$ *and* $\Delta^{inter}$ *are the achievable distortion lower bounds for union privacy and intersection privacy.*

## 5.2 Group Secrets Summary Statistic Privacy

We then consider the case where the data holder divides secrets into distinct groups, aiming to thwart the attacker from successfully guessing an entire group of secrets. We define the *group secrets privacy* metric as the probability of attacker guessing any disjoint group $b = \{g_i\}_{i\in\mathcal{I}_b} \in \mathcal{B}$ of secrets to within tolerance ranges, $\epsilon_i$ for secret $g_i$, adopting the best attack strategy:

$$\Pi_{\epsilon,\omega_\Theta}^{\text{group}} \triangleq \sup_{\hat{\boldsymbol{g}}} \ \mathbb{P}\left(\bigcup_{b\in\mathcal{B}}\left(\bigcap_{i\in\mathcal{I}_b}|\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i\right)\right), \tag{9}$$

where the secret index set $\mathcal{I}_b$ satisfies $\mathcal{I}_{b_1} \cap \mathcal{I}_{b_2} = \emptyset$ for any distinct group $b_1, b_2 \in \mathcal{B}$. Note that when $|\mathcal{B}| = 1$, group secrets privacy reduces to intersection privacy, the least strict privacy metric. On the other hand, for $|\mathcal{B}| = d$, group secrets privacy is equivalent to union privacy, the strictest metric.

Under group secrets privacy, given a privacy budget $T$, we then present a general lower bound on distortion.

**Theorem 5.3** (Lower bound of privacy-distortion tradeoff for group secrets privacy). *Let* $D(X_{\theta_1}, X_{\theta_2}) = \frac{1}{2}\mathfrak{D}\left(\omega_{X_{\theta_1}} \| \omega_{X_{\theta_2}}\right)$. *Further, let* $R^{group}(X_{\theta_1}, X_{\theta_2}) = \frac{1}{d}\sum_{i\in[d]}|g_i(\theta_1) - g_i(\theta_2)|$ *and*

$$\gamma^{group} \triangleq \inf_{\theta_1,\theta_2\in Supp(\omega_\Theta)} \frac{D(X_{\theta_1}, X_{\theta_2})}{R^{group}(X_{\theta_1}, X_{\theta_2})}. \tag{10}$$

*Then, for tolerance ranges* $\{\epsilon_i\}$ *as defined in Eq. (9) and for any mechanism* $\mathcal{M}_g$ *subject to privacy budget* $\Pi_{\epsilon,\omega_\Theta}^{group} \leq T < 1$, *we have*

$$\Delta_{\mathcal{M}_g} > 2\gamma^{group}\left(\left\lceil \frac{1}{\left(1-(1-T)^{1/\beta}\right)^{\beta/d}}\right\rceil \prod_{i\in[d]}\epsilon_i^{1/d} - \sum_{i\in[d]}\frac{\epsilon_i}{d}\right),$$

*where $\beta$ is the number of groups, i.e., $\beta = |\mathcal{B}|$.*

(Proof in App. B.4.) We can observe that the distortion lower bound in Thm. 5.3 is proportional to the group number $\beta$.

# 6 A Case Study: Multivariate Gaussian

In this section, we instantiate the general privacy-distortion tradeoff result from §4 on Gaussian distributions with multiple secrets, devise a data release mechanism, and assess its privacy-distortion performance under union privacy. We defer the case studies and mechanism analysis under other privacy metrics in §5 to App. F.

We focus on $k$-dimensional Gaussian distribution ($k \in \mathbb{Z}^+$) with independent variables (i.e., with diagonal covariance matrix), represented by distribution parameters $\theta = (\mu_1, \cdots, \mu_k, \sigma_1, \cdots, \sigma_k)$. We defer the analysis of the general case of multivariate Gaussian distributions to App. E. We aim to protect $d$ secrets ($d \leq 2k$), where each secret can represent either mean or standard deviation of any dimension within the distribution, i.e., $g_i \in \{\mu_1, \cdots, \mu_k, \sigma_1, \cdots, \sigma_k\}, \forall i \in [d]$. We first instantiate the privacy-distortion lower bound for union privacy in Prop. 6.1.

**Proposition 6.1.** *For $k$-dimensional Gaussian distribution with diagonal covariance matrix and distribution parameters $\theta = (\mu_1, \cdots, \mu_k, \sigma_1, \cdots, \sigma_k)$, consider $d$ secrets ($d \leq 2k$), where each secret satisfies $g_i(\theta) \in \{\mu_1, \cdots, \mu_k, \sigma_1, \cdots, \sigma_k\}, \forall i \in [d]$. Then, for tolerance ranges $\{\epsilon_i\}$ as defined in Eq. (1) and for any mechanism $\mathcal{M}_g$ subject to privacy budget $\Pi_{\epsilon,\omega_\Theta}^{union} \leq T < 1$, we have*

$$\Delta_{\mathcal{M}_g} > \sqrt{d} \cdot \left\lceil \frac{1}{1 - (1-T)^{1/d}} - 1 \right\rceil \cdot \left( \prod\nolimits_{i \in [d]} \epsilon_i \right)^{1/d}.$$

(Proof in App. B.5.) Next, we design a quantization mechanism to approximate the tradeoff lower bound. Quantization mechanisms have been shown to achieve (near)-optimal privacy-utility tradeoffs across various privacy pipelines, as evidenced by [25, 11]. Intuitively, we partition the ranges of possible secret values into intervals of lengths $s_{g_i}$ for each secret $g_i$, $i \in [d]$. The mechanism randomly outputs a point within the intervals where the original secrets reside. Precisely, we provide the mechanism in Alg. 1, where $U$ stands for uniform distribution.

---

**Algorithm 1:** Data release mechanism for dimensionally independent multivariate Gaussian with $d$ secrets.

**Input:** $\theta = (\mu_1, \cdots, \mu_k, \sigma_1, \cdots, \sigma_k)$, lower bound $\underline{g_i}$ for secret $g_i$, quantization interval $s_{g_i}, \forall i \in [d]$.

1 **for** each $i \in [d]$: $g_i'(\theta) \leftarrow \underline{g_i} + \lfloor \frac{g_i(\theta) - \underline{g_i}}{s_{g_i}} \rfloor \cdot s_{g_i} + U(0, s_{g_i})$;

2 Output Gaussian distribution with secret parameter $g_i$ as $g_i'(\theta), \forall i \in [d]$, and non-secret parameters as the original values.

---

For the mechanism performance analysis, we consider the union privacy and assume that the prior distribution of each secret distribution parameter $g_i, i \in [d]$, is uniform.

**Proposition 6.2** (Mechanism privacy-distortion tradeoff). *Assume that secret distribution parameters $g_1, \cdots, g_d$ follow uniform distributions. Let $_{Alg.1}\Pi_{\epsilon,\omega_\Theta}^{union}$ denote the union privacy risk of Alg. 1. Then, we have*

$$_{Alg.1}\Pi_{\epsilon,\omega_\Theta}^{union} = 1 - \prod\nolimits_{i \in [d]} \left( 1 - \frac{2\epsilon_i}{s_{g_i}} \right), \qquad \Delta_{Alg.1} = \sqrt{\sum\nolimits_{i \in [d]} s_{g_i}^2} < c_{\epsilon,s} \cdot \Delta_{opt},$$

*where $c_{\epsilon,s}$ is a constant depending on the tolerance ranges and interval lengths of the mechanism, and $\Delta_{opt}$ is the achievable distortion lower bound under the privacy budget $T = {}_{Alg.1}\Pi_{\epsilon,\omega_\Theta}^{union}$.*

(Proof in App. B.6.) From Prop. 6.2 we know that Alg. 1 achieves order-optimal privacy-distortion performance with a constant multiplication factor.

**The case of unknown distribution parameters** In the sections above, we introduced release mechanisms for the case where the data holder knows the distribution parameters of the dataset. In practice, the data

holder may only possess a dataset without knowing its underlying distribution's parameters. Our data release mechanisms can be easily extended to this case where the input and the output of the mechanism are datasets. Briefly, the data holder estimates the parameters $\theta$ from the data and maps them to corresponding intervals. Once the released parameters $\theta'$ are determined, each sample is adjusted to conform to the distribution characterized by $\theta'$. We provide an example in App. G to demonstrate the extension process.

# 7   Experiments

In this section, we employ real-world dataset to illustrate the variations in privacy-distortion tradeoffs across different privacy metrics and present the privacy-distortion performance of our mechanism. We include more results on alternative metrics and scalability of our mechanism in App. H.

**Metrics**  Our privacy and distortion metrics require the knowledge of prior distribution $\omega_\Theta$ of the distribution parameters, which cannot be obtained in practice since the data holder can only have one dataset. Consequently, we need to design surrogate privacy and distortion metrics to bound the real privacy and distortion values in experiments.

*Surrogate privacy metric.* For the original and the released datasets $\mathcal{X}$ and $\mathcal{X}'$, we define the surrogate metric for union privacy as

$$\tilde{\Pi}^{\text{union}}_{\epsilon,\omega_\Theta} = \max_{i\in[d]} \left\{ -|g_i(\mathcal{X}) - \hat{g}_i(\mathcal{X}')|/\epsilon_i \right\},$$

where $g_i(\cdot)$ is the $i$-th secret of the dataset, and $\epsilon_i$ is the tolerance range of the $i$-th secret. We measure privacy by the difference between the secrets of the original and released datasets, using the negative sign to ensure that a smaller value signifies stronger privacy. Given varying tolerance ranges for different secrets, we use $\epsilon_i$ in the denominator to normalize the difference. For union privacy, the data holder aims to prevent the estimation of any secret, and therefore, we take the maximal privacy value over all secrets (i.e., worst case privacy). Note that when the prior distribution $\omega_\Theta$ is uniform, guessing the $i$-th secret as $\hat{g}_i(\mathcal{X}')$ is the optimal attack strategy under Alg. 1. Therefore, there is a mapping between $\Pi^{\text{union}}_{\epsilon,\omega_\Theta}$ and $\tilde{\Pi}^{\text{union}}_{\epsilon,\omega_\Theta}$, making the surrogate a suitable approximation of $\Pi^{\text{union}}_{\epsilon,\omega_\Theta}$.

Similarly, we define surrogate metrics for intersection privacy and group secrets privacy as

$$\tilde{\Pi}^{\text{inter}}_{\epsilon,\omega_\Theta} = \min_{i\in[d]} \left\{ -|g_i(\mathcal{X}) - g_i(\mathcal{X}')|/\epsilon_i \right\}, \quad \tilde{\Pi}^{\text{group}}_{\epsilon,\omega_\Theta} = \max_{b\in\mathcal{B}} \left\{ \min_{i\in\mathcal{I}_b} \left\{ -|g_i(\mathcal{X}) - g_i(\mathcal{X}')|/\epsilon_i \right\} \right\},$$

where $\mathcal{B}$ represents the set of groups for group secrets privacy, and $\mathcal{I}_b$ is the index set for group $b$.

*Surrogate distortion metric.* We define the surrogate distortion metric as the Wasserstein-2 distance between the original and the released dataset:

$$\tilde{\Delta}_{\mathcal{M}_g} = \mathfrak{D}_{\text{Wasserstein-2}}(\omega_\mathcal{X} \| \omega_{\mathcal{X}'}),$$

where $\omega_\mathcal{D}$ is the empirical distribution of dataset $\mathcal{D}$.

**Dataset**  We adopt Wikipedia Web Traffic Dataset (WWT) [18] (license: CC0: Public Domain) to simulate the motivating scenarios. WWT contains daily page views of 117,277 Wikipedia web pages in 2015-2016. Our goal is to release the page views (i.e., a $365 \times 117{,}277$-dimensional dataset) while protecting the average daily page views of three websites (i.e., secrets are the means of three dimensions within data), which are $15, 68, 54$ respectively.

**Baselines**  We compare our quantization mechanism Alg. 1 with three widely-adopted privacy-preserving mechanisms: differentially-private density estimation [40] (abbreviated as DP), attribute-private Gaussian mechanism [42] (abbreviated as AP), and distribution-private Laplacian mechanism [19] (abbreviated as DistP). DP works by partitioning the space into bins to construct a histogram of the dataset, adding zero-mean Laplacian noise to the histogram, and releasing samples drawing from the obfuscated histogram. AP works by adding zero-mean Gaussian noise to each sample. DistP works by adding zero-mean Laplacian noise to each sample.

**Empirical Results**  For union, intersection, and group secrets privacy, we set the tolerance ranges of three secrets as $\epsilon_1 = 1, \epsilon_2 = 4, \epsilon_3 = 3$, according to their respective average page views. For group secrets privacy, we cluster the first two means as a group and consider the last mean separately.

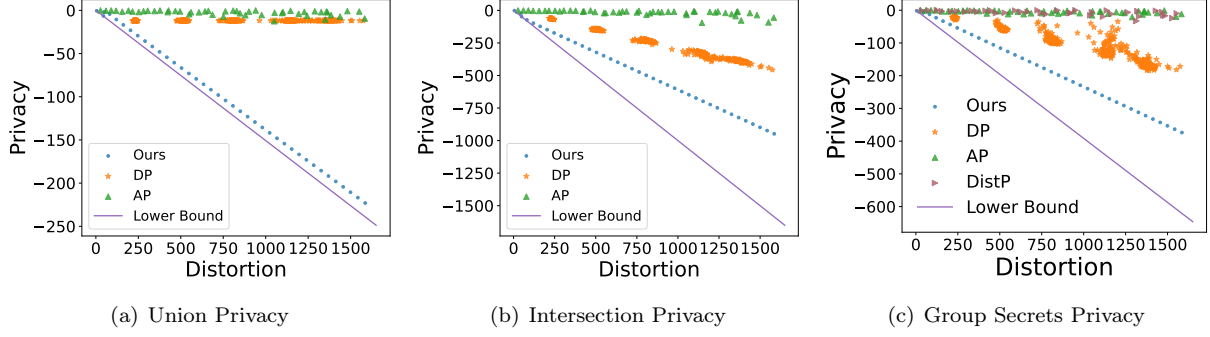(a) Union Privacy      (b) Intersection Privacy      (c) Group Secrets Privacy

Figure 3: Privacy and distortion (lower values are better) of DP, AP, DistP, and ours under different privacy metrics. The solid line represents the theoretical lower bound of achievable region.

Under different privacy metrics, we first calculate the surrogate distortion and privacy values of Alg. 1. The results are shown in Fig. 2, where each point represents a realization of the mechanism with different interval lengths. Different levels of distortion are obtained by varying the bin size. Each solid line in Fig. 2 represents a theoretical privacy-distortion lower bound with secrets as three means for a specific surrogate privacy metric. Such theoretical analysis does not require any assumptions on the data distribution (details in App. B.7). From Fig. 2, we can observe that:
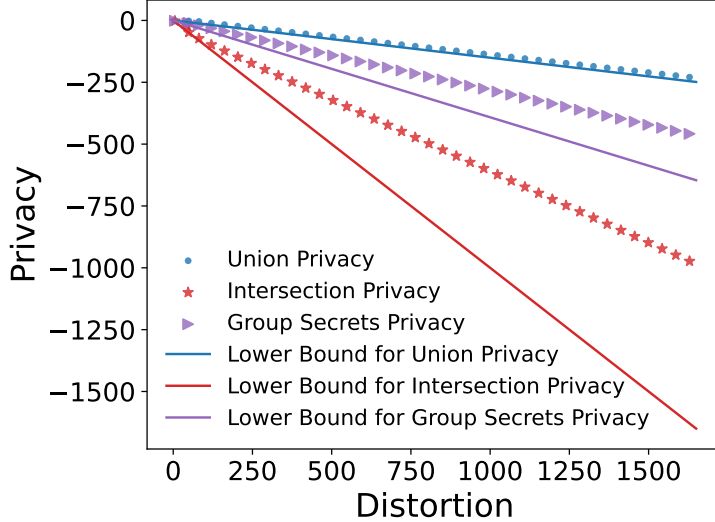


Figure 2: Privacy (lower is better) and distortion of Alg. 1 under WWT with different privacy metrics. For each metric, the solid line with the same color represents the theoretical lower bound.

*(1) The privacy-distortion tradeoffs of Alg. 1 match the theoretical lower bounds (or with a mild gap) even the distribution assumption does not hold.* For union privacy (color in blue), the privacy-distortion tradeoffs of Alg. 1 match the theoretical lower bounds. For the other privacy metrics, regardless of the privacy budget, the distortion of Alg. 1 approximates the theoretical lower bound with a multiplication factor smaller than 2. The results indicate that without assumptions on distribution type, our mechanism still achieves order-optimal privacy-distortion performance on real-world dataset.

*(2) The discrepancies in privacy-distortion tradeoffs across different privacy metrics align with our theoretical results.* Under a certain realization of Alg. 1 (i.e., with a fixed distortion), union privacy achieves the highest value, while intersection privacy is the lowest, reflecting the strictest and mildest metrics, respectively.

We then compare the privacy-distortion tradeoffs between DP, AP, DistP, and our mechanism under different privacy metrics in Fig. 3. Each point represents a realization of data release mechanism with one hyper-parameter (bin size and noise level for DP, noise level for AP and DistP, interval length for ours). We can observe that *our quantization mechanism achieves better privacy-distortion tradeoffs under different privacy metrics.* AP and DistP add noise to individual samples, which has less effect on means, and therefore achieves the worst privacy-distortion tradeoffs. DP instead adds noise to the histograms after the space quantization, which could protect the means more efficiently. However, since the added noise is unbounded, the privacy-distortion tradeoffs are still worse than our quantization mechanism.

# 8    Conclusion and Future Work

We introduce a framework to quantify, analyze, and protect multi-secret summary statistic privacy in data sharing. To accommodate varying data sharing scenarios, we propose and compare several privacy metrics, analyzing the tradeoff between privacy and distortion under each metric. For data release mechanism design, we propose a quantization-based mechanism and demonstrate its order-optimal privacy-distortion performance in certain settings, both theoretically and empirically.

Our proposed privacy metrics rely on the prior distribution of parameters $\omega_\Theta$, which may not be known in practice. Motivated by *maximal leakage* [17], an avenue for future work is to extend the privacy metrics by considering the worst-case leakage over all possible priors. Moreover, while we provide analysis of the adaptive composition property of summary statistic privacy under a specific setting in App. I, we leave the comprehensive composition analysis under the general setting to future work. Extending our quantization-based release mechanism to scenarios beyond those studied in this work is another promising direction we hope to investigate in the future.

**Disclaimer** This paper was prepared for informational purposes in part by the CDAO group of JPMorgan Chase & Co and its affiliates ("J.P. Morgan") and is not a product of the Research Department of J.P. Morgan. J.P. Morgan makes no representation and warranty whatsoever and disclaims all liability, for the completeness, accuracy or reliability of the information contained herein. This document is not intended as investment research or investment advice, or a recommendation, offer or solicitation for the purchase or sale of any security, financial instrument, financial product or service, or to be used in any way for evaluating the merits of participating in any transaction, and shall not constitute a solicitation under any jurisdiction or to any person, if such solicitation under such jurisdiction or to such person would be unlawful.

# References

[1] Nazmiye Ceren Abay, Yan Zhou, Murat Kantarcioglu, Bhavani Thuraisingham, and Latanya Sweeney. Privacy preserving synthetic data release using deep learning. In *Machine Learning and Knowledge Discovery in Databases: European Conference, ECML PKDD 2018, Dublin, Ireland, September 10–14, 2018, Proceedings, Part I 18*, pages 510–526. Springer, 2019.

[2] Mário S Alvim, Konstantinos Chatzikokolakis, Annabelle McIver, Carroll Morgan, Catuscia Palamidessi, and Geoffrey Smith. Additive and multiplicative notions of leakage, and their capacities. In *2014 IEEE 27th Computer Security Foundations Symposium*, pages 308–322. IEEE, 2014.

[3] Shahab Asoodeh, Mario Diaz, Fady Alajaji, and Tamás Linder. Privacy-aware guessing efficiency. In *2017 ieee international symposium on information theory (isit)*, pages 754–758. IEEE, 2017.

[4] Shahab Asoodeh, Mario Diaz, Fady Alajaji, and Tamás Linder. Estimation efficiency under privacy constraints. *IEEE Transactions on Information Theory*, 65(3):1512–1534, 2018.

[5] Boaz Barak, Kamalika Chaudhuri, Cynthia Dwork, Satyen Kale, Frank McSherry, and Kunal Talwar. Privacy, accuracy, and consistency too: a holistic solution to contingency table release. In *Proceedings of the twenty-sixth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, pages 273–282, 2007.

[6] Flavio P Calmon, Ali Makhdoumi, and Muriel Médard. Fundamental limits of perfect privacy. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 1796–1800. IEEE, 2015.

[7] Michelle Chen and Olga Ohrimenko. Protecting global properties of datasets with distribution privacy mechanisms. In *International Conference on Artificial Intelligence and Statistics*, pages 7472–7491. PMLR, 2023.

[8] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006. Proceedings 3*, pages 265–284. Springer, 2006.

[9] Khaled El Emam and Fida Kamal Dankar. Protecting privacy using k-anonymity. *Journal of the American Medical Informatics Association*, 15(5):627–637, 2008.

[10] Mark Elliot and Angela Dale. Scenarios of attack: the data intruder's perspective on statistical disclosure risk. *Netherlands Official Statistics*, 14(Spring):6–10, 1999.

[11] Farhad Farokhi. Noiseless privacy: Definition, guarantees, and applications. *IEEE Transactions on Big Data*, 2021.

[12] Simson Garfinkel et al. *De-identification of Personal Information:*. US Department of Commerce, National Institute of Standards and Technology, 2015.

[13] Arpita Ghosh and Robert Kleinberg. Inferential privacy guarantees for differentially private mechanisms. *arXiv preprint arXiv:1603.01508*, 2016.

[14] Atefeh Gilani, Gowtham R Kurri, Oliver Kosut, and Lalitha Sankar. $(\alpha, \beta)$-leakage: A unified privacy leakage measure. *arXiv preprint arXiv:2304.07456*, 2023.

[15] Clark R Givens and Rae Michael Shortt. A class of wasserstein metrics for probability distributions. *Michigan Mathematical Journal*, 31(2):231–240, 1984.

[16] Anco Hundepool, Josep Domingo-Ferrer, Luisa Franconi, Sarah Giessing, Rainer Lenz, Jane Longhurst, E Schulte Nordholt, Giovanni Seri, and P Wolf. Handbook on statistical disclosure control. *ESSnet on Statistical Disclosure Control*, 2010.

[17] Ibrahim Issa, Aaron B Wagner, and Sudeep Kamath. An operational approach to information leakage. *IEEE Transactions on Information Theory*, 66(3):1625–1657, 2019.

[18] Kaggle. Wikipedia web traffic 2018-19. https://www.kaggle.com/datasets/sandeshbhat/wikipedia-web-traffic-201819.

[19] Yusuke Kawamoto and Takao Murakami. Local obfuscation mechanisms for hiding probability distributions. In *European Symposium on Research in Computer Security*, pages 128–148. Springer, 2019.

[20] Daniel Kifer and Ashwin Machanavajjhala. Pufferfish: A framework for mathematical privacy definitions. *ACM Transactions on Database Systems (TODS)*, 39(1):1–36, 2014.

[21] Alexander Korotin, Lingxiao Li, Aude Genevay, Justin M Solomon, Alexander Filippov, and Evgeny Burnaev. Do neural optimal transport solvers work? a continuous wasserstein-2 benchmark. *Advances in Neural Information Processing Systems*, 34:14593–14605, 2021.

[22] Gowtham R Kurri, Lalitha Sankar, and Oliver Kosut. An operational approach to information leakage via generalized gain functions. *arXiv preprint arXiv:2209.13862*, 2022.

[23] Hau L Lee and Seungjin Whang. Information sharing in a supply chain. *International journal of manufacturing technology and management*, 1(1):79–93, 2000.

[24] Jiachun Liao, Oliver Kosut, Lalitha Sankar, and Flavio du Pin Calmon. Tunable measures for information leakage and applications to privacy-utility tradeoffs. *IEEE Transactions on Information Theory*, 65(12):8043–8066, 2019.

[25] Zinan Lin, Shuaiqi Wang, Vyas Sekar, and Giulia Fanti. Summary statistic privacy in data sharing. *IEEE Journal on Selected Areas in Information Theory*, 2024.

[26] Ali Makhdoumi, Salman Salamatian, Nadia Fawaz, and Muriel Médard. From the information bottleneck to the privacy funnel. In *2014 IEEE Information Theory Workshop (ITW 2014)*, pages 501–505. IEEE, 2014.

[27] S Alvim M'rio, Kostas Chatzikokolakis, Catuscia Palamidessi, and Geoffrey Smith. Measuring information leakage using generalized gain functions. In *2012 IEEE 25th Computer Security Foundations Symposium*, pages 265–279. IEEE, 2012.

[28] Arvind Narayanan and Vitaly Shmatikov. How to break anonymity of the netflix prize dataset. *arXiv preprint cs/0610105*, 2006.

[29] Vamsi K. Potluru, Daniel Borrajo, Andrea Coletta, Niccolò Dalmasso, Yousef El-Laham, Elizabeth Fons, Mohsen Ghassemi, Sriram Gopalakrishnan, Vikesh Gosai, Eleonora Kreačić, Ganapathy Mani, Saheed Obitayo, Deepak Paramanand, Natraj Raman, Mikhail Solonin, Srijan Sood, Svitlana Vyetrenko, Haibei Zhu, Manuela Veloso, and Tucker Balch. Synthetic data applications in finance. *arXiv preprint arXiv:2401.00081*, 2024.

[30] Wahbeh Qardaji, Weining Yang, and Ninghui Li. Priview: practical differentially private release of marginal contingency tables. In *Proceedings of the 2014 ACM SIGMOD international conference on Management of data*, pages 1435–1446, 2014.

[31] Borzoo Rassouli and Deniz Gündüz. On perfect privacy. *IEEE Journal on Selected Areas in Information Theory*, 2(1):177–191, 2021.

[32] Charles Reiss, John Wilkes, and Joseph L Hellerstein. Obfuscatory obscanturism: making workload traces of commercially-sensitive systems safe to release. In *2012 IEEE Network Operations and Management Symposium*, pages 1279–1286. IEEE, 2012.

[33] Sara Saeidian, Giulia Cervia, Tobias J Oechtering, and Mikael Skoglund. Pointwise maximal leakage. *IEEE Transactions on Information Theory*, 2023.

[34] Geoffrey Smith. On the foundations of quantitative information flow. In *International Conference on Foundations of Software Science and Computational Structures*, pages 288–302. Springer, 2009.

[35] Geoffrey Smith. Recent developments in quantitative information flow (invited tutorial). In *2015 30th Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 23–31. IEEE, 2015.

[36] Anshuman Suri and David Evans. Formalizing and estimating distribution inference risks. *arXiv preprint arXiv:2109.06024*, 2021.

[37] Anshuman Suri, Yifu Lu, Yanjin Chen, and David Evans. Dissecting distribution inference. In *2023 IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)*, pages 150–164. IEEE, 2023.

[38] Latanya Sweeney. Matching known patients to health records in washington state data. *arXiv preprint arXiv:1307.1370*, 2013.

[39] Robert E Tillman, Tucker Balch, and Manuela Veloso. Privacy-preserving energy-based generative models for marginal distribution protection. *Transactions on Machine Learning Research*, 2023.

[40] Larry Wasserman and Shuheng Zhou. A statistical framework for differential privacy. *Journal of the American Statistical Association*, 105(489):375–389, 2010.

[41] Amirreza Zamani, Tobias J Oechtering, and Mikael Skoglund. Bounds for privacy-utility trade-off with non-zero leakage. In *2022 IEEE International Symposium on Information Theory (ISIT)*, pages 620–625. IEEE, 2022.

[42] Wanrong Zhang, Olga Ohrimenko, and Rachel Cummings. Attribute privacy: Framework and mechanisms. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, pages 757–766, 2022.

[43] Xu Zheng and Zhipeng Cai. Privacy-preserved data sharing towards multiple parties in industrial iots. *IEEE Journal on Selected Areas in Communications*, 38(5):968–979, 2020.

# Appendix

## Contents

# A   Related Works

**Heuristics**   While heuristics are widely adopted in industries for data sharing [16], many lack theoretical privacy guarantees and can be vulnerable in real-world scenarios [10]. For example, *subsetting* aims to protect sensitive information by only selecting a part of available data to release [32]. However, sub-sampling data will not change the data distribution, and thus the statistical properties are still preserved. *Culling* and *de-identification* remove certain attributes of the dataset [32], but they may excise too much information and are risked from re-identification attacks based on side information or cross-attribute correlations [28, 38, 9].

**Indistinguishability Methods**   *Differential privacy* (DP) [8] is one of the most widely adopted privacy metric, and it provides privacy by ensuring that any two input neighboring datasets are indistinguishable. However, DP cannot be directly applied to protect summary statistic secrets as it aims to protect whether an individual record (or group) contribute to the released data, rather than to hide statistical properties of a distribution. For example, typical DP or Local DP approaches like Laplacian mechanism [8, 40] would add zero mean noise to each sample. Obfuscating data in such way will not change statistical properties like the mean of the distribution on expectation. While several works have applied DP to release summary statistics[5, 30], the problems they address do not align with typical data sharing scenarios, as those methods only provide a synopsis of the dataset.

Motivating by differential privacy, several works proposed approaches aiming to make pairs of datasets or distributions with similar summary statistic secrets indistinguishable [42, 13, 7, 36]. *Attribute privacy* [42] also aims to protect properties of the dataset and parameters of the underlying distribution from which dataset is sampled, but not under the data sharing scenarios. Adopting the Pufferfish privacy framework [20], the paper designed mechanisms ensuring indistinguishablility. However, the attribute privacy framework only outputs certain statistical query, rather than releases the dataset, making it not suitable for data sharing. *Distribution privacy* [19] and *distribution inference* [36, 37] also share the similar goal of protecting statistical secrets of the data. Roughly, they design indistinguishably mechanisms ensuring that the output distribution are similar for any input distribution with similar statistical secrets. Since we only aim to hide certain statistics rather than the whole distribution, this framework is far stronger than what we need and will cause worse utility. Totally different distributions may have similar statistics (e,g, a Dirac delta distribution and a Gaussian distribution may have the same mean), and prohibitive noise should be added to make the whole distributions indistinguishable.

**Leakage-Based Methods**   Another category of works adopt information theoretic approaches to define and protect statistical privacy. Typically, works in this category aim to limit the disclosure of private information while maximizing disclosure of others. Specifically, those works quantify disclosure of sensitive information by the notion of leakage [2, 35]. Leakage can be defined by various of measures, such as Shannon entropy [26, 31, 41, 6], min-entropy [3, 4, 34], and gain function [27, 2, 24, 33]. One important theme is the development of leakage measures with operational significance [2]. *Maximal leakage* [17], an operationally-interpretable and robust measure, has been proposed recently. Maximal leakage is defined as the increase of the probability of correctly guessing the secrets after observing the released dataset. However, maximal leakage and its generalizations (e.g., [14, 22]) are unsuitable to our scenario since they assume the secrets to protect are not known in advance and therefore take the worst-case leakage over all possible secrets.

# B   Proofs

## B.1   Proof of Thm. 4.1

*Proof.* We prove the tradeoff lower bound by constructing a sequence of attackers guessing different possible secrets values, such that there exists attackers guessing at least one secret successfully. Specifically, for each secret, we divide the range of possible secret values into segments, and design a series of individual-secret attack strategies, guessing the midpoint of each segment. We subsequently formulate multi-secret attack strategies by choosing one individual-secret strategy for each secret. We then establish the distortion lower bound based on the privacy constraint that the attack success rate is at most $T$ and by utilizing the conversion parameter $\gamma^{\mathrm{union}}$ that serves as a linkage between the distributional distance and the distance between secrets.

$$T \geq \Pi_{\epsilon,\omega_\Theta}^{\mathrm{union}}$$

$$= \sup_{\hat{g}} \ \mathbb{P}\left( \bigcup_{i \in [d]} |\hat{g}_i\left(\theta'\right) - g_i\left(\theta\right)| \leq \epsilon_i \right)$$

$$= \sup_{\hat{g}} \mathbb{E}\left( \mathbb{P}\left( \bigcup_{i \in [d]} |\hat{g}_i\left(\theta'\right) - g_i\left(\theta\right)| \leq \epsilon_i \middle| \theta' \right) \right)$$

$$= \mathbb{E}\left( \sup_{\hat{g}} \mathbb{P}\left( \bigcup_{i \in [d]} |\hat{g}_i\left(\theta'\right) - g_i\left(\theta\right)| \leq \epsilon_i \middle| \theta' \right) \right) \ , \tag{11}$$

where Eq. (11) is due to the fact that $\hat{g}$ only depends on $\theta'$ and therefore one can devise an attacker that for each $\theta'$, performs the optimal attack. It follows from Eq. (11) there exists $\theta'$ s.t. $\sup_{\hat{g}} \mathbb{P}\left( \bigcup_{i \in [d]} |\hat{g}_i\left(\theta'\right) - g_i\left(\theta\right)| \leq \epsilon_i \middle| \theta' \right) \leq T$. For any $i \in [d]$, let $L_{\theta'}^{(i)}$ and $H_{\theta'}^{(i)}$ be the smallest and the largest possible value of secret $g_i$ given the released distribution parameter $\theta'$:

$$L_{\theta'}^{(i)} \triangleq \inf_{\theta \in \mathrm{Supp}(\omega_\Theta):\mathcal{M}_g(\theta)=\theta'} g_i\left(\theta\right) \ ,$$

$$H_{\theta'}^{(i)} \triangleq \sup_{\theta \in \mathrm{Supp}(\omega_\Theta):\mathcal{M}_g(\theta)=\theta'} g_i\left(\theta\right) \ .$$

For each secret $g_i$, where $i \in [d]$, we partition the range of possible secret values, i.e., $[L_{\theta'}^{(i)}, H_{\theta'}^{(i)}]$, into segments with length $2\epsilon_i$. Subsequently, we develop a set of individual-secret attack strategies by guessing the midpoint of each segment. As a result, the number of individual-secret attack strategies, denoted as $N_i$, satisfies $L_{\theta'}^{(i)} + 2N_i\epsilon_i \geq H_{\theta'}^{(i)} > L_{\theta'}^{(i)} + 2(N_i - 1)\epsilon_i$.

We then construct multi-secret attack strategies by selecting one individual-secret strategy for each secret. For the multi-secret attack strategy $\hat{\boldsymbol{g}}^{(\boldsymbol{v})}$, where $\boldsymbol{v} = [v_1, v_2, \cdots, v_d]$ and $v_i \in [N_i]$ for all $i \in [d]$, it guesses the secret $g_i$ as the midpoint of the $v_i$-th segment, i.e., $\hat{g}_i^{[\boldsymbol{v}]}\left(\theta'\right) = L_{\theta'}^{(i)} + (v_i - 0.5) \cdot 2\epsilon_i$. The number of multi-secret attack strategies, denoted as $\mathcal{N}$, is $\mathcal{N} = \prod_{i \in [d]} N_i$. We can get that

$$T \cdot \mathcal{N} \geq \sum_{\boldsymbol{v}} \mathbb{P}\left( \bigcup_{i \in [d]} |\hat{g}_i^{[\boldsymbol{v}]}\left(\theta'\right) - g_i\left(\theta\right)| \leq \epsilon_i \middle| \theta' \right)$$

$$\stackrel{1}{=} \sum_{\boldsymbol{v}} \sum_{j \in [d]} (-1)^{j-1} \sum_{\substack{i_1 < i_2 < \cdots < i_j \\ i_1, i_2, \cdots, i_j \in [d]}} \mathbb{P}\left( \bigcap_{i \in \{i_1, i_2, \cdots, i_j\}} |\hat{g}_i^{[\boldsymbol{v}]}\left(\theta'\right) - g_i\left(\theta\right)| \leq \epsilon_i \middle| \theta' \right)$$

$$\stackrel{2}{\geq} \sum_{j \in [d]} (-1)^{j-1} \sum_{\substack{i_1 < i_2 < \cdots < i_j \\ i_1, i_2, \cdots, i_j \in [d]}} \frac{\mathcal{N}}{\prod_{k \in \{i_1, i_2, \cdots, i_j\}} N_k}. \tag{12}$$

2

where $\stackrel{1}{=}$ is because for any attack strategy $\hat{\boldsymbol{g}}^{(\boldsymbol{v})}$, we have

$$\mathbb{P}\left(\bigcup_{i\in[d]}|\hat{g}_i^{[\boldsymbol{v}]}(\theta')-g_i(\theta)|\le\epsilon_i\Big|\theta'\right)$$

$$=\sum_{i\in[d]}\mathbb{P}\left(|\hat{g}_i^{[\boldsymbol{v}]}(\theta')-g_i(\theta)|\le\epsilon_i\Big|\theta'\right)-\sum_{\substack{i_1<i_2\\i_1,i_2\in[d]}}\mathbb{P}\left(\bigcap_{i\in\{i_1,i_2\}}|\hat{g}_i^{[\boldsymbol{v}]}(\theta')-g_i(\theta)|\le\epsilon_i\Big|\theta'\right)$$

$$+\cdots+(-1)^{j-1}\sum_{\substack{i_1<i_2<\cdots<i_j\\i_1,i_2,\cdots,i_j\in[d]}}\mathbb{P}\left(\bigcap_{i\in\{i_1,i_2,\cdots,i_j\}}|\hat{g}_i^{[\boldsymbol{v}]}(\theta')-g_i(\theta)|\le\epsilon_i\Big|\theta'\right)$$

$$+\cdots+(-1)^{d-1}\mathbb{P}\left(\bigcap_{i\in[d]}|\hat{g}_i^{[\boldsymbol{v}]}(\theta')-g_i(\theta)|\le\epsilon_i\Big|\theta'\right)$$

$$=\sum_{j\in[d]}(-1)^{j-1}\sum_{\substack{i_1<i_2<\cdots<i_j\\i_1,i_2,\cdots,i_j\in[d]}}\mathbb{P}\left(\bigcap_{i\in\{i_1,i_2,\cdots,i_j\}}|\hat{g}_i^{[\boldsymbol{v}]}(\theta')-g_i(\theta)|\le\epsilon_i\Big|\theta'\right).$$

$\stackrel{2}{\ge}$ is because

$$\sum_{\boldsymbol{v}}\sum_{j\in[d]}(-1)^{j-1}\sum_{\substack{i_1<i_2<\cdots<i_j\\i_1,i_2,\cdots,i_j\in[d]}}\mathbb{P}\left(\bigcap_{i\in\{i_1,i_2,\cdots,i_j\}}|\hat{g}_i^{[\boldsymbol{v}]}(\theta')-g_i(\theta)|\le\epsilon_i\Big|\theta'\right)$$

$$=\sum_{j\in[d]}(-1)^{j-1}\sum_{\boldsymbol{v}}\sum_{\substack{i_1<i_2<\cdots<i_j\\i_1,i_2,\cdots,i_j\in[d]}}\mathbb{P}\left(\bigcap_{i\in\{i_1,i_2,\cdots,i_j\}}|\hat{g}_i^{[\boldsymbol{v}]}(\theta')-g_i(\theta)|\le\epsilon_i\Big|\theta'\right)$$

$$=\sum_{j\in[d]}(-1)^{j-1}\sum_{\substack{i_1<i_2<\cdots<i_j\\i_1,i_2,\cdots,i_j\in[d]}}\sum_{\boldsymbol{v}}\mathbb{P}\left(\bigcap_{i\in\{i_1,i_2,\cdots,i_j\}}|\hat{g}_i^{[\boldsymbol{v}]}(\theta')-g_i(\theta)|\le\epsilon_i\Big|\theta'\right)$$

$$\ge\sum_{j\in[d]}(-1)^{j-1}\sum_{\substack{i_1<i_2<\cdots<i_j\\i_1,i_2,\cdots,i_j\in[d]}}\prod_{k_1\in[d]\backslash\{i_1,i_2,\cdots,i_j\}}N_{k_1}$$

$$=\sum_{j\in[d]}(-1)^{j-1}\sum_{\substack{i_1<i_2<\cdots<i_j\\i_1,i_2,\cdots,i_j\in[d]}}\frac{\mathcal{N}}{\prod_{k\in\{i_1,i_2,\cdots,i_j\}}N_k}.$$

Since $H_{\theta'}^{(i)}>L_{\theta'}^{(i)}+2(N_i-1)\epsilon_i,\ \forall i\in[d]$, we can get that

$$\prod_{i\in[d]}\left(H_{\theta'}^{(i)}-L_{\theta'}^{(i)}\right)>\prod_{i\in[d]}2\epsilon_i\left(N_i-1\right)$$

$$=\prod_{i\in[d]}2\epsilon_i\cdot\prod_{i\in[d]}\left(N_i-1\right)$$

$$=\left(\mathcal{N}-\sum_{j\in[d]}(-1)^{j-1}\sum_{\substack{i_1<i_2<\cdots<i_j\\i_1,i_2,\cdots,i_j\in[d]}}\frac{\mathcal{N}}{\prod_{k\in\{i_1,i_2,\cdots,i_j\}}N_k}\right)\cdot\prod_{i\in[d]}2\epsilon_i$$

$$\stackrel{1}{\ge}\lceil(1-T)\mathcal{N}\rceil\cdot\prod_{i\in[d]}2\epsilon_i,\tag{13}$$

3

where $\overset{1}{\geq}$ is because based on Eq. (12) and the fact that $N_i$ is an integer for any $i \in [d]$, we have

$$\sum_{j \in [d]} (-1)^{j-1} \sum_{\substack{i_1 < i_2 < \cdots < i_j \\ i_1, i_2, \cdots, i_j \in [d]}} \frac{\mathcal{N}}{\prod_{k \in \{i_1, i_2, \cdots, i_j\}} N_k} \leq \lfloor T\mathcal{N} \rfloor.$$

We analyze the value of $\mathcal{N}$ as follows. Based on Eq. (12), we have

$$T \cdot \mathcal{N} \geq \sum_{j \in [d]} (-1)^{j-1} \sum_{\substack{i_1 < i_2 < \cdots < i_j \\ i_1, i_2, \cdots, i_j \in [d]}} \frac{\mathcal{N}}{\prod_{k \in \{i_1, i_2, \cdots, i_j\}} N_k} = \mathcal{N} - \prod_{i \in [d]} (N_i - 1). \qquad (14)$$

Define $a_i = N_i - 1$. Then we have $a_i \geq 0$ and $\mathcal{N} = \prod_{i \in [d]} (a_i + 1)$. We can get that

$$\mathcal{N} = \prod_{i \in [d]} (a_i + 1)$$

$$= 1 + \sum_{j \in [d]} \sum_{\substack{i_1 < i_2 < \cdots < i_j \\ i_1, i_2, \cdots, i_j \in [d]}} \prod_{k \in \{i_1, i_2, \cdots, i_j\}} a_k$$

$$\overset{1}{\geq} \sum_{j \in [d] \cup \{0\}} \binom{d}{j} \cdot \left( \prod_{i \in [d]} a_i \right)^{\frac{j}{d}}$$

$$= \left( \left( \prod_{i \in [d]} a_i \right)^{\frac{1}{d}} + 1 \right)^d$$

$$= \left( \left( \prod_{i \in [d]} (N_i - 1) \right)^{\frac{1}{d}} + 1 \right)^d,$$

where $\overset{1}{\geq}$ is because when $j = 0$, $\binom{d}{j} \cdot \left( \prod_{i \in [d]} a_i \right)^{\frac{j}{d}} = 1$, and for any $j \in [d]$, we have

$$\sum_{\substack{i_1 < i_2 < \cdots < i_j \\ i_1, i_2, \cdots, i_j \in [d]}} \prod_{k \in \{i_1, i_2, \cdots, i_j\}} a_k \geq \binom{d}{j} \cdot \left( \prod_{\substack{i_1 < i_2 < \cdots < i_j \\ i_1, i_2, \cdots, i_j \in [d]}} \prod_{k \in \{i_1, i_2, \cdots, i_j\}} a_k \right)^{\frac{1}{\binom{d}{j}}}$$

$$= \binom{d}{j} \cdot \left( \prod_{i \in [d]} a_i \right)^{\frac{\binom{d-1}{j-1}}{\binom{d}{j}}}$$

$$= \binom{d}{j} \cdot \left( \prod_{i \in [d]} a_i \right)^{\frac{j}{d}}.$$

Therefore, we can get that

$$\prod_{i \in [d]} (N_i - 1) \leq \left( \mathcal{N}^{\frac{1}{d}} - 1 \right)^d.$$

Combined with Eq. (14) and the fact that $\mathcal{N}$ is an integer, we have

$$T \cdot \mathcal{N} \geq \mathcal{N} - \left(\mathcal{N}^{\frac{1}{d}} - 1\right)^d$$

$$\left(\mathcal{N}^{\frac{1}{d}} - 1\right)^d \geq (1 - T)\mathcal{N}$$

$$\mathcal{N}^{\frac{1}{d}} \geq \frac{1}{1 - (1-T)^{\frac{1}{d}}}$$

$$\mathcal{N} \geq \left\lceil \frac{1}{\left(1 - (1-T)^{1/d}\right)^d} \right\rceil.$$

Combined with Eq. (13), we can get that

$$\prod_{i \in [d]} \left(H_{\theta'}^{(i)} - L_{\theta'}^{(i)}\right) > \lceil (1-T)\mathcal{N} \rceil \cdot \prod_{i \in [d]} 2\epsilon_i \geq \left\lceil (1-T) \left\lceil \frac{1}{\left(1 - (1-T)^{1/d}\right)^d} \right\rceil \right\rceil \cdot \prod_{i \in [d]} 2\epsilon_i.$$

Hence, we have

$$\prod_{i \in [d]} \left(H_{\theta'}^{(i)} - L_{\theta'}^{(i)}\right)^{1/d} > 2\left\lceil (1-T)^{1/d} \left\lceil \frac{1}{1 - (1-T)^{1/d}} \right\rceil \right\rceil \cdot \left(\prod_{i \in [d]} \epsilon_i\right)^{1/d}. \tag{15}$$

Then we have

$$\Delta_{\mathcal{M}_g} = \sup_{\substack{\theta \in \mathrm{Supp}(\omega_\Theta), \\ \theta' \in \mathrm{Supp}(\mathcal{M}_g(\theta))}} \mathfrak{D}\left(\omega_{X_\theta} \| \omega_{X_{\theta'}}\right)$$

$$\geq \sup_{\theta_i \in \mathrm{Supp}(\omega_\Theta), i \in \{1,2\} : \mathcal{M}_g(\theta_i) = \theta'} D\left(X_{\theta_1}, X_{\theta_2}\right) \tag{16}$$

$$> 2\gamma^{\mathrm{union}} \cdot \left\lceil (1-T)^{1/d} \left\lceil \frac{1}{1 - (1-T)^{1/d}} \right\rceil \right\rceil \cdot \left(\prod_{i \in [d]} \epsilon_i\right)^{1/d} \tag{17}$$

$$> 2\gamma^{\mathrm{union}} \cdot \left\lceil \frac{1}{1 - (1-T)^{1/d}} - 1 \right\rceil \cdot \left(\prod_{i \in [d]} \epsilon_i\right)^{1/d},$$

where in Eq. (16), $\theta_i$ for $i \in \{1, 2\}$ denotes two arbitrary parameter vectors in the support space. Eq. (16) comes from the triangle inequality, and Eq. (17) utilizes Eq. (15) and the definition of $\gamma^{\mathrm{union}}$. $\qquad \square$

## B.2 Proof of Thm. 5.1

*Proof.* Similar to the proof of Thm. 4.1, we construct a sequence of attackers guessing different possible secrets values, such that there exists attackers guessing all secrets successfully. Specifically, for each secret, we divide the range of possible secret values into segments, and design a series of individual-secret attack strategies, guessing the midpoint of each segment. We subsequently formulate multi-secret attack strategies by choosing one individual-secret strategy for each secret. We then establish the distortion lower bound based on the privacy constraint that the attack success rate is at most $T$ and by utilizing the conversion parameter $\gamma^{\mathrm{inter}}$ that serves as a linkage between the distributional distance and the distance between secrets.

It follows from Eq. (11) that there exists $\theta'$ s.t. $\sup_{\hat{g}} \mathbb{P}\left(\bigcap_{i \in [d]} |\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i \middle| \theta'\right) \leq T$. For any $i \in [d]$, let $L_{\theta'}^{(i)}$ and $H_{\theta'}^{(i)}$ be the smallest and the largest possible value of secret $g_i$ given the released

distribution parameter $\theta'$:

$$L_{\theta'}^{(i)} \triangleq \inf_{\theta \in \text{Supp}(\omega_\Theta): \mathcal{M}_g(\theta)=\theta'} g_i(\theta) \ ,$$

$$H_{\theta'}^{(i)} \triangleq \sup_{\theta \in \text{Supp}(\omega_\Theta): \mathcal{M}_g(\theta)=\theta'} g_i(\theta) \ .$$

For each secret $g_i$, where $i \in [d]$, we partition the range of possible secret values, i.e., $[L_{\theta'}^{(i)}, H_{\theta'}^{(i)}]$, into segments with length $2\epsilon_i$. Subsequently, we develop a set of individual-secret attack strategies by guessing the midpoint of each segment. As a result, the number of individual-secret attack strategies, denoted as $N_i$, satisfies $L_{\theta'}^{(i)} + 2N_i\epsilon_i \geq H_{\theta'}^{(i)} > L_{\theta'}^{(i)} + 2(N_i-1)\epsilon_i$.

We then construct multi-secret attack strategies by selecting one individual-secret strategy for each secret. For the multi-secret attack strategy $\hat{g}^{(v)}$, where $v = [v_1, v_2, \cdots, v_d]$ and $v_i \in [N_i]$ for all $i \in [d]$, it guesses the secret $g_i$ as the midpoint of the $v_i$-th segment, i.e., $\hat{g}_i^{[v]}(\theta') = L_{\theta'}^{(i)} + (v_i - 0.5) \cdot 2\epsilon_i$. The number of multi-secret attack strategies, denoted as $\mathcal{N}$, is $\mathcal{N} = \prod_{i \in [d]} N_i$. We can get that

$$T \cdot \mathcal{N} \geq \sum_v \mathbb{P}\left( \bigcap_{i \in [d]} |\hat{g}_i^{[v]}(\theta') - g_i(\theta)| \leq \epsilon_i \Big| \theta' \right) = 1.$$

Since $\mathcal{N} \in \mathbb{N}^+$, we have $\mathcal{N} \geq \lceil \frac{1}{T} \rceil$.

Therefore, we can get that

$$\sum_{i \in [d]} \left( H_{\theta'}^{(i)} - L_{\theta'}^{(i)} \right) > \sum_{i \in [d]} 2\epsilon_i (N_i - 1)$$

$$\geq 2d \left( \prod_{i \in [d]} \epsilon_i N_i \right)^{1/d} - 2\sum_{i \in [d]} \epsilon_i$$

$$\geq 2d \cdot \left\lceil \frac{1}{T} \right\rceil^{1/d} \cdot \left( \prod_{i \in [d]} \epsilon_i \right)^{1/d} - 2\sum_{i \in [d]} \epsilon_i.$$

Hence, we have

$$\Delta_{\mathcal{M}_g} = \sup_{\substack{\theta \in \text{Supp}(\omega_\Theta), \\ \theta' \in \text{Supp}(\mathcal{M}_g(\theta))}} \mathfrak{D}\left( \omega_{X_\theta} \| \omega_{X_{\theta'}} \right)$$

$$\geq \sup_{\theta_i \in \text{Supp}(\omega_\Theta), i \in \{1,2\}: \mathcal{M}_g(\theta_i)=\theta'} D\left( X_{\theta_1}, X_{\theta_2} \right)$$

$$> 2\gamma^{\text{inter}} \cdot \left\lceil \frac{1}{T} \right\rceil^{1/d} \cdot \left( \prod_{i \in [d]} \epsilon_i \right)^{1/d} - 2\gamma^{\text{inter}} \cdot \frac{1}{d} \sum_{i \in [d]} \epsilon_i. \tag{18}$$

$\square$

## B.3 Proof of Prop. 5.2

*Proof.* We first prove that for any fixed distortion budget $\delta_0$, when $\Delta \leq \delta_0$, the achievable lower bound for union privacy, denoted as $\Pi_{\epsilon,\omega_\Theta}^{\text{union}}$, is no smaller than that for intersection privacy, denoted as $\Pi_{\epsilon,\omega_\Theta}^{\text{inter}}$.

For any attack strategy $\hat{g}$ and data release mechanism $\mathcal{M}_g$ that satisfies $\Delta \leq \delta_0$, we have

$$\mathbb{P}\left( \bigcap_{i \in [d]} |\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i \right) \leq \mathbb{P}\left( \bigcup_{i \in [d]} |\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i \right).$$

Therefore, we can get that for any data release mechanism $\mathcal{M}_g$ that satisfies $\Delta \leq \delta_0$:

$$\sup_{\hat{\boldsymbol{g}}} \mathbb{P}\left(\bigcap_{i\in[d]} |\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i\right) \leq \sup_{\hat{\boldsymbol{g}}} \mathbb{P}\left(\bigcup_{i\in[d]} |\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i\right),$$

which indicates that with a fixed distortion budget $\delta_0$, $\Pi_{\epsilon,\omega_\Theta}^{\text{inter}} \leq \Pi_{\epsilon,\omega_\Theta}^{\text{union}}$. Hence, we can easily get that with a privacy budget $T$, the achievable distortion lower bounds for union privacy $\Delta^{\text{union}}$ and intersection privacy $\Delta^{\text{inter}}$ satisfy $\Delta^{\text{union}} \geq \Delta^{\text{inter}}$. $\quad\square$

## B.4 Proof of Thm. 5.3

*Proof.* Similar to the proof of Thm. 4.1, we construct a sequence of attackers guessing different possible secrets values, such that there exists attackers successfully guessing secrets. Specifically, for each secret, we divide the range of possible secret values into segments, and design a series of individual-secret attack strategies, guessing the midpoint of each segment. We subsequently formulate multi-secret attack strategies by choosing one individual-secret strategy for each secret. We then establish the distortion lower bound based on the privacy constraint that the attack success rate is at most $T$ and by utilizing the conversion parameter $\gamma^{\text{group}}$ that serves as a linkage between the distributional distance and the distance between secrets.

It follows from Eq. (11) there exists $\theta'$ s.t. $\sup_{\hat{g}} \mathbb{P}\left(\bigcap_{i\in[d]} |\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i \Big| \theta'\right) \leq T$. For any $i \in [d]$, let $L_{\theta'}^{(i)}$ and $H_{\theta'}^{(i)}$ be the smallest and the largest possible value of secret $g_i$ given the released distribution parameter $\theta'$:

$$L_{\theta'}^{(i)} \triangleq \inf_{\theta\in\text{Supp}(\omega_\Theta):\mathcal{M}_g(\theta)=\theta'} g_i(\theta),$$

$$H_{\theta'}^{(i)} \triangleq \sup_{\theta\in\text{Supp}(\omega_\Theta):\mathcal{M}_g(\theta)=\theta'} g_i(\theta).$$

For each secret $g_i$, where $i \in [d]$, we partition the range of possible secret values, i.e., $[L_{\theta'}^{(i)}, H_{\theta'}^{(i)}]$, into segments with length $2\epsilon_i$. Subsequently, we develop a set of individual-secret attack strategies by guessing the midpoint of each segment. As a result, the number of individual-secret attack strategies, denoted as $N_i$, satisfies $L_{\theta'}^{(i)} + 2N_i\epsilon_i \geq H_{\theta'}^{(i)} > L_{\theta'}^{(i)} + 2(N_i - 1)\epsilon_i$.

We then construct multi-secret attack strategies by selecting one individual-secret strategy for each secret. For the multi-secret attack strategy $\hat{\boldsymbol{g}}^{(\boldsymbol{v})}$, where $\boldsymbol{v} = [v_1, v_2, \cdots, v_d]$ and $v_i \in [N_i]$ for all $i \in [d]$, it guesses the secret $g_i$ as the midpoint of the $v_i$-th segment, i.e., $\hat{g}_i^{[\boldsymbol{v}]}(\theta') = L_{\theta'}^{(i)} + (v_i - 0.5) \cdot 2\epsilon_i$. The number of multi-secret attack strategies, denoted as $\mathcal{N}$, is $\mathcal{N} = \prod_{i\in[d]} N_i$. We can get that

$$
\begin{aligned}
T \cdot \mathcal{N} &\geq \sum_{\boldsymbol{v}} \sup_{\hat{g}} \ \mathbb{P}\left(\bigcup_{b\in\mathcal{B}}\left(\bigcap_{i\in\mathcal{I}_b} |\hat{g}_i^{[\boldsymbol{v}]}(\theta') - g_i(\theta)| \leq \epsilon_i\right)\right) \\
&= \sum_{\boldsymbol{v}}\sum_{j\in[\beta]} (-1)^{j-1} \sum_{\substack{b_1\neq b_2\neq\cdots\neq b_j \\ b_1,b_2,\cdots,b_j\in\mathcal{B}}} \mathbb{P}\left(\bigcap_{\substack{i\in\mathcal{I}_b \\ b\in\{b_1,b_2,\cdots,b_j\}}} |\hat{g}_i^{[\boldsymbol{v}]}(\theta') - g_i(\theta)| \leq \epsilon_i \Big| \theta'\right) \\
&\overset{1}{\geq} \sum_{j\in[\beta]} (-1)^{j-1} \sum_{\substack{b_1\neq b_2\neq\cdots\neq b_j \\ b_1,b_2,\cdots,b_j\in\mathcal{B}}} \frac{\mathcal{N}}{\prod_{b\in\{b_1,b_2,\cdots,b_j\}} \prod_{k\in\mathcal{I}_b} N_k} \\
&= \mathcal{N} - \prod_{b\in\mathcal{B}}\left(\prod_{i\in\mathcal{I}_b} N_i - 1\right),
\end{aligned}
\tag{19}
$$

where $\overset{1}{\geq}$ is because

$$\sum_{\boldsymbol{v}} \sum_{j \in [\beta]} (-1)^{j-1} \sum_{\substack{b_1 \neq b_2 \neq \cdots \neq b_j \\ b_1, b_2, \cdots, b_j \in \mathcal{B}}} \mathbb{P} \left( \bigcap_{\substack{i \in \mathcal{I}_b \\ b \in \{b_1, b_2, \cdots, b_j\}}} |\hat{g}_i^{[\boldsymbol{v}]}(\theta') - g_i(\theta)| \leq \epsilon_i \Big| \theta' \right)$$

$$= \sum_{j \in [\beta]} (-1)^{j-1} \sum_{\substack{b_1 \neq b_2 \neq \cdots \neq b_j \\ b_1, b_2, \cdots, b_j \in \mathcal{B}}} \sum_{\boldsymbol{v}} \mathbb{P} \left( \bigcap_{\substack{i \in \mathcal{I}_b \\ b \in \{b_1, b_2, \cdots, b_j\}}} |\hat{g}_i^{[\boldsymbol{v}]}(\theta') - g_i(\theta)| \leq \epsilon_i \Big| \theta' \right)$$

$$\geq \sum_{j \in [\beta]} (-1)^{j-1} \sum_{\substack{b_1 \neq b_2 \neq \cdots \neq b_j \\ b_1, b_2, \cdots, b_j \in \mathcal{B}}} \prod_{k_1 \in [d] \setminus \bigcup_{b \in \{b_1, b_2, \cdots, b_j\}} \mathcal{I}_b} N_{k_1}$$

$$= \sum_{j \in [\beta]} (-1)^{j-1} \sum_{\substack{b_1 \neq b_2 \neq \cdots \neq b_j \\ b_1, b_2, \cdots, b_j \in \mathcal{B}}} \frac{\mathcal{N}}{\prod_{b \in \{b_1, b_2, \cdots, b_j\}} \prod_{k \in \mathcal{I}_b} N_k}.$$

Define $A_b = \prod_{i \in \mathcal{I}_b} N_i - 1$. We have $A_b \geq 0$ and $\mathcal{N} = \prod_{b \in \mathcal{B}} (A_b + 1)$. We can get that

$$\mathcal{N} = \prod_{b \in \mathcal{B}} (A_b + 1)$$

$$= 1 + \sum_{j \in [\beta]} \sum_{\substack{b_1 \neq b_2 \neq \cdots \neq b_j \\ b_1, b_2, \cdots, b_j \in \mathcal{B}}} \prod_{b \in \{b_1, b_2, \cdots, b_j\}} A_b$$

$$\overset{1}{\geq} \sum_{j \in [\beta] \cup \{0\}} \binom{\beta}{j} \cdot \left( \prod_{b \in \mathcal{B}} A_b \right)^{\frac{j}{\beta}}$$

$$= \left( \left( \prod_{b \in \mathcal{B}} A_b \right)^{\frac{1}{\beta}} + 1 \right)^{\beta}$$

$$= \left( \left( \prod_{b \in \mathcal{B}} \left( \prod_{i \in \mathcal{I}_b} N_i - 1 \right) \right)^{\frac{1}{\beta}} + 1 \right)^{\beta}.$$

$\overset{1}{\geq}$ is because when $j = 0$, $\binom{\beta}{j} \cdot \left( \prod_{b \in \mathcal{B}} A_b \right)^{\frac{j}{\beta}} = 1$, and for any $j \in [\mathcal{B}]$, we have

$$\sum_{\substack{b_1 \neq b_2 \neq \cdots \neq b_j \\ b_1, b_2, \cdots, b_j \in \mathcal{B}}} \prod_{b \in \{b_1, b_2, \cdots, b_j\}} A_b \geq \binom{\beta}{j} \cdot \left( \prod_{\substack{b_1 \neq b_2 \neq \cdots \neq b_j \\ b_1, b_2, \cdots, b_j \in \mathcal{B}}} \prod_{b \in \{b_1, b_2, \cdots, b_j\}} A_b \right)^{\frac{1}{\binom{\beta}{j}}}$$

$$= \binom{\beta}{j} \cdot \left( \prod_{b \in \mathcal{B}} A_b \right)^{\frac{\binom{\beta-1}{j-1}}{\binom{\beta}{j}}}$$

$$= \binom{\beta}{j} \cdot \left( \prod_{b \in \mathcal{B}} A_b \right)^{\frac{j}{\beta}}.$$

Therefore, we have

$$\prod_{b \in \mathcal{B}} \left( \prod_{i \in \mathcal{I}_b} N_i - 1 \right) \leq \left( \mathcal{N}^{\frac{1}{\beta}} - 1 \right)^{\beta}. \tag{20}$$

Combining this result with Eq. (19) and the fact that $\mathcal{N}$ is an integer, we have

$$T \cdot \mathcal{N} \geq \mathcal{N} - \left(\mathcal{N}^{\frac{1}{\beta}} - 1\right)^{\beta}$$

$$\left(\mathcal{N}^{\frac{1}{\beta}} - 1\right)^{\beta} \geq (1 - T)\mathcal{N}$$

$$\mathcal{N}^{\frac{1}{\beta}} \geq \frac{1}{1 - (1 - T)^{\frac{1}{\beta}}}$$

$$\mathcal{N} \geq \left\lceil \frac{1}{\left(1 - (1 - T)^{1/\beta}\right)^{\beta}} \right\rceil.$$

Hence, we can get that

$$\sum_{i \in [d]} \left(H_{\theta'}^{(i)} - L_{\theta'}^{(i)}\right) > \sum_{i \in [d]} 2\epsilon_i \left(N_i - 1\right)$$

$$\geq 2d \left(\prod_{i \in [d]} \epsilon_i N_i\right)^{1/d} - 2\sum_{i \in [d]} \epsilon_i$$

$$\geq 2d \cdot \left\lceil \frac{1}{\left(1 - (1 - T)^{1/\beta}\right)^{\beta/d}} \right\rceil \cdot \left(\prod_{i \in [d]} \epsilon_i\right)^{1/d} - 2\sum_{i \in [d]} \epsilon_i.$$

Then we have

$$\Delta_{\mathcal{M}_g} = \sup_{\substack{\theta \in \mathrm{Supp}(\omega_\Theta), \\ \theta' \in \mathrm{Supp}(\mathcal{M}_g(\theta))}} \mathfrak{D}\left(\omega_{X_\theta} \| \omega_{X_{\theta'}}\right)$$

$$\geq \sup_{\theta_i \in \mathrm{Supp}(\omega_\Theta), i \in \{1,2\}: \mathcal{M}_g(\theta_i) = \theta'} D\left(X_{\theta_1}, X_{\theta_2}\right)$$

$$> 2\gamma^{\mathrm{group}} \cdot \left\lceil \frac{1}{\left(1 - (1 - T)^{1/\beta}\right)^{\beta/d}} \right\rceil \cdot \left(\prod_{i \in [d]} \epsilon_i\right)^{1/d} - 2\gamma^{\mathrm{group}} \cdot \frac{1}{d} \sum_{i \in [d]} \epsilon_i.$$

$\square$

## B.5 Proof of Prop. 6.1

*Proof.* Define $\theta' = (\mu'_1, \cdots, \mu'_k, \sigma'_1, \cdots, \sigma'_k)$. We first provide the lemma as follows.

**Lemma B.1.** $D\left(X_\theta, X_{\theta'}\right)$ *can be derived as:*

$$D\left(X_\theta, X_{\theta'}\right) = \frac{1}{2}\sqrt{\sum_{j \in [k]} \left(\mu_j - \mu'_j\right)^2 + \sum_{j \in [k]} \left(\sigma_j - \sigma'_j\right)^2}.$$

The proof is in App. B.5.1.

Based on Lemma B.1, we can get that

$$
\begin{aligned}
\frac{D\left(X_\theta, X_{\theta'}\right)}{R^{\mathrm{union}}\left(X_\theta, X_{\theta'}\right)} &\geq \frac{\sqrt{\sum_{j\in[k]}\left(\mu_j - \mu_j'\right)^2 + \sum_{j\in[k]}\left(\sigma_j - \sigma_j'\right)^2}}{2\prod_{i\in[d]}|g_i(\theta) - g_i(\theta')|^{1/d}} \\
&\geq \frac{\sqrt{\sum_{i\in[d]}\left(g_i(\theta) - g_i(\theta')\right)^2}}{2\prod_{i\in[d]}|g_i(\theta) - g_i(\theta')|^{1/d}} \\
&= \frac{1}{2}\sqrt{\frac{\sum_{i\in[d]}\left(g_i(\theta) - g_i(\theta')\right)^2}{\prod_{i\in[d]}|g_i(\theta) - g_i(\theta')|^{2/d}}} \\
&\geq \frac{1}{2}\sqrt{d\cdot\frac{\prod_{i\in[d]}|g_i(\theta) - g_i(\theta')|^{2/d}}{\prod_{i\in[d]}|g_i(\theta) - g_i(\theta')|^{2/d}}} \\
&= \frac{\sqrt{d}}{2}.
\end{aligned}
$$

Therefore, we have

$$
\gamma^{\mathrm{union}} = \inf_{\theta_1,\theta_2\in\mathrm{Supp}(\omega_\Theta)} \frac{D\left(X_{\theta_1}, X_{\theta_2}\right)}{R^{\mathrm{union}}\left(X_{\theta_1}, X_{\theta_2}\right)} = \frac{\sqrt{d}}{2}.
$$

Based on Thm. 4.1, we can get that

$$
\Delta_{\mathcal{M}_g} > \sqrt{d}\cdot\left[\frac{1}{1-(1-T)^{1/d}} - 1\right]\cdot\left(\prod_{i\in[d]}\epsilon_i\right)^{1/d}.
$$

$\square$

### B.5.1 Proof of Lemma B.1

*Proof.* From [15], we have

$$
\mathfrak{D}\left(\omega_{X_\theta}\|\omega_{X_{\theta'}}\right)^2 = \sum_{j\in[k]}\left(\mu_j - \mu_j'\right)^2 + \mathrm{Tr}\left(\Sigma + \Sigma' - 2\left(\Sigma^{\frac{1}{2}}\Sigma'\Sigma^{\frac{1}{2}}\right)^{\frac{1}{2}}\right),
$$

where diagonal covariance matrices $\Sigma, \Sigma'$ are $\Sigma = \begin{bmatrix} \sigma_1^2 & & & \\ & \sigma_2^2 & & \\ & & \ddots & \\ & & & \sigma_k^2 \end{bmatrix}$ and $\Sigma' = \begin{bmatrix} \sigma_1'^2 & & & \\ & \sigma_2'^2 & & \\ & & \ddots & \\ & & & \sigma_k'^2 \end{bmatrix}$. We

can get that

$$
\begin{aligned}
\Sigma + \Sigma' - 2\left(\Sigma^{\frac{1}{2}}\Sigma'\Sigma^{\frac{1}{2}}\right)^{\frac{1}{2}} &= \begin{bmatrix} \sigma_1^2 + \sigma_1'^2 & & & \\ & \sigma_2^2 + \sigma_2'^2 & & \\ & & \ddots & \\ & & & \sigma_k^2 + \sigma_k'^2 \end{bmatrix} - 2\begin{bmatrix} \sigma_1^2\sigma_1'^2 & & & \\ & \sigma_2^2\sigma_2'^2 & & \\ & & \ddots & \\ & & & \sigma_k^2\sigma_k'^2 \end{bmatrix}^{\frac{1}{2}} \\
&= \begin{bmatrix} (\sigma_1 - \sigma_1')^2 & & & \\ & (\sigma_2 - \sigma_2')^2 & & \\ & & \ddots & \\ & & & (\sigma_k - \sigma_k')^2 \end{bmatrix}.
\end{aligned}
$$

10

Therefore, we can get that

$$\mathfrak{D}\left(\omega_{X_\theta}\|\omega_{X_{\theta'}}\right)^2 = \sum_{j\in[k]}\left(\mu_j - \mu'_j\right)^2 + \mathrm{Tr}\left(\Sigma + \Sigma' - 2\left(\Sigma^{\frac{1}{2}}\Sigma'\Sigma^{\frac{1}{2}}\right)^{\frac{1}{2}}\right) = \sum_{j\in[k]}\left(\mu_j - \mu'_j\right)^2 + \sum_{j\in[k]}\left(\sigma_j - \sigma'_j\right)^2.$$

Hence, we have

$$D\left(X_\theta, X_{\theta'}\right) = \frac{1}{2}\sqrt{\sum_{j\in[k]}\left(\mu_j - \mu'_j\right)^2 + \sum_{j\in[k]}\left(\sigma_j - \sigma'_j\right)^2}.$$

$\square$

## B.6  Proof of Prop. 6.2

*Proof.* Based on Lemma B.1, we can easily can get that the distortion $\Delta_{\mathrm{Alg.1}}$ of Alg. 1 is

$$\Delta_{\mathcal{M}_g} = \sqrt{\sum_{i\in[d]} s_{g_i}{}^2}.$$

Since the secret distribution parameters are independent of each other and follow the uniform distributions, we can get that the privacy of Alg. 1 is

$$\begin{aligned}
\Pi_{\epsilon,\omega_\Theta}^{\mathrm{union}} &= \sup_{\hat{g}} \ \mathbb{P}\left(\bigcup_{i\in[d]} |\hat{g}_i\left(\theta'\right) - g_i\left(\theta\right)| \le \epsilon_i\right) \\
&= 1 - \sup_{\hat{g}} \ \mathbb{P}\left(\bigcap_{i\in[d]} |\hat{g}_i\left(\theta'\right) - g_i\left(\theta\right)| > \epsilon_i\right) \\
&= 1 - \sup_{\hat{g}} \ \prod_{i\in[d]} \mathbb{P}\left(|\hat{g}_i\left(\theta'\right) - g_i\left(\theta\right)| > \epsilon_i\right) \\
&= 1 - \prod_{i\in[d]}\left(1 - \frac{2\epsilon_i}{s_{g_i}}\right).
\end{aligned}$$

From Prop. 6.1, we know that the optimal achievable distortion $\Delta_{opt}$ satisfy

$$\begin{aligned}
\Delta_{opt} &> \sqrt{d}\cdot\left[\frac{1}{1 - \left(1 - \Pi_{\epsilon,\omega_\Theta}\right)^{1/d}} - 1\right]\cdot\left(\prod_{i\in[d]}\epsilon_i\right)^{1/d} \\
&= \sqrt{d}\cdot\left[\frac{1}{1 - \prod_{i\in[d]}\left(1 - \frac{2\epsilon_i}{s_{g_i}}\right)^{1/d}} - 1\right]\cdot\left(\prod_{i\in[d]}\epsilon_i\right)^{1/d}.
\end{aligned}$$

Let $k = \frac{\Delta}{\Delta_{opt}}$, $x_i = \frac{\epsilon_i}{s_{g_i}}$, $\forall i \in [d]$, $c_1 = \min_{i \in [d]} \{x_i\}$, and $c_2 = \max_{i \in [d]} \{x_i\}$, we have

$$
\begin{aligned}
k &< \frac{\sqrt{\sum_{i \in [d]} s_{g_i}{}^2}}{\sqrt{d} \cdot \left[ \frac{1}{1 - \prod_{i \in [d]} \left(1 - \frac{2\epsilon_i}{s_{g_i}}\right)^{1/d}} - 1 \right] \cdot \left(\prod_{i \in [d]} \epsilon_i\right)^{1/d}} \\
&= \frac{\sqrt{\sum_{i \in [d]} \left(\frac{\epsilon_i}{x_i}\right)^2}}{\sqrt{d} \cdot \left[ \frac{1}{1 - \prod_{i \in [d]} (1 - 2x_i)^{1/d}} - 1 \right] \cdot \left(\prod_{i \in [d]} \epsilon_i\right)^{1/d}} \\
&\leq \frac{2c_2 \sqrt{\sum_{i \in [d]} \epsilon_i^2}}{c_1 (1 - 2c_2) \sqrt{d} \left(\prod_{i \in [d]} \epsilon_i\right)^{1/d}} \\
&= \frac{\sqrt{\frac{1}{d} \sum_{i \in [d]} \epsilon_i^2}}{\left(\prod_{i \in [d]} \epsilon_i\right)^{1/d}} \cdot \frac{2c_2}{c_1 (1 - 2c_2)}.
\end{aligned}
$$

Let $c_\epsilon = \frac{\sqrt{\frac{1}{d} \sum_{i \in [d]} \epsilon_i^2}}{\left(\prod_{i \in [d]} \epsilon_i\right)^{1/d}}$, and we can easily get that $c_\epsilon \leq \max_{i,j \in [d]} \left\{\frac{\epsilon_i}{\epsilon_j}\right\}$, a constant depending on the values of tolerance ranges. Denoting $c_{\epsilon,s} = \frac{2c_\epsilon c_2}{c_1 (1 - 2c_2)}$, we can finally get that

$$
\Delta_{\mathcal{M}_g} = k \Delta_{opt} < c_{\epsilon,s} \Delta_{opt},
$$

where $c_{\epsilon,s}$ is a constant depending on tolerance ranges and the interval lengths of the mechanism.

Specifically, when $\epsilon_1 = \cdots = \epsilon_d$, and the designed data released mechanism satisfy $\frac{\epsilon_1}{s_{g_1}} = \cdots = \frac{\epsilon_d}{s_{g_d}} \leq \frac{1}{6}$, we can get that $\Delta < 3\Delta_{opt}$. $\qquad \square$

## B.7 Theoretical Lower Bounds of Surrogate Metrics with Secrets $=$ Three Means

Without loss of generality, we assume our objective is to protect the means of the first three dimensions of the data distribution. Let $x^{(i)}$ be the $i$-th dimension of the data sample $\boldsymbol{x} \in \mathbb{R}^t$ $(t \geq 3)$. For the original and released dataset $\mathcal{X} = \{\boldsymbol{x}_1, \cdots, \boldsymbol{x}_m\}$, $\mathcal{X}' = \{\boldsymbol{y}_1, \cdots, \boldsymbol{y}_m\}$, the empirical means are

$$
\hat{\mu}_x^{(1)} = \frac{1}{m} \sum_{i \in [m]} x_i^{(1)}, \quad \hat{\mu}_x^{(2)} = \frac{1}{m} \sum_{i \in [m]} x_i^{(2)}, \quad \hat{\mu}_x^{(3)} = \frac{1}{m} \sum_{i \in [m]} x_i^{(3)},
$$

$$
\hat{\mu}_y^{(1)} = \frac{1}{m} \sum_{i \in [m]} y_i^{(1)}, \quad \hat{\mu}_y^{(2)} = \frac{1}{m} \sum_{i \in [m]} y_i^{(2)}, \quad \hat{\mu}_y^{(3)} = \frac{1}{m} \sum_{i \in [m]} y_i^{(3)}.
$$

Regardless of the distribution type, the surrogate distortion, i.e., Wasserstein-2 distance between $\mathcal{X}$ and $\mathcal{X}'$, satisfies

$$
\tilde{\Delta}_{\mathcal{M}_g} = \mathfrak{D} \left(\mathcal{P}_\mathcal{X} \| \mathcal{P}_{\mathcal{X}'}\right) \geq \sqrt{\left(\hat{\mu}_x^{(1)} - \hat{\mu}_y^{(1)}\right)^2 + \left(\hat{\mu}_x^{(2)} - \hat{\mu}_y^{(2)}\right)^2 + \left(\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}\right)^2}.
$$

We analyze the theoretical lower bounds of surrogate metrics under different privacy formulations as follows.

For union privacy, we have

$$\tilde{\Delta}_{\mathcal{M}_g} \geq \sqrt{\left(\hat{\mu}_x^{(1)} - \hat{\mu}_y^{(1)}\right)^2 + \left(\hat{\mu}_x^{(2)} - \hat{\mu}_y^{(2)}\right)^2 + \left(\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}\right)^2}$$

$$= \sqrt{\epsilon_1^2 \cdot \frac{|\hat{\mu}_x^{(1)} - \hat{\mu}_y^{(1)}|^2}{\epsilon_1^2} + \epsilon_2^2 \cdot \frac{|\hat{\mu}_x^{(2)} - \hat{\mu}_y^{(2)}|^2}{\epsilon_2^2} + \epsilon_3^2 \cdot \frac{|\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}|^2}{\epsilon_3^2}}$$

$$\geq \sqrt{\epsilon_1^2 + \epsilon_2^2 + \epsilon_3^2} \cdot \min_{i \in [3]} \left\{ \frac{|\hat{\mu}_x^{(i)} - \hat{\mu}_y^{(i)}|}{\epsilon_i} \right\}$$

$$= -\sqrt{\epsilon_1^2 + \epsilon_2^2 + \epsilon_3^2} \cdot \max_{i \in [3]} \left\{ -\frac{|\hat{\mu}_x^{(i)} - \hat{\mu}_y^{(i)}|}{\epsilon_i} \right\}$$

$$= -\sqrt{\epsilon_1^2 + \epsilon_2^2 + \epsilon_3^2} \cdot \tilde{\Pi}_{\epsilon,\omega_\Theta}^{\text{union}}.$$

For intersection privacy, we have

$$\tilde{\Delta}_{\mathcal{M}_g} \geq \sqrt{\left(\hat{\mu}_x^{(1)} - \hat{\mu}_y^{(1)}\right)^2 + \left(\hat{\mu}_x^{(2)} - \hat{\mu}_y^{(2)}\right)^2 + \left(\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}\right)^2}$$

$$= \sqrt{\epsilon_1^2 \cdot \frac{|\hat{\mu}_x^{(1)} - \hat{\mu}_y^{(1)}|^2}{\epsilon_1^2} + \epsilon_2^2 \cdot \frac{|\hat{\mu}_x^{(2)} - \hat{\mu}_y^{(2)}|^2}{\epsilon_2^2} + \epsilon_3^2 \cdot \frac{|\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}|^2}{\epsilon_3^2}}$$

$$\geq \min\{\epsilon_1, \epsilon_2, \epsilon_3\} \cdot \max_{i \in [3]} \left\{ \frac{|\hat{\mu}_x^{(i)} - \hat{\mu}_y^{(i)}|}{\epsilon_i} \right\}$$

$$= -\min\{\epsilon_1, \epsilon_2, \epsilon_3\} \cdot \min_{i \in [3]} \left\{ -\frac{|\hat{\mu}_x^{(i)} - \hat{\mu}_y^{(i)}|}{\epsilon_i} \right\}$$

$$= -\min\{\epsilon_1, \epsilon_2, \epsilon_3\} \tilde{\Pi}_{\epsilon,\omega_\Theta}^{\text{inter}}.$$

For group secrets privacy, let the means in the first two dimension be one group, and the third mean be one group. Then we have

$$\tilde{\Delta}_{\mathcal{M}_g} \geq \sqrt{\left(\hat{\mu}_x^{(1)} - \hat{\mu}_y^{(1)}\right)^2 + \left(\hat{\mu}_x^{(2)} - \hat{\mu}_y^{(2)}\right)^2 + \left(\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}\right)^2}$$

$$= \sqrt{\epsilon_1^2 \cdot \frac{|\hat{\mu}_x^{(1)} - \hat{\mu}_y^{(1)}|^2}{\epsilon_1^2} + \epsilon_2^2 \cdot \frac{|\hat{\mu}_x^{(2)} - \hat{\mu}_y^{(2)}|^2}{\epsilon_2^2} + \epsilon_3^2 \cdot \frac{|\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}|^2}{\epsilon_3^2}}$$

$$\geq \sqrt{\min\{\epsilon_1^2, \epsilon_2^2\} \cdot \max_{i \in [2]} \left\{ \frac{|\hat{\mu}_x^{(i)} - \hat{\mu}_y^{(i)}|^2}{\epsilon_i^2} \right\} + \epsilon_3^2 \cdot \frac{|\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}|^2}{\epsilon_3^2}}$$

$$\geq \sqrt{\min\{\epsilon_1^2, \epsilon_2^2\} + \epsilon_3^2} \cdot \min \left\{ \max_{i \in [2]} \left\{ \frac{|\hat{\mu}_x^{(i)} - \hat{\mu}_y^{(i)}|}{\epsilon_i} \right\}, \frac{|\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}|}{\epsilon_3} \right\}$$

$$= -\sqrt{\min\{\epsilon_1^2, \epsilon_2^2\} + \epsilon_3^2} \cdot \max \left\{ \min_{i \in [2]} \left\{ -\frac{|\hat{\mu}_x^{(i)} - \hat{\mu}_y^{(i)}|}{\epsilon_i} \right\}, -\frac{|\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}|}{\epsilon_3} \right\}$$

$$= -\sqrt{\min\{\epsilon_1^2, \epsilon_2^2\} + \epsilon_3^2} \cdot \tilde{\Pi}_{\epsilon,\omega_\Theta}^{\text{group}}.$$

For $l_p$ norm privacy with $p = 1$, we have

$$
\begin{aligned}
\tilde{\Delta}_{\mathcal{M}_g} &\geq \sqrt{\left(\hat{\mu}_x^{(1)} - \hat{\mu}_y^{(1)}\right)^2 + \left(\hat{\mu}_x^{(2)} - \hat{\mu}_y^{(2)}\right)^2 + \left(\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}\right)^2} \\
&\geq \frac{\sqrt{3}}{3}\left(|\hat{\mu}_x^{(1)} - \hat{\mu}_y^{(1)}| + |\hat{\mu}_x^{(2)} - \hat{\mu}_y^{(2)}| + |\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}|\right) \\
&= \frac{\sqrt{3}}{3}\varepsilon_1 \cdot \left(|\hat{\mu}_x^{(1)} - \hat{\mu}_y^{(1)}| + |\hat{\mu}_x^{(2)} - \hat{\mu}_y^{(2)}| + |\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}|\right) / \varepsilon_1 \\
&= -\frac{\sqrt{3}}{3}\varepsilon_1 \cdot \tilde{\Pi}_{\epsilon,\omega_\Theta}^{l_1}.
\end{aligned}
$$

For $l_p$ norm privacy with $p = \infty$, we have

$$
\begin{aligned}
\tilde{\Delta}_{\mathcal{M}_g} &\geq \sqrt{\left(\hat{\mu}_x^{(1)} - \hat{\mu}_y^{(1)}\right)^2 + \left(\hat{\mu}_x^{(2)} - \hat{\mu}_y^{(2)}\right)^2 + \left(\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}\right)^2} \\
&\geq \max_{i \in [3]}\left\{|\hat{\mu}_x^{(i)} - \hat{\mu}_y^{(i)}|\right\} \\
&\geq \varepsilon_\infty \cdot \max_{i \in [3]}\left\{|\hat{\mu}_x^{(i)} - \hat{\mu}_y^{(i)}|\right\} / \varepsilon_\infty \\
&= -\varepsilon_\infty \cdot \tilde{\Pi}_{\epsilon,\omega_\Theta}^{l_\infty}.
\end{aligned}
$$

# C  Comparsion Between Union Privacy and Group Secrets Privacy

When the group size $\beta$ is equal to $d$, group secrets privacy transforms into union privacy. As shown in Prop. C.1, Thm. 4.1 provides a tighter (i.e., higher) distortion lower bound for the union privacy compared with Thm. 5.3 when $\beta = d$.

**Proposition C.1.** *Given a privacy budget $T$ and tolerance ranges $\epsilon_1, \cdots, \epsilon_d$, Thm. 4.1 provides a tighter distortion lower bound for union privacy compared with Thm. 5.3 when $\beta = d$.*

*Proof.* When $\beta = d$, the distortion lower bound for the union privacy in Thm. 5.3, denoted as $\Delta_g$, is

$$
\Delta_g = 2\gamma_g \left\lceil \frac{1}{1 - (1-T)^{1/d}} \right\rceil \left(\prod_{i \in [d]} \epsilon_i\right)^{1/d} - 2\gamma_g \cdot \frac{1}{d}\sum_{i \in [d]} \epsilon_i,
$$

where $\gamma_g \triangleq \inf_{\theta_1, \theta_2 \in \text{Supp}(\omega_\Theta)} \frac{\frac{1}{2}\mathfrak{D}\left(\omega_{X_{\theta_1}} \| \omega_{X_{\theta_2}}\right)}{\frac{1}{d}\sum_{i \in [d]}|g_i(\theta_1) - g_i(\theta_2)|}$.

The distortion lower bound for the union privacy in Thm. 4.1, denoted as $\Delta_u$, is

$$
\Delta_u = 2\gamma_u \left\lceil \frac{1}{1 - (1-T)^{1/d}} \right\rceil \left(\prod_{i \in [d]} \epsilon_i\right)^{1/d} - 2\gamma_u \left(\prod_{i \in [d]} \epsilon_i\right)^{1/d},
$$

where $\gamma_u \triangleq \inf_{\theta_1, \theta_2 \in \text{Supp}(\omega_\Theta)} \frac{\frac{1}{2}\mathfrak{D}\left(\omega_{X_{\theta_1}} \| \omega_{X_{\theta_2}}\right)}{\prod_{i \in [d]}|g_i(\theta_1) - g_i(\theta_2)|^{1/d}}$.

According to the inequality of arithmetic and geometric means, we have

$$
\frac{1}{d}\sum_{i \in [d]} \epsilon_i \geq \left(\prod_{i \in [d]} \epsilon_i\right)^{1/d},
$$

$$
\frac{1}{d}\sum_{i \in [d]}|g_i(\theta_1) - g_i(\theta_2)| \geq \prod_{i \in [d]}|g_i(\theta_1) - g_i(\theta_2)|^{1/d}.
$$

Therefore, we can get that $\gamma_u \geq \gamma_g$ as well as

$$
\begin{aligned}
\Delta_u &= 2\gamma_u \left| \frac{1}{1-(1-T)^{1/d}} - 1 \right| \left( \prod_{i \in [d]} \epsilon_i \right)^{1/d} \\
&\geq 2\gamma_g \left| \frac{1}{1-(1-T)^{1/d}} - 1 \right| \left( \prod_{i \in [d]} \epsilon_i \right)^{1/d} \\
&= 2\gamma_g \left| \frac{1}{1-(1-T)^{1/d}} \right| \left( \prod_{i \in [d]} \epsilon_i \right)^{1/d} - 2\gamma_g \left( \prod_{i \in [d]} \epsilon_i \right)^{1/d} \\
&\geq 2\gamma_g \left| \frac{1}{1-(1-T)^{1/d}} \right| \left( \prod_{i \in [d]} \epsilon_i \right)^{1/d} - 2\gamma_g \cdot \frac{1}{d} \sum_{i \in [d]} \epsilon_i \\
&= \Delta_g.
\end{aligned}
$$

Hence, Thm. 4.1 provides a tighter distortion lower bound for union privacy compared with Thm. 5.3 when $\beta = d$. $\qquad\square$

# D    Alternative Privacy Metrics: $l_p$ Norm Summary Statistic Privacy

In this section, we consider the scenario where the data holder aims to ensure a significant separation between the original and the attacker guessed secret vectors, rather than emphasizing whether a single or a group of secrets are disclosed. For example, consider the cluster performance traces with secrets as the proportions of different server types. The data holder may care more about whether the attacker can approximate the overall deployment of servers.

We adopt $l_p$ norm $(p > 0)$ as the distance metric and define the $l_p$ *norm privacy* metric as the probability of the $l_p$ norm distance between the attacker guessed secret vector $\hat{\boldsymbol{g}}$ and the original secret vector $\boldsymbol{g}$ being within a tolerance $\varepsilon_p$, taking the best attack strategy:

$$
\Pi^{l_p}_{\epsilon,\omega_\Theta} \triangleq \sup_{\hat{\boldsymbol{g}}} \ \mathbb{P}\left( \|\hat{\boldsymbol{g}}(\theta') - \boldsymbol{g}(\theta)\|_p \leq \varepsilon_p \right) \ . \tag{21}
$$

Under $l_p$ norm privacy, given a privacy budget $T$, we then present a general lower bound on distortion.

**Theorem D.1** (Lower bound of privacy-distortion tradeoff for $l_p$ norm privacy)**.** *Let $D\left(X_{\theta_1}, X_{\theta_2}, =\right) \frac{1}{2}\mathfrak{D}\left(\omega_{X_{\theta_1}} \| \omega_{X_{\theta_2}}\right)$. Further, let $R^{l_p}\left(X_{\theta_1}\right)X_{\theta_2} = \frac{1}{d}\sum_{i \in [d]}|g_i(\theta_1) - g_i(\theta_2)|$ and*

$$
\gamma^{l_p} = \inf_{\theta_1, \theta_2 \in Supp(\omega_\Theta)} \frac{D\left(X_{\theta_1}, X_{\theta_2}\right)}{R^{l_p}\left(X_{\theta_1}, X_{\theta_2}\right)}.
$$

*Then, for tolerance ranges $\varepsilon_p$ as defined in Eq. (21) and for any mechanism $\mathcal{M}_g$ subject to privacy budget $\Pi^{l_p}_{\epsilon,\omega_\Theta} \leq T < 1$, we have*

$$
\Delta_{\mathcal{M}_g} > 2\gamma^{l_p}\left( \left\lceil \frac{1}{T} \right\rceil^{1/d} - 1 \right) \varepsilon_p / d^{\frac{1}{p}}.
$$

(Proof in App. D.1.) From Thm. D.1, we know that the distortion lower bound is positively correlated to the tolerance range $\varepsilon_p$ and negatively correlated to the privacy budget $T$. As shown in Prop. D.2, $l_p$ norm privacy metric is less strict than union privacy but stricter than intersection privacy.

**Proposition D.2.** *For union and intersection privacy, let $\epsilon_1, \cdots, \epsilon_d$ be the tolerance ranges. Let the tolerance $\varepsilon_p$ for $l_p$ norm privacy be $\varepsilon_p = \left( \sum_{i \in [d]} \epsilon_i^p \right)^{1/p}$. Given a privacy budget $T$, for any $p > 0$, we have*

$$\Delta^{inter} \leq \Delta^{l_p} \leq \Delta^{union},$$

*where $\Delta^{union}$, $\Delta^{inter}$, and $\Delta^{l_p}$ represents the achievable distortion lower bounds for union privacy, intersection privacy, and $l_p$ norm privacy respectively.*

The proof and further analysis for $l_p$ norm privacy with different norm order $p$ are detailed in App. D.2.

## D.1 Proof of Thm. D.1

*Proof.* When $\Pi_{\epsilon,\omega_\Theta} = \sup_{\hat{g}} \ \mathbb{P} \left( \| \hat{g}(\theta') - g(\theta) \|_p \leq \varepsilon_p \right) \leq T$, we can get that for any non-negative values $\epsilon_1, \epsilon_2, \cdots, \epsilon_d$ that satisfy $\left( \sum_{i \in [d]} \epsilon_i^p \right)^{1/p} = \varepsilon_p$:

$$\sup_{\hat{g}} \ \mathbb{P} \left( \bigcap_{i \in [d]} | \hat{g}_i(\theta') - g_i(\theta) | \leq \epsilon_i \right) \leq T.$$

This is because if there exists non-negative values $\tilde{\epsilon}_1, \tilde{\epsilon}_2, \cdots, \tilde{\epsilon}_d$ that satisfy $\left( \sum_{i \in d} \tilde{\epsilon}_i^p \right)^{1/p} = \varepsilon_p$ and

$$\sup_{\hat{g}} \ \mathbb{P} \left( \bigcap_{i \in [d]} | \hat{g}_i(\theta') - g_i(\theta) | \leq \tilde{\epsilon}_i \right) > T,$$

then we can get that

$$\sup_{\hat{g}} \ \mathbb{P} \left( \| \hat{g}(\theta') - g(\theta) \|_p \leq \varepsilon_p \right) \geq \mathbb{P} \left( \| \tilde{g}(\theta') - g(\theta) \|_p \leq \varepsilon_p \right)$$

$$\geq \mathbb{P} \left( \bigcap_{i \in [d]} | \tilde{g}_i(\theta') - g_i(\theta) | \leq \tilde{\epsilon}_i \right)$$

$$= \sup_{\hat{g}} \ \mathbb{P} \left( \bigcap_{i \in [d]} | \hat{g}_i(\theta') - g_i(\theta) | \leq \tilde{\epsilon}_i \right)$$

$$> T,$$

which contradicts with the constraint that $\sup_{\hat{g}} \ \mathbb{P} \left( \| \hat{g}(\theta') - g(\theta) \|_p \leq \varepsilon_p \right) \leq T$.

Based on Thm. 5.1, we know that when $\sup_{\hat{g}} \ \mathbb{P} \left( \bigcap_{i \in [d]} | \hat{g}_i(\theta') - g_i(\theta) | \leq \epsilon_i \right) \leq T$, the distortion satisfies

$$\Delta_{\mathcal{M}_g} > 2\gamma^{l_p} \cdot \left\lceil \frac{1}{T} \right\rceil^{1/d} \cdot \left( \prod_{i \in [d]} \epsilon_i \right)^{1/d} - 2\gamma^{l_p} \cdot \frac{1}{d} \sum_{i \in [d]} \epsilon_i.$$

When $\epsilon_i = \varepsilon_p / d^{\frac{1}{p}}$ for all $i \in [d]$, we can get that

$$\Delta_{\mathcal{M}_g} > 2\gamma^{l_p} \cdot \left( \left\lceil \frac{1}{T} \right\rceil^{1/d} - 1 \right) \cdot \varepsilon_p / d^{\frac{1}{p}}.$$

$\square$

16

## D.2  Proof of Prop. D.2 and More Analysis of $l_p$ Norm Privacy

### D.2.1  Proof of Prop. D.2

*Proof.* We first prove that for any fixed distortion budget $\delta_0$, when $\Delta \leq \delta_0$, the achievable lower bounds for union privacy $\Pi^{\text{union}}_{\epsilon,\omega_\Theta}$, intersection privacy $\Pi^{\text{inter}}_{\epsilon,\omega_\Theta}$, and $l_p$ norm privacy $\Pi^{l_p}_{\epsilon,\omega_\Theta}$ satisfy $\Pi^{\text{inter}}_{\epsilon,\omega_\Theta} \leq \Pi^{l_p}_{\epsilon,\omega_\Theta} \leq \Pi^{\text{union}}_{\epsilon,\omega_\Theta}$.

For any attack strategy $\hat{\boldsymbol{g}}$ and data release mechanism $\mathcal{M}_g$ that satisfies $\Delta \leq \delta_0$, when $|\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i$, $\forall i \in [d]$, we have $\|\hat{\boldsymbol{g}}(\theta') - \boldsymbol{g}(\theta)\|_p \leq \left( \sum_{i \in [d]} \epsilon_i^p \right)^{1/p} = \varepsilon_p$. Besides, when $\|\hat{\boldsymbol{g}}(\theta') - \boldsymbol{g}(\theta)\|_p \leq \varepsilon_p$, there exists $i \in [d]$, such that $|\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i$. Therefore, we can get that

$$\mathbb{P}\left( \bigcap_{i \in [d]} |\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i \right) \leq \mathbb{P}\left( \|\hat{\boldsymbol{g}}(\theta') - \boldsymbol{g}(\theta)\|_p \leq \varepsilon_p \right) \leq \mathbb{P}\left( \bigcup_{i \in [d]} |\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i \right).$$

Hence, for any data release mechanism $\mathcal{M}_g$ that satisfies $\Delta \leq \delta_0$:

$$\sup_{\hat{\boldsymbol{g}}} \mathbb{P}\left( \bigcap_{i \in [d]} |\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i \right) \leq \sup_{\hat{\boldsymbol{g}}} \mathbb{P}\left( \|\hat{\boldsymbol{g}}(\theta') - \boldsymbol{g}(\theta)\|_p \leq \varepsilon_p \right) \leq \sup_{\hat{\boldsymbol{g}}} \mathbb{P}\left( \bigcup_{i \in [d]} |\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i \right),$$

which indicates that with a fixed distortion budget $\delta_0$, $\Pi^{\text{inter}}_{\epsilon,\omega_\Theta} \leq \Pi^{l_p}_{\epsilon,\omega_\Theta} \leq \Pi^{\text{union}}_{\epsilon,\omega_\Theta}$. Therefore, we can easily get that with a privacy budget $T$, the achievable distortion lower bounds for union privacy $\Delta^{\text{union}}$, intersection privacy $\Delta^{\text{inter}}$, and $l_p$ norm privacy $\Delta^{l_p}$ satisfy $\Delta^{\text{union}} \geq \Delta^{l_p} \geq \Delta^{\text{inter}}$. $\qquad\square$

### D.2.2  More Analysis of $l_p$ Norm Privacy

In this section, we compare the distortion lower bounds for $l_p$ norm privacy with different norm order $p$.

**Proposition D.3.** *Consider two $l_p$ norm privacy metrics with norm orders $p = \alpha$ and $p = \tau$ respectively. If $\alpha \geq \tau > 0$, and their tolerance ranges satisfy $\frac{\varepsilon_\tau}{\varepsilon_\alpha} \geq d^{\frac{1}{\tau} - \frac{1}{\alpha}}$, given a privacy budget $T$, we have*

$$\Delta^{l_\alpha} \leq \Delta^{l_\tau},$$

*where $\Delta^{l_\alpha}$ and $\Delta^{l_\tau}$ are the achievable distortion lower bounds for $l_p$ norm privacy with $p = \alpha$ and $p = \tau$ respectively.*

*Proof.* We first prove that for any fixed distortion budget $\delta_0$, when $\Delta \leq \delta_0$, the achievable lower bound for $l_\tau$ privacy, denoted as $\Pi^{l_\tau}_{\epsilon,\omega_\Theta}$, is no smaller than that for $l_\alpha$ privacy, denoted as $\Pi^{l_\alpha}_{\epsilon,\omega_\Theta}$.

For any attack strategy $\hat{\boldsymbol{g}}$ and data release mechanism $\mathcal{M}_g$ that satisfies $\Delta \leq \delta_0$, we have $d^{\frac{1}{\tau} - \frac{1}{\alpha}} \|\hat{\boldsymbol{g}}(\theta') - \boldsymbol{g}(\theta)\|_\alpha \geq \|\hat{\boldsymbol{g}}(\theta') - \boldsymbol{g}(\theta)\|_\tau$. Therefore, when $\|\hat{\boldsymbol{g}}(\theta') - \boldsymbol{g}(\theta)\|_\alpha \leq \varepsilon_\alpha$, we can get that

$$\|\hat{\boldsymbol{g}}(\theta') - \boldsymbol{g}(\theta)\|_\tau \leq d^{\frac{1}{\tau} - \frac{1}{\alpha}} \|\hat{\boldsymbol{g}}(\theta') - \boldsymbol{g}(\theta)\|_\alpha \leq d^{\frac{1}{\tau} - \frac{1}{\alpha}} \varepsilon_\alpha \leq \varepsilon_\tau,$$

which indicates that

$$\mathbb{P}\left( \|\hat{\boldsymbol{g}}(\theta') - \boldsymbol{g}(\theta)\|_\alpha \leq \varepsilon_\alpha \right) \leq \mathbb{P}\left( \|\hat{\boldsymbol{g}}(\theta') - \boldsymbol{g}(\theta)\|_\tau \leq \varepsilon_\tau \right).$$

Then we can get that for any data release mechanism $\mathcal{M}_g$ that satisfies $\Delta \leq \delta_0$:

$$\sup_{\hat{\boldsymbol{g}}} \mathbb{P}\left( \|\hat{\boldsymbol{g}}(\theta') - \boldsymbol{g}(\theta)\|_\alpha \leq \varepsilon_\alpha \right) \leq \sup_{\hat{\boldsymbol{g}}} \mathbb{P}\left( \|\hat{\boldsymbol{g}}(\theta') - \boldsymbol{g}(\theta)\|_\tau \leq \varepsilon_\tau \right),$$

which indicates that with a fixed distortion budget $\delta_0$, $\Pi^{l_\alpha}_{\epsilon,\omega_\Theta} \leq \Pi^{l_\tau}_{\epsilon,\omega_\Theta}$. Hence, we can easily get that with a privacy budget $T$, the achievable distortion lower bounds for $l_\alpha$ privacy $\Delta^{l_\alpha}$ and $l_\tau$ privacy $\Delta^{l_\tau}$ satisfy $\Delta^{l_\alpha} \leq \Delta^{l_\tau}$. $\qquad\square$

# E   Case Study: Secrets = $\{\text{mean}, \text{SD}\}^d$, distribution = Multivariate Gaussian

In this section, we first focus on 2-dimensional Gaussian distribution, and then generalize the data release mechanism for multivariate Gaussian distribution.

For 2-dimensional Gaussian distribution $\mathcal{N}(\boldsymbol{\mu}, \Sigma)$, the distribution parameters can be represented as $\boldsymbol{\mu} = [\mu_1, \mu_2]$, and

$$\Sigma = \begin{bmatrix} \sigma_1^2 & \sigma_{12} \\ \sigma_{21} & \sigma_2^2 \end{bmatrix} = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix},$$

where $\alpha \in [0, \pi)$. We can see that the 2-dimensional Gaussian distribution is determined by five independent parameters $\theta = (\mu_1, \mu_2, \lambda_1, \lambda_2, \alpha)$. We consider $d$ secrets, where $d \leq 4$, and each secret can be either mean or standard deviation of any dimension of the distribution, i.e., $g_i \in \{\mu_1, \mu_2, \sigma_1, \sigma_2\}$, $\forall i \in [d]$. Let $\mathcal{G} = \{g_i\}_{i \in [d]}$ be the secret set. We first instantiate the privacy-distortion tradeoff lower bound for 2-dimensional Gaussian in Prop. E.1.

**Proposition E.1.** *For* 2*-dimensional Gaussian distribution with distribution parameters* $\theta = (\mu_1, \mu_2, \lambda_1, \lambda_2, \alpha)$, *consider* $d$ *secrets* $(d \leq 4)$, *where each secret satisfies* $g_i(\theta) \in \{\mu_1, \mu_2, \sigma_1, \sigma_2\}$, $\forall i \in [d]$. *For any* $T \in (0, 1)$, *when* $\Pi_{\epsilon, \omega_\Theta} \leq T$,

$$\Delta_{\mathcal{M}_g} > \sqrt{d} \cdot \left[ \frac{1}{1 - (1 - T)^{1/d}} - 1 \right] \cdot \left( \prod_{i \in [d]} \epsilon_i \right)^{1/d}.$$

The proof is shown in App. E.1. We then design a quantization data release mechanism to approximate the tradeoff lower bound. Intuitively, if the secret is a mean $\mu_i$ $(i \in \{1, 2\})$, we partition the range of possible values of it into intervals of lengths $s_{\mu_i}$. Otherwise, we divide the ranges of possible values of $\sqrt{\lambda_1}, \sqrt{\lambda_2}$ into intervals of lengths $s_a$ and $s_b$. The mechanism then outputs the midpoints of the respective intervals into which the original distribution parameters fit. Precisely, the designed mechanism is shown in Alg. 2. Here we use independent parameters $(\mu_1, \mu_2, \lambda_1, \lambda_2, \alpha)$ so that the attacker cannot infer the value of a parameter based on any other parameters.

---

**Algorithm 2:** Data release mechanism for 2-dimensional Gaussian with $d$ secrets.

**Input** : $\theta = (\mu_1, \mu_2, \lambda_1, \lambda_2, \alpha)$, lower bounds $\underline{\mu_1}, \underline{\mu_2}, \underline{a}, \underline{b}$ for parameters $\mu_1, \mu_2, a = \sqrt{\lambda_1}, b = \sqrt{\lambda_2}$, quantization intervals $s_{\mu_1}, s_{\mu_2}, s_a, s_b$, secret set $\mathcal{G}$.

1 **for** each $i \in \{1, 2\}$:
2      **if** $\mu_i \in \mathcal{G}$: $\mu_i' \leftarrow \underline{\mu_i} + \left( \lfloor \frac{\mu_i - \underline{\mu_i}}{s_{\mu_i}} \rfloor + 0.5 \right) \cdot s_{\mu_i}$;
3      **else**: $\mu_i' \leftarrow \mu_i$;
4 **if** $\{\sigma_1, \sigma_2\} \cap \mathcal{G} \neq \emptyset$:
5      $a' \leftarrow \underline{a} + \left( \lfloor \frac{a - \underline{a}}{s_a} \rfloor + 0.5 \right) \cdot s_a$;
6      $b' \leftarrow \underline{b} + \left( \lfloor \frac{b - \underline{b}}{s_b} \rfloor + 0.5 \right) \cdot s_b$;
7 **else**: $a' \leftarrow a, b' \leftarrow b$;
     **Output:** Gaussian distribution with parameter $\theta' = \left( \mu_1', \mu_2', a'^2, b'^2, \alpha \right)$.

---

For the mechanism privacy-distortion analysis, we consider the case where the prior distributions of parameters $\mu_1, \mu_2, \sqrt{\lambda_1}, \sqrt{\lambda_2}$ are uniform.

**Proposition E.2** (Mechanism privacy-distortion tradeoff). *Under the assumption that the distribution parameters $\mu_1, \mu_2, \sqrt{\lambda_1}, \sqrt{\lambda_2}$ follow the uniform distribution, Alg. 2 has*

$$\Pi_{\epsilon,\omega_\Theta} \leq P_\mu + P_\sigma - P_\mu P_\sigma,$$

$$\Delta_{\mathcal{M}_g} = \frac{1}{2} \sqrt{\sum_{i:\mu_i \in \mathcal{G}} s_{\mu_i}^2 + \mathbb{1}_{\{\sigma_1,\sigma_2\} \cap \mathcal{G} \neq \emptyset} \cdot (s_a^2 + s_b^2)},$$

*where* $P_\mu = 1 - \prod_{i=\{1,2\}} \left(1 - \mathbb{1}_{\mu_i \in \mathcal{G}} \cdot \frac{2\epsilon_{\mu_i}}{s_{\mu_i}}\right)$, $P_\sigma = \mathbb{1}_{(\sigma_1 \in \mathcal{G}) \cap (\sigma_2 \notin \mathcal{G})} \cdot P_{\sigma_1} + \mathbb{1}_{(\sigma_1 \notin \mathcal{G}) \cap (\sigma_2 \in \mathcal{G})} \cdot P_{\sigma_2} + \mathbb{1}_{(\sigma_1 \in \mathcal{G}) \cap (\sigma_2 \in \mathcal{G})} \cdot P_{\sigma_1,\sigma_2}$, $P_{\sigma_1} = 1 - \mathbb{1}_{\left(L_{\sigma_1}^{(\alpha)} > 0\right) \cap \left(L_{\sigma_1}^{(\beta)} > 0\right)} \cdot \frac{1}{2} L_{\sigma_1}^{(\alpha)} L_{\sigma_1}^{(\beta)} / s_a s_b$, $P_{\sigma_2} = 1 - \mathbb{1}_{\left(L_{\sigma_2}^{(\alpha)} > 0\right) \cap \left(L_{\sigma_2}^{(\beta)} > 0\right)} \cdot \frac{1}{2} L_{\sigma_2}^{(\alpha)} L_{\sigma_2}^{(\beta)} / s_a s_b$,

$P_{\sigma_1,\sigma_2} = 1 - \mathbb{1}_{\left(L_{\sigma_1,\sigma_2}^{(\alpha)} > 0\right) \cap \left(L_{\sigma_1,\sigma_2}^{(\beta)} > 0\right)} \cdot \frac{1}{2} L_{\sigma_1,\sigma_2}^{(\alpha)} L_{\sigma_1,\sigma_2}^{(\beta)} / s_a s_b$, *and*

$$L_{\sigma_1}^{(\alpha)} = s_a - 2\frac{\epsilon_{\sigma_1}}{\cos\alpha} - \sqrt{2}\epsilon_{\sigma_1} \cos\alpha, \qquad L_{\sigma_1}^{(\beta)} = s_b - 2\frac{\epsilon_{\sigma_1}}{\sin\alpha} - \sqrt{2}\epsilon_{\sigma_1} \sin\alpha,$$

$$L_{\sigma_2}^{(\alpha)} = s_a - 2\frac{\epsilon_{\sigma_2}}{\sin\alpha} - \sqrt{2}\epsilon_{\sigma_2} \sin\alpha, \qquad L_{\sigma_2}^{(\beta)} = s_b - 2\frac{\epsilon_{\sigma_2}}{\cos\alpha} - \sqrt{2}\epsilon_{\sigma_2} \cos\alpha,$$

$$L_{\sigma_1,\sigma_2}^{(\alpha)} = s_a - \max\left\{\frac{\epsilon_{\sigma_1}}{\cos\alpha}, \frac{\epsilon_{\sigma_2}}{\sin\alpha}\right\} - \max\left\{\frac{\epsilon_{\sigma_1}}{\cos\alpha} + \sqrt{2}\epsilon_{\sigma_1} \cos\alpha, \frac{\epsilon_{\sigma_2}}{\sin\alpha} + \sqrt{2}\epsilon_{\sigma_2} \sin\alpha\right\},$$

$$L_{\sigma_1,\sigma_2}^{(\beta)} = s_b - \max\left\{\frac{\epsilon_{\sigma_1}}{\sin\alpha}, \frac{\epsilon_{\sigma_2}}{\cos\alpha}\right\} - \max\left\{\frac{\epsilon_{\sigma_1}}{\sin\alpha} + \sqrt{2}\epsilon_{\sigma_1} \sin\alpha, \frac{\epsilon_{\sigma_2}}{\cos\alpha} + \sqrt{2}\epsilon_{\sigma_2} \cos\alpha\right\}.$$

The proof is shown in App. E.5.

Drawing upon the similar idea used in the data release mechanism for 2-dimensional Gaussian distribution, we proceed to design a general mechanism suitable for multivariate Gaussian distributions as follows.

For a $k$-dimensional Gaussian distribution ($k \in \mathbb{Z}^+$), it can be fully characterized by $3k - 1$ independent parameters denoted as $\theta = (\mu_1, \cdots, \mu_k, \lambda_1, \cdots, \lambda_k, \alpha_1, \cdots, \alpha_{k-1})$. Here, $\mu_1, \cdots, \mu_k$ represent the means, while $\lambda_1, \cdots, \lambda_k$ and $\alpha_1, \cdots, \alpha_{k-1}$ correspond to the eigenvalues and eigenvectors of the covariance matrix, respectively. We consider $d$ secrets, where $d \leq 2k$, and each secret can be either mean or standard deviation of any dimension of the distribution, i.e., $g_i \in \{\mu_1, \cdots, \mu_k, \sigma_1, \cdots, \sigma_k\}$, $\forall i \in [d]$. Let $\mathcal{G} = \{g_i\}_{i \in [d]}$ be the secret set.

Similar to Alg. 2, we design a quantization data release mechanism. If a secret is mean $\mu_i$ ($i \in [k]$), we partition the range of possible values of it into intervals of lengths $s_{\mu_i}$. Otherwise, we divide the ranges of possible values for $\sqrt{\lambda_1}, \cdots, \sqrt{\lambda_k}$ into intervals with lengths $s_{a_1}, \cdots, s_{a_k}$. Subsequently, this mechanism outputs the midpoints of the respective intervals into which the original distribution parameters fit. Precisely, the designed mechanism is shown in Alg. 3.

---

**Algorithm 3:** Data release mechanism for multivariate Gaussian with $d$ secrets.

**Input** : $\theta = (\mu_1, \cdots, \mu_k, \lambda_1, \cdots, \lambda_k, \alpha_1, \cdots, \alpha_{k-1})$, lower bounds $\underline{\mu_1}, \cdots, \underline{\mu_k}, \underline{a_1}, \cdots, \underline{a_k}$ for parameters $\mu_1, \cdots, \mu_k, a_1 = \sqrt{\lambda_1}, \cdots, a_k = \sqrt{\lambda_k}$, quantization intervals $s_{\mu_1}, \cdots, s_{\mu_k}, s_{a_1}, \cdots, s_{a_k}$, secret set $\mathcal{G}$.

1 **for** each $i \in [k]$:

2     **if** $\mu_i \in \mathcal{G}$: $\mu_i' \leftarrow \underline{\mu_i} + \left(\lfloor \frac{\mu_i - \underline{\mu_i}}{s_{\mu_i}} \rfloor + 0.5\right) \cdot s_{\mu_i}$;

3     **else**: $\mu_i' \leftarrow \mu_i$;

4 **if** $\{\sigma_1, \cdots, \sigma_k\} \cap \mathcal{G} \neq \emptyset$:

5     **for** each $i \in [k]$: $a_i' \leftarrow \underline{a_i} + \left(\lfloor \frac{a_i - \underline{a_i}}{s_{a_i}} \rfloor + 0.5\right) \cdot s_{a_i}$;

6 **else**: **for** each $i \in [k]$: $a_i' \leftarrow a_i$;

**Output:** Gaussian distribution with parameter $\theta' = \left(\mu_1', \cdots, \mu_k', {a_1'}^2, \cdots, {a_k'}^2, \alpha_1, \cdots, \alpha_{k-1}\right)$

---

## E.1 Proof of Prop. E.1

*Proof.* Let $\theta' = (\mu_1', \mu_2', \lambda_1', \lambda_2', \alpha')$. From [15], we have

$$\mathfrak{D}\left(\omega_{X_\theta} \| \omega_{X_{\theta'}}\right)^2 = (\mu_1 - \mu_1')^2 + (\mu_2 - \mu_2')^2 + \text{Tr}\left(\Sigma + \Sigma' - 2\left(\Sigma^{\frac{1}{2}}\Sigma'\Sigma^{\frac{1}{2}}\right)^{\frac{1}{2}}\right).$$

We provide a lower bound on $\mathfrak{D}\left(\omega_{X_\theta} \| \omega_{X_{\theta'}}\right)$ in Lemma E.3.

**Lemma E.3.** $\mathfrak{D}\left(\omega_{X_\theta} \| \omega_{X_{\theta'}}\right)^2$ *can be lower bounded as*

$$\mathfrak{D}\left(\omega_{X_\theta} \| \omega_{X_{\theta'}}\right)^2 \geq (\mu_1 - \mu_1')^2 + (\mu_2 - \mu_2')^2 + (\sigma_1 - \sigma_1')^2 + (\sigma_2 - \sigma_2')^2.$$

The proof is shown in App. E.2.
Based on Lemma E.3, we can get that

$$
\begin{aligned}
\frac{D\left(X_\theta, X_{\theta'}\right)}{R\left(X_\theta, X_{\theta'}\right)} &\geq \frac{\sqrt{\sum_{j\in[2]}\left(\mu_j - \mu_j'\right)^2 + \sum_{j\in[2]}\left(\sigma_j - \sigma_j'\right)^2}}{2\prod_{i\in[d]}|g_i(\theta) - g_i(\theta')|^{1/d}} \\
&\geq \frac{\sqrt{\sum_{i\in[d]}\left(g_i(\theta) - g_i(\theta')\right)^2}}{2\prod_{i\in[d]}|g_i(\theta) - g_i(\theta')|^{1/d}} \\
&= \frac{1}{2}\sqrt{\frac{\sum_{i\in[d]}\left(g_i(\theta) - g_i(\theta')\right)^2}{\prod_{i\in[d]}|g_i(\theta) - g_i(\theta')|^{2/d}}} \\
&\geq \frac{1}{2}\sqrt{d \cdot \frac{\prod_{i\in[d]}|g_i(\theta) - g_i(\theta')|^{2/d}}{\prod_{i\in[d]}|g_i(\theta) - g_i(\theta')|^{2/d}}} \\
&= \frac{\sqrt{d}}{2}.
\end{aligned}
$$

$\square$

## E.2 Proof of Lemma E.3

*Proof.* To proof Lemma E.3, we first provide two lemmas as follows.

**Lemma E.4.** $\mathfrak{D}\left(\omega_{X_\theta} \| \omega_{X_{\theta'}}\right)^2$ *can be derived as:*

$$
\begin{aligned}
\mathfrak{D}\left(\omega_{X_\theta} \| \omega_{X_{\theta'}}\right)^2 = {}&(\mu_1 - \mu_1')^2 + (\mu_2 - \mu_2')^2 + \lambda_1 + \lambda_1' + \lambda_2 + \lambda_2' \\
&- 2\sqrt{(\lambda_1\lambda_1' + \lambda_2\lambda_2')\cos^2(\alpha - \alpha') + (\lambda_1\lambda_2' + \lambda_2\lambda_1')\sin^2(\alpha - \alpha') + 2\sqrt{\lambda_1\lambda_1'\lambda_2\lambda_2'}}.
\end{aligned}
$$

The proof is shown in App. E.3.

**Lemma E.5.**

$$\sigma_1\sigma_1' + \sigma_2\sigma_2' \geq \sqrt{(\lambda_1\lambda_1' + \lambda_2\lambda_2')\cos^2(\alpha - \alpha') + (\lambda_1\lambda_2' + \lambda_2\lambda_1')\sin^2(\alpha - \alpha') + 2\sqrt{\lambda_1\lambda_1'\lambda_2\lambda_2'}}.$$

The proof is in App. E.4

Based on Lemma E.4 and Lemma E.5, we have

$$
\begin{aligned}
\mathfrak{D}\left(\omega_{X_\theta}\|\omega_{X_{\theta'}}\right)^2 &= (\mu_1 - \mu_1')^2 + (\mu_2 - \mu_2')^2 + \lambda_1 + \lambda_1' + \lambda_2 + \lambda_2' \\
&\quad - 2\sqrt{(\lambda_1\lambda_1' + \lambda_2\lambda_2')\cos^2(\alpha - \alpha') + (\lambda_1\lambda_2' + \lambda_2\lambda_1')\sin^2(\alpha - \alpha') + 2\sqrt{\lambda_1\lambda_1'\lambda_2\lambda_2'}} \\
&= (\mu_1 - \mu_1')^2 + (\mu_2 - \mu_2')^2 + \sigma_1^2 + \sigma_2^2 + {\sigma_1'}^2 + {\sigma_2'}^2 \\
&\quad - 2\sqrt{(\lambda_1\lambda_1' + \lambda_2\lambda_2')\cos^2(\alpha - \alpha') + (\lambda_1\lambda_2' + \lambda_2\lambda_1')\sin^2(\alpha - \alpha') + 2\sqrt{\lambda_1\lambda_1'\lambda_2\lambda_2'}} \\
&\geq (\mu_1 - \mu_1')^2 + (\mu_2 - \mu_2')^2 + \sigma_1^2 + \sigma_2^2 + {\sigma_1'}^2 + {\sigma_2'}^2 - 2\sigma_1\sigma_1' - 2\sigma_2\sigma_2' \\
&= (\mu_1 - \mu_1')^2 + (\mu_2 - \mu_2')^2 + (\sigma_1 - \sigma_1')^2 + (\sigma_2 - \sigma_2')^2.
\end{aligned}
$$

$\square$

## E.3  Proof of Lemma E.4

*Proof.* Define $A = \left(\Sigma^{\frac{1}{2}}\Sigma'\Sigma^{\frac{1}{2}}\right)^{\frac{1}{2}}$, and we have

$$
(\mathrm{Tr}A)^2 = \mathrm{Tr}\left(A^2\right) + 2\det(A).
$$

We can get that

$$
\mathrm{Tr}\left(A^2\right) = \mathrm{Tr}\left(\Sigma^{\frac{1}{2}}\Sigma'\Sigma^{\frac{1}{2}}\right) = \mathrm{Tr}\left(\Sigma^{\frac{1}{2}}\Sigma^{\frac{1}{2}}\Sigma'\right) = \mathrm{Tr}\left(\Sigma\Sigma'\right),
$$

where

$$
\begin{aligned}
\Sigma\Sigma' &= \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} \cos\alpha' & -\sin\alpha' \\ \sin\alpha' & \cos\alpha' \end{bmatrix} \begin{bmatrix} \lambda_1' & 0 \\ 0 & \lambda_2' \end{bmatrix} \begin{bmatrix} \cos\alpha' & \sin\alpha' \\ -\sin\alpha' & \cos\alpha' \end{bmatrix} \\
&= \begin{bmatrix} \lambda_1\cos\alpha & -\lambda_2\sin\alpha \\ \lambda_1\sin\alpha & \lambda_2\cos\alpha \end{bmatrix} \begin{bmatrix} \cos(\alpha'-\alpha) & -\sin(\alpha'-\alpha) \\ \sin(\alpha'-\alpha) & \cos(\alpha'-\alpha) \end{bmatrix} \begin{bmatrix} \lambda_1'\cos\alpha' & \lambda_1'\sin\alpha' \\ -\lambda_2'\sin\alpha' & \lambda_2'\cos\alpha' \end{bmatrix}.
\end{aligned}
$$

Therefore, we have

$$
\begin{aligned}
\mathrm{Tr}\left(A^2\right) &= \mathrm{Tr}\left(\Sigma\Sigma'\right) \\
&= \lambda_1\lambda_1'\cos\alpha\cos\alpha'\cos(\alpha'-\alpha) - \lambda_2\lambda_1'\sin\alpha\cos\alpha'\sin(\alpha'-\alpha) + \lambda_1\lambda_2'\cos\alpha\sin\alpha'\sin(\alpha'-\alpha) \\
&\quad + \lambda_2\lambda_2'\sin\alpha\sin\alpha'\cos(\alpha'-\alpha) + \lambda_1\lambda_1'\sin\alpha\sin\alpha'\cos(\alpha'-\alpha) + \lambda_2\lambda_1'\cos\alpha\sin\alpha'\sin(\alpha'-\alpha) \\
&\quad - \lambda_1\lambda_2'\sin\alpha\cos\alpha'\sin(\alpha'-\alpha) + \lambda_2\lambda_2'\cos\alpha\cos\alpha'\cos(\alpha'-\alpha) \\
&= (\lambda_1\lambda_1' + \lambda_2\lambda_2')\cos^2(\alpha - \alpha') + (\lambda_1\lambda_2' + \lambda_2\lambda_1')\sin^2(\alpha - \alpha').
\end{aligned}
$$

As for $\det(A)$, we have

$$
\det(A) = \sqrt{\det(A^2)} = \sqrt{\det\left(\Sigma^{\frac{1}{2}}\Sigma'\Sigma^{\frac{1}{2}}\right)} = \sqrt{\det(\Sigma)\det(\Sigma')} = \sqrt{\lambda_1\lambda_1'\lambda_2\lambda_2'}.
$$

Therefore, we have

$$
\begin{aligned}
(\mathrm{Tr}A)^2 &= \mathrm{Tr}\left(A^2\right) + 2\det(A) \\
&= (\lambda_1\lambda_1' + \lambda_2\lambda_2')\cos^2(\alpha - \alpha') + (\lambda_1\lambda_2' + \lambda_2\lambda_1')\sin^2(\alpha - \alpha') + 2\sqrt{\lambda_1\lambda_1'\lambda_2\lambda_2'}.
\end{aligned}
$$

Hence,

$$
\begin{aligned}
\mathfrak{D}\left(\omega_{X_\theta}\|\omega_{X_{\theta'}}\right)^2 &= (\mu_1 - \mu_1')^2 + (\mu_2 - \mu_2')^2 + \mathrm{Tr}\left(\Sigma + \Sigma' - 2A\right) \\
&= (\mu_1 - \mu_1')^2 + (\mu_2 - \mu_2')^2 + \mathrm{Tr}(\Sigma) + \mathrm{Tr}(\Sigma') - 2\mathrm{Tr}(A) \\
&= (\mu_1 - \mu_1')^2 + (\mu_2 - \mu_2')^2 + \lambda_1 + \lambda_1' + \lambda_2 + \lambda_2' \\
&\quad - 2\sqrt{(\lambda_1\lambda_1' + \lambda_2\lambda_2')\cos^2(\alpha - \alpha') + (\lambda_1\lambda_2' + \lambda_2\lambda_1')\sin^2(\alpha - \alpha') + 2\sqrt{\lambda_1\lambda_1'\lambda_2\lambda_2'}}.
\end{aligned}
$$

$\square$

## E.4 Proof of Lemma E.5

*Proof.* Let $a = \sqrt{\lambda_1}, b = \sqrt{\lambda_2}, \tilde{a} = \sqrt{\lambda_1'}$ and $\tilde{b} = \sqrt{\lambda_2'}$. We can get that

$$A \triangleq \sigma_1\sigma_1' + \sigma_2\sigma_2' = \sqrt{\left(a^2\cos^2\alpha + b^2\sin^2\alpha\right)\left(\tilde{a}^2\cos^2\alpha' + \tilde{b}^2\sin^2\alpha'\right)} + \sqrt{\left(a^2\sin^2\alpha + b^2\cos^2\alpha\right)\left(\tilde{a}^2\sin^2\alpha' + \tilde{b}^2\cos^2\alpha'\right)},$$

and

$$B \triangleq \sqrt{(\lambda_1\lambda_1' + \lambda_2\lambda_2')\cos^2(\alpha - \alpha') + (\lambda_1\lambda_2' + \lambda_2\lambda_1')\sin^2(\alpha - \alpha') + 2\sqrt{\lambda_1\lambda_1'\lambda_2\lambda_2'}}$$

$$= \sqrt{\left(a\tilde{a} + b\tilde{b}\right)^2\cos^2(\alpha - \alpha') + \left(a\tilde{b} + b\tilde{a}\right)^2\sin^2(\alpha - \alpha')}.$$

We then can derive that

$$A^2 - B^2 = 2\sqrt{\left(a^2\cos^2\alpha + b^2\sin^2\alpha\right)\left(\tilde{a}^2\cos^2\alpha' + \tilde{b}^2\sin^2\alpha'\right)\left(a^2\sin^2\alpha + b^2\cos^2\alpha\right)\left(\tilde{a}^2\sin^2\alpha' + \tilde{b}^2\cos^2\alpha'\right)}$$

$$- 2a\tilde{a}b\tilde{b} - 2\cos\alpha\cos\alpha'\sin\alpha\sin\alpha'\left(a^2\tilde{a}^2 + b^2\tilde{b}^2 - a^2\tilde{b}^2 - b^2\tilde{a}^2\right).$$

Let

$$C \triangleq \sqrt{\left(a^2\cos^2\alpha + b^2\sin^2\alpha\right)\left(\tilde{a}^2\cos^2\alpha' + \tilde{b}^2\sin^2\alpha'\right)\left(a^2\sin^2\alpha + b^2\cos^2\alpha\right)\left(\tilde{a}^2\sin^2\alpha' + \tilde{b}^2\cos^2\alpha'\right)},$$

$$D \triangleq a\tilde{a}b\tilde{b} + \cos\alpha\cos\alpha'\sin\alpha\sin\alpha'\left(a^2\tilde{a}^2 + b^2\tilde{b}^2 - a^2\tilde{b}^2 - b^2\tilde{a}^2\right).$$

We can get that

$$C^2 = a^2\tilde{a}^2b^2\tilde{b}^2\left(\cos^4\alpha + \sin^4\alpha\right)\left(\cos^4\alpha' + \sin^4\alpha'\right) + a^4\tilde{a}^2\tilde{b}^2\cos^2\alpha\sin^2\alpha\left(\cos^4\alpha' + \sin^4\alpha'\right)$$

$$+ a^2b^2\tilde{b}^4\cos^2\alpha'\sin^2\alpha'\left(\cos^4\alpha + \sin^4\alpha\right) + \tilde{a}^2b^4\tilde{b}^2\cos^2\alpha\sin^2\alpha\left(\cos^4\alpha' + \sin^4\alpha'\right)$$

$$+ a^2\tilde{a}^4b^2\cos^2\alpha'\sin^2\alpha'\left(\cos^4\alpha + \sin^4\alpha\right)$$

$$= a^2\tilde{a}^2b^2\tilde{b}^2\left(1 - 2\cos^2\alpha\sin^2\alpha\right)\left(1 - 2\cos^2\alpha'\sin^2\alpha'\right) + \left(a^4 + b^4\right)\tilde{a}^2\tilde{b}^2\cos^2\alpha\sin^2\alpha\left(1 - 2\cos^2\alpha'\sin^2\alpha'\right)$$

$$+ \left(\tilde{a}^4 + \tilde{b}^4\right)a^2b^2\cos^2\alpha'\sin^2\alpha'\left(1 - 2\cos^2\alpha\sin^2\alpha\right),$$

and

$$D^2 = a^2\tilde{a}^2b^2\tilde{b}^2\left(1 + 4\cos^2\alpha\cos^2\alpha'\sin^2\alpha\sin^2\alpha'\right) + 2\cos\alpha\cos\alpha'\sin\alpha\sin\alpha'a\tilde{a}b\tilde{b}\left(a^2\tilde{a}^2 + b^2\tilde{b}^2 - a^2\tilde{b}^2 - b^2\tilde{a}^2\right)$$

$$- 2\cos^2\alpha\cos^2\alpha'\sin^2\alpha\sin^2\alpha'\left(\left(a^4 + b^4\right)\tilde{a}^2\tilde{b}^2 + \left(\tilde{a}^4 + \tilde{b}^4\right)a^2b^2\right).$$

Then we have

$$C^2 - D^2 = \cos^2\alpha\sin^2\alpha\left(a^4 + b^4\right)\tilde{a}^2\tilde{b}^2 + \cos^2\alpha'\sin^2\alpha'\left(\tilde{a}^4 + \tilde{b}^4\right)a^2b^2 - 2a^2\tilde{a}^2b^2\tilde{b}^2\left(\cos^2\alpha\sin^2\alpha + \cos^2\alpha'\sin^2\alpha'\right)$$

$$- 2\cos\alpha\cos\alpha'\sin\alpha\sin\alpha'a\tilde{a}b\tilde{b}\left(a^2\tilde{a}^2 + b^2\tilde{b}^2 - a^2\tilde{b}^2 - b^2\tilde{a}^2\right)$$

$$= \cos^2\alpha\sin^2\alpha\left(a^2 - b^2\right)^2\tilde{a}^2\tilde{b}^2 + \cos^2\alpha'\sin^2\alpha'\left(\tilde{a}^2 - \tilde{b}^2\right)^2a^2b^2 - 2\cos\alpha\cos\alpha'\sin\alpha\sin\alpha'a\tilde{a}b\tilde{b}\left(a^2 - b^2\right)\left(\tilde{a}^2 - \tilde{b}^2\right)$$

$$\geq 2\sqrt{\cos^2\alpha\sin^2\alpha\cos^2\alpha'\sin^2\alpha'\tilde{a}^2\tilde{b}^2a^2b^2\left(a^2 - b^2\right)^2\left(\tilde{a}^2 - \tilde{b}^2\right)^2} - 2\cos\alpha\cos\alpha'\sin\alpha\sin\alpha'a\tilde{a}b\tilde{b}\left(a^2 - b^2\right)\left(\tilde{a}^2 - \tilde{b}^2\right)$$

$$= 0$$

Since $C \geq 0$, we have $C \geq D$. Therefore, we have

$$A^2 - B^2 = 2\left(C - D\right) \geq 0.$$

Since $A \geq 0$, we have $A \geq B$, i.e.,

$$\sigma_1\sigma_1' + \sigma_2\sigma_2' \geq \sqrt{(\lambda_1\lambda_1' + \lambda_2\lambda_2')\cos^2(\alpha - \alpha') + (\lambda_1\lambda_2' + \lambda_2\lambda_1')\sin^2(\alpha - \alpha') + 2\sqrt{\lambda_1\lambda_1'\lambda_2\lambda_2'}}.$$

$\square$

## E.5   Proof of Prop. E.2

*Proof.* Regarding the notation, we define $\theta' = (\mu'_1, \mu'_2, \lambda'_1, \lambda'_2, \alpha')$, $a = \sqrt{\lambda_1}, b = \sqrt{\lambda_2}, \tilde{a} = \sqrt{\lambda'_1}, \tilde{b} = \sqrt{\lambda'_2}$. As for the distortion, since $\alpha' = \alpha$, we have

$$
\begin{aligned}
\mathfrak{D}\left(\omega_{X_\theta} \| \omega_{X_{\theta'}}\right)^2 &= (\mu_1 - \mu'_1)^2 + (\mu_2 - \mu'_2)^2 + \lambda_1 + \lambda'_1 + \lambda_2 + \lambda'_2 \\
&\quad - 2\sqrt{(\lambda_1\lambda'_1 + \lambda_2\lambda'_2)\cos^2(\alpha - \alpha') + (\lambda_1\lambda'_2 + \lambda_2\lambda'_1)\sin^2(\alpha - \alpha') + 2\sqrt{\lambda_1\lambda'_1\lambda_2\lambda'_2}} \\
&= (\mu_1 - \mu'_1)^2 + (\mu_2 - \mu'_2)^2 + \lambda_1 + \lambda'_1 + \lambda_2 + \lambda'_2 - 2\sqrt{\left(\sqrt{\lambda_1\lambda'_1} + \sqrt{\lambda_2\lambda'_2}\right)^2} \\
&= (\mu_1 - \mu'_1)^2 + (\mu_2 - \mu'_2)^2 + a^2 + \tilde{a}^2 + b^2 + \tilde{b}^2 - 2a\tilde{a} - 2b\tilde{b} \\
&= (\mu_1 - \mu'_1)^2 + (\mu_2 - \mu'_2)^2 + \left(a^2 - \tilde{a}^2\right)^2 + \left(b^2 - \tilde{b}^2\right)^2. \\
&\le \frac{1}{4}\left(\sum_{i:\mu_i\in\mathcal{G}} s^2_{\mu_i} + \mathbb{1}_{\{\sigma_1,\sigma_2\}\cap\mathcal{G}\neq\emptyset} \cdot \left(s^2_a + s^2_b\right)\right).
\end{aligned}
$$

Therefore, we have

$$
\Delta_{\mathcal{M}_g} = \sup_{\substack{\theta\in\mathrm{Supp}(\omega_\Theta), \\ \theta'\in\mathrm{Supp}(\mathcal{M}_g(\theta))}} \mathfrak{D}\left(\omega_{X_\theta} \| \omega_{X_{\theta'}}\right) = \frac{1}{2}\sqrt{\sum_{i:\mu_i\in\mathcal{G}} s^2_{\mu_i} + \mathbb{1}_{\{\sigma_1,\sigma_2\}\cap\mathcal{G}\neq\emptyset} \cdot (s^2_a + s^2_b)}.
$$

As for the privacy, we first provide a lemma as follows.

**Lemma E.6.** *Let* $\delta_{\sigma_1,\alpha} = \frac{\epsilon_{\sigma_1}}{\cos\alpha}$, $\delta_{\sigma_1,\beta} = \frac{\epsilon_{\sigma_1}}{\sin\alpha}$, $\delta_{\sigma_2,\alpha} = \frac{\epsilon_{\sigma_2}}{\sin\alpha}$ *and* $\delta_{\sigma_2,\beta} = \frac{\epsilon_{\sigma_2}}{\cos\alpha}$. *For all* $a, b \ge 0$, *we have*

$$
\sqrt{(a + \delta_{\sigma_1,\alpha})^2 \cos^2\alpha + (b + \delta_{\sigma_1,\beta})^2 \sin^2\alpha} \ge \sqrt{a^2\cos^2\alpha + b^2\sin^2\alpha} + \epsilon_{\sigma_1},
$$

$$
\sqrt{(a + \delta_{\sigma_2,\alpha})^2 \sin^2\alpha + (b + \delta_{\sigma_2,\beta})^2 \cos^2\alpha} \ge \sqrt{a^2\sin^2\alpha + b^2\cos^2\alpha} + \epsilon_{\sigma_2}.
$$

*Let* $\delta'_{\sigma_1,\alpha} = \frac{\epsilon_{\sigma_1}}{\cos\alpha} + \sqrt{2}\epsilon_{\sigma_1}\cos\alpha$, $\delta'_{\sigma_1,\beta} = \frac{\epsilon_{\sigma_1}}{\sin\alpha} + \sqrt{2}\epsilon_{\sigma_1}\sin\alpha$. *For all* $a \ge \delta'_{\sigma_1,\alpha}, b \ge \delta'_{\sigma_1,\beta}$, *we have*

$$
\sqrt{\left(a - \delta'_{\sigma_1,\alpha}\right)^2 \cos^2\alpha + \left(b - \delta'_{\sigma_1,\beta}\right)^2 \sin^2\alpha} \le \sqrt{a^2\cos^2\alpha + b^2\sin^2\alpha} - \epsilon_{\sigma_1}.
$$

*Let* $\delta'_{\sigma_2,\alpha} = \frac{\epsilon_{\sigma_2}}{\sin\alpha} + \sqrt{2}\epsilon_{\sigma_2}\sin\alpha$ *and* $\delta'_{\sigma_2,\beta} = \frac{\epsilon_{\sigma_2}}{\cos\alpha} + \sqrt{2}\epsilon_{\sigma_2}\cos\alpha$. *For all* $a \ge \delta'_{\sigma_2,\alpha}, b \ge \delta'_{\sigma_2,\beta}$, *we have*

$$
\sqrt{\left(a - \delta'_{\sigma_2,\alpha}\right)^2 \sin^2\alpha + \left(b - \delta'_{\sigma_2,\beta}\right)^2 \cos^2\alpha} \le \sqrt{a^2\sin^2\alpha + b^2\cos^2\alpha} - \epsilon_{\sigma_2}.
$$

The proof is shown in App. E.6.

Suppose the parameters Alg. 2 releases satisfy $\tilde{a} = \underline{a} + \left(I_a + \frac{1}{2}\right) \cdot s_a$ and $\tilde{b} = \underline{b} + \left(I_b + \frac{1}{2}\right) \cdot s_b$, and let the secret value $g_{\sigma_1}(\theta)$ that the optimal attack strategy guesses be $\hat{\sigma}_1$. Then there exist $\hat{a}$ and $\hat{b}$ that satisfy $\hat{a}^2\cos^2\alpha + \hat{b}^2\sin^2\alpha = \hat{\sigma}_1^2$, where

$$
\left\{(\hat{a} < \underline{a} + I_a s_a) \cap \left(\hat{b} < \underline{b} + I_b s_b\right)\right\} \cup \left\{(I_a s_a \le \hat{a} \le \underline{a} + (I_a + 1) \cdot s_a) \cap \left(\underline{b} + I_b s_b \le \hat{b} \le \underline{b} + (I_b + 1) \cdot s_b\right)\right\}
$$

$$
\cup \left\{(\hat{a} > \underline{a} + ((I_a + 1) \cdot s_a)) \cap \left(\hat{b} > \underline{b} + (I_b + 1) \cdot s_b\right)\right\} = \text{True}.
$$

The probability of the attacker guessing the secret $\sigma_1$ within the tolerance range is:

$$
\mathbb{P}\left(|\hat{g}_{\sigma_1}(\theta') - g_{\sigma_1}(\theta)| \le \epsilon_{\sigma_1}\right) = \mathbb{P}\left(\left|\sqrt{\hat{a}^2\cos^2\alpha + \hat{b}^2\sin^2\alpha} - \sqrt{a^2\cos^2\alpha + b^2\sin^2\alpha}\right| \le \epsilon_{\sigma_1}\right)
$$

Based on Lemma E.6, we have

$$\sqrt{\left(\hat{a} - \delta'_{\sigma_1,\alpha}\right)^2 \cos^2 \alpha + \left(\hat{b} - \delta'_{\sigma_1,\beta}\right)^2 \sin^2 \alpha} \le \sqrt{\hat{a}^2 \cos^2 \alpha + \hat{b}^2 \sin^2 \alpha} - \epsilon_{\sigma_1},$$

when $\hat{a} \ge \delta'_{\sigma_1,\alpha}, \hat{b} \ge \delta'_{\sigma_1,\beta}$, and

$$\sqrt{\left(\hat{a} + \delta_{\sigma_1,\alpha}\right)^2 \cos^2 \alpha + \left(\hat{b} + \delta_{\sigma_1,\beta}\right)^2 \sin^2 \alpha} \ge \sqrt{\hat{a}^2 \cos^2 \alpha + \hat{b}^2 \sin^2 \alpha} + \epsilon_{\sigma_1}.$$

Let $\hat{a} = \underline{a} + (I_a + t_a) \cdot s_a$ and $\hat{b} = \underline{b} + (I_b + t_b) \cdot s_b$, where $t_a, t_b \in (-\infty, 0)$ or $t_a, t_b \in [0, 1]$ or $t_a, t_b \in (1, \infty)$. Besides, the original parameter $a, b$ satisfy $a \in [\underline{a} + I_a \cdot s_a, \ \underline{a} + (I_a + 1) \cdot s_a)$ and $b \in [\underline{b} + I_b \cdot s_b, \ \underline{b} + (I_b + 1) \cdot s_b)$. Therefore, we can get that

$$\mathbb{P}\left(|\hat{g}_{\sigma_1}(\theta') - g_{\sigma_1}(\theta)| \le \epsilon_{\sigma_1}\right) = \mathbb{P}\Bigg[\left(\sqrt{a^2 \cos^2 \alpha + b^2 \sin^2 \alpha} \ge \sqrt{\hat{a}^2 \cos^2 \alpha + \hat{b}^2 \sin^2 \alpha} - \epsilon_{\sigma_1}\right) \cup$$

$$\left(\sqrt{a^2 \cos^2 \alpha + b^2 \sin^2 \alpha} \le \sqrt{\hat{a}^2 \cos^2 \alpha + \hat{b}^2 \sin^2 \alpha} + \epsilon_{\sigma_1}\right)\Bigg]$$

$$\le \sup_{\hat{a},\hat{b}} \Big(1 - \max\left\{t_a s_a - \delta'_{\sigma_1,\alpha}, 0\right\} \cdot \max\left\{t_b s_b - \delta'_{\sigma_1,\beta}, 0\right\}/s_a s_b$$

$$- \max\left\{(1 - t_a) s_a - \delta_{\sigma_1,\alpha}, 0\right\} \cdot \max\left\{(1 - t_b) s_b - \delta_{\sigma_1,\beta}, 0\right\}/s_a s_b\Big).$$

Let $x = t_a s_a - \delta'_{\sigma_1,\alpha}$, $y = t_b s_b - \delta'_{\sigma_1,\beta}$, $L^{(\alpha)}_{\sigma_1} = s_a - 2\frac{\epsilon_{\sigma_1}}{\cos \alpha} - \sqrt{2}\epsilon_{\sigma_1} \cos \alpha$ and $L^{(\beta)}_{\sigma_1} = s_b - 2\frac{\epsilon_{\sigma_1}}{\sin \alpha} - \sqrt{2}\epsilon_{\sigma_1} \sin \alpha$, we have

$$\mathbb{P}\left(|\hat{g}_{\sigma_1}(\theta') - g_{\sigma_1}(\theta)| \le \epsilon_{\sigma_1}\right) \le \sup_{x,y} \Big(1 - \max\{x, 0\} \cdot \max\{y, 0\}/s_a s_b$$

$$- \max\left\{s_a - \delta_{\sigma_1,\alpha} - \delta'_{\sigma_1,\alpha} - x, 0\right\} \cdot \max\left\{s_b - \delta_{\sigma_1,\beta} - \delta'_{\sigma_1,\beta} - y, 0\right\}/s_a s_b\Big)$$

$$= 1 - \frac{1}{2}\max\left\{s_a - \delta_{\sigma_1,\alpha} - \delta'_{\sigma_1,\alpha}, 0\right\} \cdot \max\left\{s_b - \delta_{\sigma_1,\beta} - \delta'_{\sigma_1,\beta}, 0\right\}/s_a s_b$$

$$= \begin{cases} 1, & L^{(\alpha)}_{\sigma_1} \le 0 \text{ or } L^{(\beta)}_{\sigma_1} \le 0 \\ 1 - \frac{1}{2} L^{(\alpha)}_{\sigma_1} L^{(\beta)}_{\sigma_1}/s_a s_b, & \text{otherwise} \end{cases}$$

$$= P_{\sigma_1}.$$

Similarly, let $L^{(\alpha)}_{\sigma_2} = s_a - 2\frac{\epsilon_{\sigma_2}}{\sin \alpha} - \sqrt{2}\epsilon_{\sigma_2} \sin \alpha$ and $L^{(\beta)}_{\sigma_2} = s_b - 2\frac{\epsilon_{\sigma_2}}{\cos \alpha} - \sqrt{2}\epsilon_{\sigma_2} \cos \alpha$, we can get that

$$\mathbb{P}\left(|\hat{g}_{\sigma_2}(\theta') - g_{\sigma_2}(\theta)| \le \epsilon_{\sigma_2}\right) \le \sup_{\hat{a},\hat{b}} \Big(1 - \max\left\{t_a s_a - \delta'_{\sigma_2,\alpha}, 0\right\} \cdot \max\left\{t_b s_b - \delta'_{\sigma_2,\beta}, 0\right\}/s_a s_b$$

$$- \max\left\{(1 - t_a) s_a - \delta_{\sigma_2,\alpha}, 0\right\} \cdot \max\left\{(1 - t_b) s_b - \delta_{\sigma_2,\beta}, 0\right\}/s_a s_b\Big)$$

$$= \begin{cases} 1, & L^{(\alpha)}_{\sigma_2} \le 0 \text{ or } L^{(\beta)}_{\sigma_2} \le 0 \\ 1 - \frac{1}{2} L^{(\alpha)}_{\sigma_2} L^{(\beta)}_{\sigma_2}/s_a s_b, & \text{otherwise} \end{cases}$$

$$= P_{\sigma_2}.$$

Let $L^{(\alpha)}_{\sigma_1,\sigma_2} = s_a - \max\left\{\frac{\epsilon_{\sigma_1}}{\cos \alpha}, \frac{\epsilon_{\sigma_2}}{\sin \alpha}\right\} - \max\left\{\frac{\epsilon_{\sigma_1}}{\cos \alpha} + \sqrt{2}\epsilon_{\sigma_1} \cos \alpha, \frac{\epsilon_{\sigma_2}}{\sin \alpha} + \sqrt{2}\epsilon_{\sigma_2} \sin \alpha\right\}$ and $L^{(\beta)}_{\sigma_1,\sigma_2} = s_b - $

$\max\left\{\frac{\epsilon_{\sigma_1}}{\sin\alpha}, \frac{\epsilon_{\sigma_2}}{\cos\alpha}\right\} - \max\left\{\frac{\epsilon_{\sigma_1}}{\sin\alpha} + \sqrt{2}\epsilon_{\sigma_1}\sin\alpha, \frac{\epsilon_{\sigma_2}}{\cos\alpha} + \sqrt{2}\epsilon_{\sigma_2}\cos\alpha\right\}$, we can get that

$$\mathbb{P}\left(|\hat{g}_{\sigma_1}(\theta') - g_{\sigma_1}(\theta)| \le \epsilon_{\sigma_1} \cup |\hat{g}_{\sigma_2}(\theta') - g_{\sigma_2}(\theta)| \le \epsilon_{\sigma_2}\right)$$

$$\le \sup_{\hat{a}, \hat{b}} \Big(1 - \max\left\{t_a s_a - \max\left\{\delta'_{\sigma_1,\alpha}, \delta'_{\sigma_2,\alpha}\right\}, 0\right\} \cdot \max\left\{t_b s_b - \max\left(\delta'_{\sigma_1,\beta}, \delta'_{\sigma_2,\beta}\right), 0\right\} / s_a s_b$$

$$- \max\left\{(1 - t_a) s_a - \max\left(\delta_{\sigma_1,\alpha}, \delta_{\sigma_2,\alpha}\right), 0\right\} \cdot \max\left\{(1 - t_b) s_b - \max\left(\delta_{\sigma_1,\beta}, \delta_{\sigma_2,\beta}\right), 0\right\} / s_a s_b\Big)$$

$$= \begin{cases} 1, & L^{(\alpha)}_{\sigma_1,\sigma_2} \le 0 \text{ or } L^{(\beta)}_{\sigma_1,\sigma_2} \le 0 \\ 1 - \frac{1}{2} L^{(\alpha)}_{\sigma_1,\sigma_2} L^{(\beta)}_{\sigma_1,\sigma_2} / s_a s_b, & \text{otherwise} \end{cases}$$

$$= P_{\sigma_1, \sigma_2}.$$

Besides, we have

$$\mathbb{P}\left(|\hat{g}_{\mu_1}(\theta') - g_{\mu_1}(\theta)| \le \epsilon_{\mu_1}\right) = \frac{2\epsilon_{\mu_1}}{s_{\mu_1}},$$

$$\mathbb{P}\left(|\hat{g}_{\mu_2}(\theta') - g_{\mu_2}(\theta)| \le \epsilon_{\mu_2}\right) = \frac{2\epsilon_{\mu_2}}{s_{\mu_2}},$$

$$\mathbb{P}\left(|\hat{g}_{\mu_1}(\theta') - g_{\mu_1}(\theta)| \le \epsilon_{\mu_1} \cup |\hat{g}_{\mu_2}(\theta') - g_{\mu_2}(\theta)| \le \epsilon_{\mu_2}\right) = \frac{2\epsilon_{\mu_1}}{s_{\mu_1}} + \frac{2\epsilon_{\mu_2}}{s_{\mu_2}} - \frac{4\epsilon_{\mu_1}\epsilon_{\mu_2}}{s_{\mu_1} s_{\mu_2}}.$$

Denote $P_\mu = 1 - \prod_{i=\{1,2\}} \left(1 - \mathbb{1}_{\mu_i \in \mathcal{G}} \cdot \frac{2\epsilon_{\mu_i}}{s_{\mu_i}}\right)$ and $P_\sigma = \mathbb{1}_{(\sigma_1 \in \mathcal{G}) \cap (\sigma_2 \notin \mathcal{G})} \cdot P_{\sigma_1} + \mathbb{1}_{(\sigma_1 \notin \mathcal{G}) \cap (\sigma_2 \in \mathcal{G})} \cdot P_{\sigma_2} + \mathbb{1}_{(\sigma_1 \in \mathcal{G}) \cap (\sigma_2 \in \mathcal{G})} \cdot P_{\sigma_1,\sigma_2}$. We can get that the privacy of Alg. 2 satisfies

$$\Pi_{\epsilon,\omega_\Theta} \le P_\mu + P_\sigma - P_\mu P_\sigma.$$

<div style="text-align:right">□</div>

## E.6 Proof of Lemma E.6

*Proof.* Let $A = \sqrt{(a + \delta_{\sigma_1,\alpha})^2 \cos^2\alpha + (b + \delta_{\sigma_1,\beta})^2 \sin^2\alpha}$ and $B = \sqrt{a^2 \cos^2\alpha + b^2 \sin^2\alpha} + \epsilon_{\sigma_1}$, we can get that

$$\begin{aligned} A^2 - B^2 &= 2a\epsilon_{\sigma_1} \cos\alpha + 2b\epsilon_{\sigma_1} \sin\alpha + \epsilon_{\sigma_1}^2 - 2\epsilon_{\sigma_1}\sqrt{a^2 \cos^2\alpha + b^2 \sin^2\alpha} \\ &\ge 2a\epsilon_{\sigma_1} \cos\alpha + 2b\epsilon_{\sigma_1} \sin\alpha + \epsilon_{\sigma_1}^2 - 2\epsilon_{\sigma_1}(a \cos\alpha + b \sin\alpha) \\ &= \epsilon_{\sigma_1}^2 \\ &\ge 0. \end{aligned}$$

Since $A \ge 0$, we have $A \ge B$, i.e.,

$$\sqrt{(a + \delta_{\sigma_1,\alpha})^2 \cos^2\alpha + (b + \delta_{\sigma_1,\beta})^2 \sin^2\alpha} \ge \sqrt{a^2 \cos^2\alpha + b^2 \sin^2\alpha} + \epsilon_{\sigma_1}.$$

Similarly, we can get that

$$\sqrt{(a + \delta_{\sigma_2,\alpha})^2 \sin^2\alpha + (b + \delta_{\sigma_2,\beta})^2 \cos^2\alpha} \ge \sqrt{a^2 \sin^2\alpha + b^2 \cos^2\alpha} + \epsilon_{\sigma_2}.$$

Let $C = \sqrt{\left(a - \delta'_{\sigma_1,\alpha}\right)^2 \cos^2 \alpha + \left(b - \delta'_{\sigma_1,\beta}\right)^2 \sin^2 \alpha}$, $D = \sqrt{a^2 \cos^2 \alpha + b^2 \sin^2 \alpha} - \epsilon_{\sigma_1}$. We have

$$
\begin{aligned}
C^2 - D^2 &= \epsilon_{\sigma_1}^2 - 2a\epsilon_{\sigma_1}\cos\alpha - 2b\epsilon_{\sigma_1}\sin\alpha + 2\epsilon_{\sigma_1}^2\left(\cos^4\alpha + \sin^4\alpha\right) - 2\sqrt{2}a\epsilon_{\sigma_1}\cos^3\alpha - 2\sqrt{2}b\epsilon_{\sigma_1}\sin^3\alpha + 2\sqrt{2}\epsilon_{\sigma_1}^2 \\
&\quad + 2\epsilon_{\sigma_1}\sqrt{a^2\cos^2\alpha + b^2\sin^2\alpha} \\
&\leq \epsilon_{\sigma_1}^2 + 2\epsilon_{\sigma_1}^2\left(\cos^4\alpha + \sin^4\alpha\right) - 2\sqrt{2}a\epsilon_{\sigma_1}\cos^3\alpha - 2\sqrt{2}b\epsilon_{\sigma_1}\sin^3\alpha + 2\sqrt{2}\epsilon_{\sigma_1}^2 \\
&\leq \epsilon_{\sigma_1}^2 + 2\epsilon_{\sigma_1}^2\left(\cos^4\alpha + \sin^4\alpha\right) - 2\sqrt{2}\left(\frac{\epsilon_{\sigma_1}}{\cos\alpha} + \sqrt{2}\epsilon_{\sigma_1}\cos\alpha\right)\epsilon_{\sigma_1}\cos^3\alpha \\
&\quad - 2\sqrt{2}\left(\frac{\epsilon_{\sigma_1}}{\sin\alpha} + \sqrt{2}\epsilon_{\sigma_1}\sin\alpha\right)\epsilon_{\sigma_1}\sin^3\alpha + 2\sqrt{2}\epsilon_{\sigma_1}^2 \\
&= \epsilon_{\sigma_1}^2 - 2\epsilon_{\sigma_1}^2\left(\cos^4\alpha + \sin^4\alpha\right) \\
&\leq 0.
\end{aligned}
$$

Since $D \geq 0$, we have $C \leq D$, i.e.,

$$
\sqrt{\left(a - \delta'_{\sigma_1,\alpha}\right)^2 \cos^2 \alpha + \left(b - \delta'_{\sigma_1,\beta}\right)^2 \sin^2 \alpha} \leq \sqrt{a^2 \cos^2 \alpha + b^2 \sin^2 \alpha} - \epsilon_{\sigma_1}.
$$

Similarly, we can get that

$$
\sqrt{\left(a - \delta'_{\sigma_2,\alpha}\right)^2 \sin^2 \alpha + \left(b - \delta'_{\sigma_2,\beta}\right)^2 \cos^2 \alpha} \leq \sqrt{a^2 \sin^2 \alpha + b^2 \cos^2 \alpha} - \epsilon_{\sigma_2}.
$$

$\square$

# F  Case studies under Alternative Privacy Metrics

Under intersection privacy, union privacy and $l_p$ norm privacy metrics, we instantiate the privacy-distortion lower bounds for multivariate Gaussian with dimensionally independent variables, and analyze the performance of Alg. 1.

## F.1  Intersection Privacy

Under the intersection privacy metric, we focus on the multivariate Gaussian with dimensionally independent variables, and provide the privacy-distortion lower bound in Prop. F.1.

**Proposition F.1.** *For $k$-dimensional Gaussian distribution with diagonal covariance matrix and distribution parameters $\theta = (\mu_1, \cdots, \mu_k, \sigma_1, \cdots, \sigma_k)$, consider $d$ secrets ($d \leq 2k$), where each secret satisfies $g_i(\theta) \in \{\mu_1, \cdots, \mu_k, \sigma_1, \cdots, \sigma_k\}$, $\forall i \in [d]$. For any $T \in (0,1)$, when $\Pi_{\epsilon,\omega_\Theta} \leq T$,*

$$
\Delta_{\mathcal{M}_g} > \sqrt{d} \cdot \left[\frac{1}{T}\right]^{1/d} \cdot \left(\prod_{i \in [d]} \epsilon_i\right)^{1/d} - \frac{1}{\sqrt{d}}\sum_{i \in [d]} \epsilon_i.
$$

The proof is shown in App. F.1.1. We then analyze the performance of Alg. 1 under intersection privacy as follows.

**Proposition F.2** (Mechanism privacy-distortion tradeoff under intersection privacy)**.** *Under the assumption that secret distribution parameters $g_1, \cdots, g_d$ follow the uniform distribution, Alg. 1 has*

$$
\Pi_{\epsilon,\omega_\Theta}^{inter} = \prod_{i \in [d]} \frac{2\epsilon_i}{s_{g_i}},
$$

$$
\Delta_{\mathcal{M}_g} = \sqrt{\sum_{i \in [d]} s_{g_i}^2} < c_{\epsilon,s} \cdot \Delta_{opt}.
$$

*where $c_{\epsilon,s}$ is a constant depending on tolerance ranges and the interval lengths of the mechanism, and $\Delta_{opt}$ is the optimal achievable distortion under the privacy achieved by Alg. 1.*

The proof is shown in App. F.1.2. From Prop. F.2 we know that Alg. 1 is order-optimal with a constant multiplication factor.

### F.1.1 Proof of Prop. F.1

Define $\theta' = (\mu'_1, \cdots, \mu'_k, \sigma'_1, \cdots, \sigma'_k)$. Based on Lemma B.1, we can get that

$$
\begin{aligned}
\frac{D\left(X_\theta, X_{\theta'}\right)}{R\left(X_\theta, X_{\theta'}\right)} &\geq \frac{\sqrt{\sum_{j\in[k]}\left(\mu_j - \mu'_j\right)^2 + \sum_{j\in[k]}\left(\sigma_j - \sigma'_j\right)^2}}{\frac{2}{d}\sum_{i\in[d]}|g_i(\theta) - g_i(\theta')|} \\
&\geq \frac{\sqrt{\sum_{i\in[d]}\left(g_i(\theta) - g_i(\theta')\right)^2}}{\frac{2}{d}\sum_{i\in[d]}|g_i(\theta) - g_i(\theta')|} \\
&\geq \frac{\frac{1}{\sqrt{d}}\sum_{i\in[d]}|g_i(\theta) - g_i(\theta')|}{\frac{2}{d}\sum_{i\in[d]}|g_i(\theta) - g_i(\theta')|} \\
&= \frac{\sqrt{d}}{2}.
\end{aligned}
$$

Therefore, we have

$$
\gamma^{\text{inter}} = \inf_{\theta_1, \theta_2 \in \text{Supp}(\omega_\Theta)} \frac{D\left(X_{\theta_1}, X_{\theta_2}\right)}{R\left(X_{\theta_1}, X_{\theta_2}\right)} = \frac{\sqrt{d}}{2}.
$$

Based on Thm. 5.1, we can get that

$$
\Delta_{\mathcal{M}_g} > \sqrt{d} \cdot \left[\frac{1}{T}\right]^{1/d} \cdot \left(\prod_{i\in[d]} \epsilon_i\right)^{1/d} - \frac{1}{\sqrt{d}}\sum_{i\in[d]} \epsilon_i.
$$

### F.1.2 Proof of Prop. F.2

*Proof.* Based on Lemma B.1, we can easily can get that the distortion $\Delta$ of Alg. 1 is

$$
\Delta_{\mathcal{M}_g} = \sqrt{\sum_{i\in[d]} s_{g_i}{}^2}.
$$

Since the secret distribution parameters are independent of each other and follow the uniform distributions, we can get that the privacy of Alg. 1 is

$$
\begin{aligned}
\Pi_{\epsilon, \omega_\Theta}^{\text{inter}} &= \sup_{\hat{g}} \ \mathbb{P}\left(\bigcap_{i\in[d]} |\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i\right) \\
&= \sup_{\hat{g}} \ \prod_{i\in[d]} \mathbb{P}\left(|\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i\right) \\
&= \prod_{i\in[d]} \frac{2\epsilon_i}{s_{g_i}}.
\end{aligned}
$$

From Prop. F.1, we know that the optimal achievable distortion $\Delta_{opt}$ satisfy

$$
\begin{aligned}
\Delta_{opt} &> \sqrt{d} \cdot \left[\frac{1}{\prod_{i\in[d]} \frac{2\epsilon_i}{s_{g_i}}}\right]^{1/d} \cdot \left(\prod_{i\in[d]} \epsilon_i\right)^{1/d} - \frac{1}{\sqrt{d}}\sum_{i\in[d]} \epsilon_i \\
&= \frac{\sqrt{d}}{2} \cdot \left(\prod_{i\in[d]} s_{g_i}\right)^{1/d} - \frac{1}{\sqrt{d}}\sum_{i\in[d]} \epsilon_i.
\end{aligned}
$$

Let $k = \frac{\Delta}{\Delta_{opt}}$, $x_i = \frac{\epsilon_i}{s_{g_i}}, \forall i \in [d]$, $c_1 = \min_{i \in [d]} \{x_i\}$, and $c_2 = \max_{i \in [d]} \{x_i\}$, we have

$$k < \frac{2\sqrt{\sum_{i \in [d]} s_{g_i}{}^2}}{\sqrt{d} \cdot \left(\prod_{i \in [d]} s_{g_i}\right)^{1/d} - \frac{2}{\sqrt{d}} \sum_{i \in [d]} \epsilon_i}$$

$$= \frac{2\sqrt{\sum_{i \in [d]} \left(\frac{\epsilon_i}{x_i}\right)^2}}{\sqrt{d} \cdot \left(\prod_{i \in [d]} \frac{\epsilon_i}{x_i}\right)^{1/d} - \frac{2}{\sqrt{d}} \sum_{i \in [d]} \epsilon_i}$$

$$\leq \frac{2c_2\sqrt{\sum_{i \in [d]} \epsilon_i^2}}{c_1\sqrt{d} \cdot \left(\prod_{i \in [d]} \epsilon_i\right)^{1/d} - \frac{2c_1 c_2}{\sqrt{d}} \sum_{i \in [d]} \epsilon_i}$$

$$= \frac{2c_2\sqrt{\sum_{i \in [d]} \epsilon_i^2/d}}{c_1 \left(\prod_{i \in [d]} \epsilon_i\right)^{1/d} - 2c_1 c_2 \sum_{i \in [d]} \epsilon_i/d}$$

$$\triangleq c_{\epsilon,s}.$$

Therefore, we can get that

$$\Delta_{\mathcal{M}_g} = k\Delta_{opt} < c_{\epsilon,s}\Delta_{opt},$$

where $c_{\epsilon,s}$ is a constant depending on tolerance ranges and the interval lengths of the mechanism.

Specifically, when $\epsilon_1 = \cdots = \epsilon_d$, and the designed data released mechanism satisfy $\frac{\epsilon_1}{s_{g_1}} = \cdots = \frac{\epsilon_d}{s_{g_d}} \leq \frac{1}{6}$, we can get that $\Delta < 3\Delta_{opt}$. $\qquad\square$

## F.2 Group Secrets Privacy

Under the group secrets privacy metric, we focus on the multivariate Gaussian with dimensionally independent variables, and provide the privacy-distortion lower bound in Prop. F.3.

**Proposition F.3.** *For $k$-dimensional Gaussian distribution with diagonal covariance matrix and distribution parameters $\theta = (\mu_1, \cdots, \mu_k, \sigma_1, \cdots, \sigma_k)$, consider $d$ secrets $(d \leq 2k)$, where each secret satisfies $g_i(\theta) \in \{\mu_1, \cdots, \mu_k, \sigma_1, \cdots, \sigma_k\}, \forall i \in [d]$. For any $T \in (0,1)$, when $\Pi_{\epsilon,\omega_\Theta} \leq T$,*

$$\Delta_{\mathcal{M}_g} > \sqrt{d} \left[\frac{1}{\left(1 - (1-T)^{1/\beta}\right)^{\beta/d}}\right] \left(\prod_{i \in [d]} \epsilon_i\right)^{1/d} - \frac{1}{\sqrt{d}} \sum_{i \in [d]} \epsilon_i.$$

The proof is shown in App. F.2.1. We then analyze the performance of Alg. 1 under group secrets privacy as follows.

**Proposition F.4** (Mechanism privacy-distortion tradeoff under group secrets privacy)**.** *Denote $\mathcal{B}$ as the set of the secrets groups, and $\mathcal{I}_b$ as the secret index set of group $b \in \mathcal{B}$. Under the assumption that secret distribution parameters $g_1, \cdots, g_d$ follow the uniform distribution, Alg. 1 has*

$$\Pi_{\epsilon,\omega_\Theta}^{group} = 1 - \prod_{b \in \mathcal{B}} \left(1 - \prod_{i \in \mathcal{I}_b} \frac{2\epsilon_i}{s_{g_i}}\right),$$

$$\Delta_{\mathcal{M}_g} = \sqrt{\sum_{i \in [d]} s_{g_i}{}^2} < c_{\epsilon,s,\mathcal{B}} \cdot \Delta_{opt}.$$

where $c_{\epsilon,s,\mathcal{B}}$ is a constant depending on tolerance ranges, the interval lengths of the mechanism, and the set of secret groups $\mathcal{B}$. $\Delta_{opt}$ is the optimal achievable distortion under the privacy achieved by Alg. 1.

The proof is shown in App. F.2.2. From Prop. F.4 we know that Alg. 1 is order-optimal with a constant multiplication factor.

For the 1-dimensional Gaussian scenario where $\theta = (\mu, \sigma)$, when $\mu$ and $\sigma$ are treated as distinct secret groups (i.e., $\mathcal{B} = \{\{\mu\}, \{\sigma\}\}$), the group secrets privacy is equivalent to the union privacy. If $\mu$ and $\sigma$ are in the same secret group (i.e., $\mathcal{B} = \{\{\mu, \sigma\}\}$), the group secrets privacy is equivalent to the intersection privacy.

### F.2.1 Proof of Prop. F.3

Define $\theta' = (\mu'_1, \cdots, \mu'_k, \sigma'_1, \cdots, \sigma'_k)$. Based on Lemma B.1, we can get that

$$
\begin{aligned}
\frac{D(X_\theta, X_{\theta'})}{R(X_\theta, X_{\theta'})} &\geq \frac{\sqrt{\sum_{j\in[k]}(\mu_j - \mu'_j)^2 + \sum_{j\in[k]}(\sigma_j - \sigma'_j)^2}}{\frac{2}{d}\sum_{i\in[d]}|g_i(\theta) - g_i(\theta')|} \\
&\geq \frac{\sqrt{\sum_{i\in[d]}(g_i(\theta) - g_i(\theta'))^2}}{\frac{2}{d}\sum_{i\in[d]}|g_i(\theta) - g_i(\theta')|} \\
&\geq \frac{\frac{1}{\sqrt{d}}\sum_{i\in[d]}|g_i(\theta) - g_i(\theta')|}{\frac{2}{d}\sum_{i\in[d]}|g_i(\theta) - g_i(\theta')|} \\
&= \frac{\sqrt{d}}{2}.
\end{aligned}
$$

Therefore, we have

$$
\gamma^{\text{group}} = \inf_{\theta_1, \theta_2 \in \text{Supp}(\omega_\Theta)} \frac{D(X_{\theta_1}, X_{\theta_2})}{R(X_{\theta_1}, X_{\theta_2})} = \frac{\sqrt{d}}{2}.
$$

Based on Thm. 5.3, we can get that

$$
\Delta_{\mathcal{M}_g} > \sqrt{d} \left\lceil \frac{1}{\left(1 - (1-T)^{1/\beta}\right)^{\beta/d}} \right\rceil \left(\prod_{i\in[d]} \epsilon_i\right)^{1/d} - \frac{1}{\sqrt{d}}\sum_{i\in[d]} \epsilon_i.
$$

### F.2.2 Proof of Prop. F.4

*Proof.* Based on Lemma B.1, we can easily can get that the distortion $\Delta$ of Alg. 1 is

$$
\Delta_{\mathcal{M}_g} = \sqrt{\sum_{i\in[d]} s_{g_i}^2}.
$$

Since the secret distribution parameters are independent of each other and follow the uniform distributions, we can get that the privacy of Alg. 1 is

$$
\begin{aligned}
\Pi^{\text{group}}_{\epsilon, \omega_\Theta} &= \sup_{\hat{g}} \mathbb{P}\left(\bigcup_{b\in\mathcal{B}}\left(\bigcap_{i\in\mathcal{I}_b}|\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i\right)\right) \\
&= 1 - \sup_{\hat{g}} \mathbb{P}\left(\bigcap_{b\in\mathcal{B}}\left(\bigcup_{i\in\mathcal{I}_b}|\hat{g}_i(\theta') - g_i(\theta)| > \epsilon_i\right)\right) \\
&= 1 - \sup_{\hat{g}} \prod_{b\in\mathcal{B}} \mathbb{P}\left(\bigcup_{i\in\mathcal{I}_b}|\hat{g}_i(\theta') - g_i(\theta)| > \epsilon_i\right) \\
&= 1 - \prod_{b\in\mathcal{B}}\left(1 - \prod_{i\in\mathcal{I}_b}\frac{2\epsilon_i}{s_{g_i}}\right).
\end{aligned}
$$

From Prop. F.3, we know that the optimal achievable distortion $\Delta_{opt}$ satisfy

$$\Delta_{opt} > \sqrt{d} \left[ \frac{1}{\left(1 - \left[\prod_{b\in\mathcal{B}}\left(1 - \prod_{i\in\mathcal{I}_b}\frac{2\epsilon_i}{s_{g_i}}\right)\right]^{1/\beta}\right)^{\beta/d}} \right] \left(\prod_{i\in[d]}\epsilon_i\right)^{1/d} - \frac{1}{\sqrt{d}}\sum_{i\in[d]}\epsilon_i.$$

Let $k = \frac{\Delta}{\Delta_{opt}}$, $x_i = \frac{\epsilon_i}{s_{g_i}}, \forall i \in [d]$, $c_1 = \min_{i\in[d]}\{x_i\}$, and $c_2 = \max_{i\in[d]}\{x_i\}$, we have

$$k < \frac{\sqrt{\sum_{i\in[d]}\left(\frac{\epsilon_i}{x_i}\right)^2}}{\sqrt{d}\left[\frac{1}{\left(1-\left[\prod_{b\in\mathcal{B}}\left(1-\prod_{i\in\mathcal{I}_b}2x_i\right)\right]^{1/\beta}\right)^{\beta/d}}\right]\left(\prod_{i\in[d]}\epsilon_i\right)^{1/d} - \frac{2}{\sqrt{d}}\sum_{i\in[d]}\epsilon_i}$$

$$\leq \frac{\sqrt{\sum_{i\in[d]}\epsilon_i^2}}{c_1\sqrt{d}\cdot\frac{1}{\left(1-\left[\prod_{b\in\mathcal{B}}\left(1-(2c_2)^{|b|}\right)\right]^{1/\beta}\right)^{\beta/d}}\cdot\left(\prod_{i\in[d]}\epsilon_i\right)^{1/d} - \frac{2c_1}{\sqrt{d}}\sum_{i\in[d]}\epsilon_i}$$

$$= \frac{\sqrt{\sum_{i\in[d]}\epsilon_i^2/d}}{\frac{c_1}{\left(1-\left[\prod_{b\in\mathcal{B}}\left(1-(2c_2)^{|b|}\right)\right]^{1/\beta}\right)^{\beta/d}}\left(\prod_{i\in[d]}\epsilon_i\right)^{1/d} - c_1\sum_{i\in[d]}\epsilon_i/d}$$

$$\triangleq c_{\epsilon,s,\mathcal{B}}.$$

Therefore, we can get that

$$\Delta_{\mathcal{M}_g} = k\Delta_{opt} < c_{\epsilon,s,\mathcal{B}}\cdot\Delta_{opt},$$

where $c_{\epsilon,s,\mathcal{B}}$ is a constant depending on the tolerance ranges, the interval lengths of the mechanism, and the set of secret groups $\mathcal{B}$.

Specifically, we can get that $\Delta < 3\Delta_{opt}$ when the size of each secret group are the same (i.e., $|b_1| = |b_2|, \forall b_1, b_2 \in \mathcal{B}$ ), $\epsilon_1 = \cdots = \epsilon_d$, and the designed data released mechanism satisfy $\frac{\epsilon_1}{s_{g_1}} = \cdots = \frac{\epsilon_d}{s_{g_d}} \leq \frac{1}{6}$. $\quad\square$

## F.3 $l_p$ Norm Privacy

Under the $l_p$ norm privacy metric, we focus on the multivariate Gaussian with dimensionally independent variables, and provide the privacy-distortion lower bound in Prop. F.5.

**Proposition F.5.** *For $k$-dimensional Gaussian distribution with diagonal covariance matrix and distribution parameters $\theta = (\mu_1, \cdots, \mu_k, \sigma_1, \cdots, \sigma_k)$, consider $d$ secrets ($d \leq 2k$), where each secret satisfies $g_i(\theta) \in \{\mu_1, \cdots, \mu_k, \sigma_1, \cdots, \sigma_k\}, \forall i \in [d]$. For any $T \in (0,1)$, when $\Pi_{\epsilon,\omega_\Theta} \leq T$,*

$$\Delta_{\mathcal{M}_g} > \sqrt{d}\cdot\left(\left\lceil\frac{1}{T}\right\rceil^{1/d} - 1\right)\cdot\varepsilon_p/d^{\frac{1}{p}}.$$

The proof is shown in App. F.3.1. We then analyze the performance of Alg. 1 under $l_p$ norm privacy as follows.

**Proposition F.6** (Mechanism privacy-distortion tradeoff under $l_p$ norm privacy)**.** *Under the assumption that secret distribution parameters $g_1, \cdots, g_d$ follow the uniform distribution, Alg. 1 has*

$$\Pi_{\epsilon,\omega_\Theta}^{l_p} \leq 1 - \prod_{i\in[d]}\left(1 - \frac{2\varepsilon_p}{d^{\frac{1}{p}}\cdot s_{g_i}}\right),$$

$$\Delta_{\mathcal{M}_g} = \sqrt{\sum_{i\in[d]}s_{g_i}^2}.$$

The proof is shown in App. F.3.2. From Prop. F.6 we know that Alg. 1 is order-optimal with a constant multiplication factor.

### F.3.1 Proof of Prop. F.5

Define $\theta' = (\mu_1', \cdots, \mu_k', \sigma_1', \cdots, \sigma_k')$. Based on Lemma B.1, we can get that

$$\frac{D\left(X_\theta, X_{\theta'}\right)}{R\left(X_\theta, X_{\theta'}\right)} \geq \frac{\sqrt{\sum_{j\in[k]}\left(\mu_j - \mu_j'\right)^2 + \sum_{j\in[k]}\left(\sigma_j - \sigma_j'\right)^2}}{\frac{2}{d}\sum_{i\in[d]}|g_i(\theta) - g_i(\theta')|}$$

$$\geq \frac{\sqrt{\sum_{i\in[d]}\left(g_i(\theta) - g_i(\theta')\right)^2}}{\frac{2}{d}\sum_{i\in[d]}|g_i(\theta) - g_i(\theta')|}$$

$$\geq \frac{\frac{1}{\sqrt{d}}\sum_{i\in[d]}|g_i(\theta) - g_i(\theta')|}{\frac{2}{d}\sum_{i\in[d]}|g_i(\theta) - g_i(\theta')|}$$

$$= \frac{\sqrt{d}}{2}.$$

Therefore, we have

$$\gamma^{l_p} = \inf_{\theta_1, \theta_2 \in \mathrm{Supp}(\omega_\Theta)} \frac{D\left(X_{\theta_1}, X_{\theta_2}\right)}{R\left(X_{\theta_1}, X_{\theta_2}\right)} = \frac{\sqrt{d}}{2}.$$

Based on Thm. D.1, we can get that

$$\Delta_{\mathcal{M}_g} > \sqrt{d} \cdot \left(\left\lceil\frac{1}{T}\right\rceil^{1/d} - 1\right) \cdot \varepsilon_p / d^{\frac{1}{p}}.$$

### F.3.2 Proof of Prop. F.6

*Proof.* Based on Lemma B.1, we can easily can get that the distortion $\Delta$ of Alg. 1 is

$$\Delta_{\mathcal{M}_g} = \sqrt{\sum_{i\in[d]} s_{g_i}{}^2}.$$

We denote $\Pi_{\epsilon,\omega_\Theta}^{\mathrm{uni}}$ as the union privacy metric with tolerance ranges $\epsilon_1, \cdots, \epsilon_d$. From App. D.2.1, we know that $\Pi_{\epsilon,\omega_\Theta}^{l_p} \leq \Pi_{\epsilon,\omega_\Theta}^{\mathrm{uni}}$ when $\left(\sum_{i\in[d]}\epsilon_i^p\right)^{1/p} = \varepsilon_p$. Therefore, we can get that

$$\Pi_{\epsilon,\omega_\Theta}^{l_p} \leq \min_{\substack{\epsilon_1,\cdots,\epsilon_d: \\ \left(\sum_{i\in[d]}\epsilon_i^p\right)^{1/p}=\varepsilon_p}} \Pi_{\epsilon,\omega_\Theta}^{\mathrm{uni}}$$

$$= \min_{\substack{\epsilon_1,\cdots,\epsilon_d: \\ \left(\sum_{i\in[d]}\epsilon_i^p\right)^{1/p}=\varepsilon_p}} 1 - \prod_{i\in[d]}\left(1 - \frac{2\epsilon_i}{s_{g_i}}\right).$$

By setting $\epsilon_i = \varepsilon_p / d^{\frac{1}{p}}$ for all $i \in [d]$, we can get that

$$\Pi_{\epsilon,\omega_\Theta}^{l_p} \leq 1 - \prod_{i\in[d]}\left(1 - \frac{2\varepsilon_p}{d^{\frac{1}{p}} \cdot s_{g_i}}\right).$$

$\square$

# G   The case of unknown distribution parameters: an example

We take 1-dimensional Gaussian distribution as an example to illustrate how the extension works. For a dataset $\mathcal{X} = \{x_1, \ldots, x_m\}$, the concrete steps of the extended mechanism are:

1. Calculate the empirical mean and standard deviation from the dataset: $\hat{\mu} = \frac{1}{m} \sum_{i \in [m]} x_i$, $\hat{\sigma} = \sqrt{\frac{1}{m} \sum_{i \in [m]} (x_i - \hat{\mu})^2}$.

2. Determine the indices $i, j$ of the intervals that $\hat{\mu}, \hat{\sigma}$ fall: $i = \lfloor \frac{\hat{\mu} - \underline{\mu}}{s_\mu} \rfloor$, $j = \lfloor \frac{\hat{\sigma} - \underline{\sigma}}{s_\sigma} \rfloor$.

3. Determine the released parameters: $\mu_r = \underline{\mu} + i \cdot s_\mu + U(0, s_\mu)$, $\sigma_r = \underline{\sigma} + j \cdot s_\sigma + U(0, s_\sigma)$.

4. Release the dataset $\mathcal{X}' = \{x'_1, \ldots, x'_m\}$ such that $x'_i = \frac{\sigma_r}{\hat{\sigma}} (x_i - \hat{\mu}) + \mu_r$.

This mechanism can also be integrated with generative models to alter the summary statistical properties of training samples or the generated dataset.

# H   Additional Empirical Results

In this section, we conduct additional experiments on different privacy metrics and analyze the scalability of our mechanism.

## H.1   Experiments on $l_p$ Norm Privacy

We include $l_p$ norm privacy to illustrate the variations in privacy-distortion tradeoffs across different privacy metrics and show the privacy-distortion performance of our mechanism. We define surrogate privacy metrics for $l_p$ norm privacy as

$$\tilde{\Pi}^{l_p}_{\epsilon, \omega_\Theta} = -\|\boldsymbol{g}(\mathcal{X}) - \boldsymbol{g}(\mathcal{X}')\|_p / \varepsilon_p,$$

and consider the same empirical settings and baselines as those in §7. We consider $l_p$ norm privacy with $p = 1$ and $p = \infty$, and set the tolerance as $\varepsilon_p = (\epsilon_1^p + \epsilon_2^p + \epsilon_3^p)^{\frac{1}{p}}$ (i.e., $\varepsilon_1 = 8$ for $l_1$ privacy and $\varepsilon_\infty = 4$ for $l_\infty$ privacy).
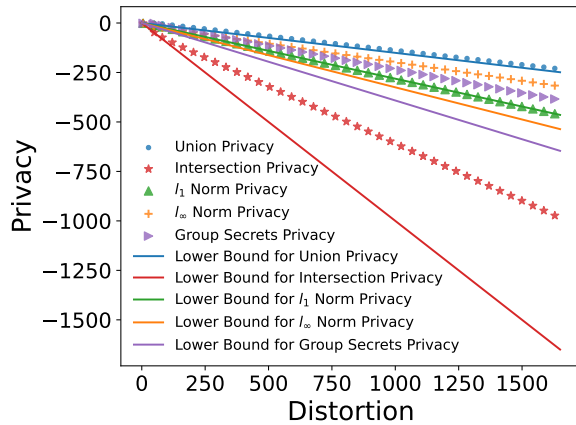


Figure 4: Privacy (lower is better) and distortion of Alg. 1 under Wikipedia Web Traffic Dataset with different privacy metrics. For each privacy formulation, the soild line with the same color represents the theoretical lower bound of achievable region.
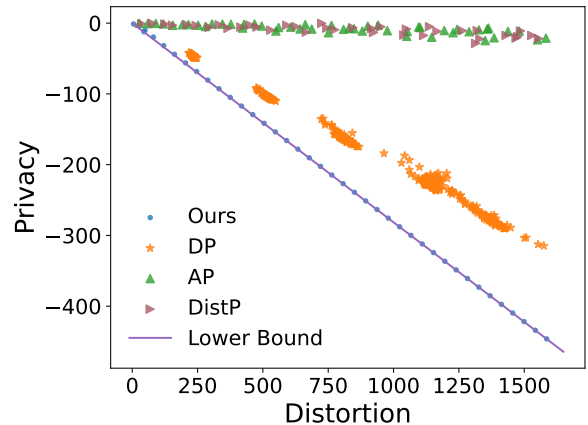
Figure 5: Privacy and distortion (lower bottom is better) of DP, AP, DistP, and ours under $l_1$ norm privacy. The solid line represents the theoretical lower bound of achievable region.

Including $l_1$ norm and $l_\infty$ norm privacy, Fig. 4 shows distortion and privacy values of Alg. 1 as well as theoretical privacy-distortion lower bounds under different privacy metrics. Similar to Fig. 2, we can observe from Fig. 4 that: (1) The privacy-distortion tradeoffs of Alg. 1 match the theoretical lower bounds (or with a mild gap) even the distribution assumption does not hold; (2) The discrepancies in privacy-distortion tradeoffs across different privacy metrics align with the theoretical justifications: the values of $l_p$ norm privacy are intermediate between union and intersection privacy.

In Fig. 5, we compare the privacy-distortion tradeoffs between DP, AP, DistP, and our mechanism under $l_1$ norm privacy. Each point represents a realization of data release mechanism with one hyper-parameter (bin size and noise level for DP, noise level for AP and DistP, interval length for ours). Similar to the results in Fig. 3, our quantization mechanism achieves better privacy-distortion tradeoffs.

## H.2 Scalability of Our Mechanism

In this section, we analyze the scalability of our mechanism Alg. 1 with respect to the input data size and the number of secrets.

**Data Size** If the data holder knows the underlying distribution, the computational complexity of our mechanism does not increase with data size, since the mechanism inputs are distribution parameters. Otherwise, the computational cost grows linearly with the data size (see §6).

We conduct experiments on a synthetic dataset whose underlying distribution is a 10-dimensional Gaussian. We vary the data size from $10^2$ to $10^8$, and record the running time of our mechanism (on an 8-core Apple M2 CPU), which is shown as follows.

Table 2: Running time of Alg. 1 under different input data size.

| Data Size | $10^2$ | $10^4$ | $10^6$ | $10^8$ |
|---|---|---|---|---|
| Runtime (s) | $< 0.01$ | $< 0.01$ | $0.03 \pm 0.001$ | $6.90 \pm 0.01$ |

Table 2 shows that even if the data size is $10^8$, our mechanism is still computationally efficient.

**Secret Number** The computational cost of our mechanism grows only linearly with the number of secrets. We conduct experiments under the web-traffic dataset and vary the secret number from $10^2$ to $10^5$, and record the running time of our mechanism (on an 8-core Apple M2 CPU), which is shown in Table 3.

Table 3: Running time of Alg. 1 under different secret number.

| Secret Number | $10^2$ | $10^3$ | $10^4$ | $10^5$ |
|---|---|---|---|---|
| Runtime (s) | $< 0.01$ | $< 0.01$ | $0.07 \pm 0.001$ | $0.90 \pm 0.01$ |

Table 3 shows that even if the secret number is as large as $10^5$, our mechanism is still computationally efficient.

# I Adaptive Composition Property of Summary Statistic Privacy

In this section, we take a first step towards analyzing the adaptive composition property of the summary statistic privacy. We focus on the setting where the distribution parameter $\theta$ belongs to a finite set, there is only one summary statistic secret, and the tolerance range $\epsilon$ is 0. We also assume that $\sup_\theta \mathbb{P}(\theta) = a < 1$ and $\inf_\theta \mathbb{P}(\theta) = b > 0$. Under such setting, the summary statistic privacy of a mechanism $\mathcal{M}$ can be written as

$$\Pi^{\mathcal{M}}_{\omega_\Theta} \triangleq \sup_{\hat{g}} \mathbb{P}\left(\hat{g}(\theta') = g(\theta)\right).$$

The following theorem shows the adaptive composition guarantee of the summary statistic privacy under such setting.

**Theorem I.1** (Adaptive Composition). *Consider a data holder sequentially applies $m$ data release mechanisms to the original dataset. For the $i$-th mechanism $\mathcal{M}_i$, $\forall i \in [m]$, it takes the original distribution parameter $\theta$ and all previous released parameters $\theta'_1, \ldots, \theta'_{i-1}$ as input and output $\theta'_i$. Suppose the summary statistic privacy of mechanism $\mathcal{M}_i$ is $\Pi^{\mathcal{M}_i}_{\omega_\Theta}$, $\forall i \in [m]$. Let $\mathcal{M}$ be the composition of these $m$ mechanisms, and suppose the adversary can get access to all released parameters $\theta'_1, \ldots, \theta'_m$. The summary statistic privacy of $\mathcal{M}$ can be bounded as $\Pi^{\mathcal{M}}_{\omega_\Theta} \leq a \cdot \prod_{i \in [m]} \frac{\Pi^{\mathcal{M}_i}_{\omega_\Theta}}{b}$.*

*Proof.* For the summary statistic privacy of $\mathcal{M}$, we can get that

$$\Pi^{\mathcal{M}}_{\omega_\Theta} = \sup_{\hat{g}} \mathbb{P}\left(\hat{g}\left(\theta'_1, \ldots, \theta'_m\right) = g\left(\theta\right)\right)$$

$$= \sum_{\theta'_1, \ldots, \theta'_m} \mathbb{P}\left(\theta'_1, \ldots, \theta'_m\right) \cdot \left(\sup_g \sum_{\theta:g(\theta)=\mathrm{g}} \mathbb{P}\left(\theta|\theta'_1, \ldots, \theta'_m\right)\right)$$

$$= \sum_{\theta'_1, \ldots, \theta'_m} \sup_g \sum_{\theta:g(\theta)=\mathrm{g}} \mathbb{P}\left(\theta, \theta'_1, \ldots, \theta'_m\right)$$

$$= \sum_{\theta'_1, \ldots, \theta'_m} \sup_g \sum_{\theta:g(\theta)=\mathrm{g}} \mathbb{P}\left(\theta\right) \cdot \mathbb{P}\left(\theta'_1, \ldots, \theta'_m|\theta\right)$$

$$\leq a \cdot \sum_{\theta'_1, \ldots, \theta'_m} \sup_g \sum_{\theta:g(\theta)=\mathrm{g}} \mathbb{P}\left(\theta'_1, \ldots, \theta'_m|\theta\right)$$

$$= a \cdot \sum_{\theta'_1, \ldots, \theta'_m} \sup_g \sum_{\theta:g(\theta)=\mathrm{g}} \prod_{i \in [m]} \mathbb{P}\left(\theta'_i|\theta, \theta'_1, \ldots, \theta'_{i-1}\right)$$

$$\leq a \cdot \sum_{\theta'_1, \ldots, \theta'_m} \sup_g \prod_{i \in [m]} \sum_{\theta:g(\theta)=\mathrm{g}} \mathbb{P}\left(\theta'_i|\theta, \theta'_1, \ldots, \theta'_{i-1}\right)$$

$$\leq a \cdot \sum_{\theta'_1, \ldots, \theta'_m} \prod_{i \in [m]} \sup_g \sum_{\theta:g(\theta)=\mathrm{g}} \mathbb{P}\left(\theta'_i|\theta, \theta'_1, \ldots, \theta'_{i-1}\right)$$

$$\leq a \cdot \prod_{i \in [m]} \sum_{\theta'_1, \ldots, \theta'_i} \sup_g \sum_{\theta:g(\theta)=\mathrm{g}} \mathbb{P}\left(\theta'_i|\theta, \theta'_1, \ldots, \theta'_{i-1}\right)$$

$$= a \cdot \prod_{i \in [m]} \sum_{\theta'_1, \ldots, \theta'_i} \sup_g \sum_{\theta:g(\theta)=\mathrm{g}} \frac{\mathbb{P}\left(\theta'_i\right) \mathbb{P}\left(\theta|\theta'_1, \ldots, \theta'_i\right)}{\mathbb{P}\left(\theta\right)}$$

$$\leq a \cdot \prod_{i \in [m]} \frac{\Pi^{\mathcal{M}_i}_{\omega_\Theta}}{b}.$$

$\square$

# J  Broader Impact

This paper proposes a framework to quantify and mitigate the leakage of distributional properties of released datasets or data distributions in data-sharing scenarios, ensuring that data can be shared safely with other entities. However, improper adoption of our framework may result in the miscalculation of privacy risks, potentially leading to unsafe data sharing. To prevent such issues, one must follow our definitions closely to calculate privacy risks accurately. Moreover, extending our proposed release mechanisms to scenarios outside of those investigated in this paper requires careful attention (which is left to future work). Naïve adoption of these mechanisms outside of the investigated scenarios may expose the data holder to privacy risks and is not recommended.