GUARDING MULTIPLE SECRETS: ENHANCED SUMMARY STATISTIC PRIVACY FOR DATA SHARING

Shuaiqi Wang
Electrical and Computer Engineering
Carnegie Mellon University
shuaiqiw@andrew.cmu.edu

Rongzhe Wei
Electrical and Computer Engineering
Georgia Institute of Technology
rongzhe.wei@gatech.edu

Mohsen Ghassemi, Eleonora Kreacic & Vamsi K. Potluru
JP 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., mean, standard deviation). Existing efforts mainly focus on protecting a single confidential quantity, while in practice, data frequently involves a range of sensitive quantities. 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. Within diverse data sharing paradigms, 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.

1 INTRODUCTION

Data sharing has become integral to modern research and applications (Lee & Whang, 2000). However, a significant challenge arises when examining the summary statistics of shared data, as they might unintentionally disclose sensitive information that data owners wish to keep private (Suri & Evans, 2021). For example, cloud service providers, in an effort to protect their business secrets, may hide information like the average cluster usage of each server type (Lin et al., 2020). In a similar vein, companies may hesitate to share average transaction amounts categorized by race, considering the sensitive nature of this data (Gelb & Decker, 2012). Notably, while many studies address individual privacy concerns (e.g., Dwork et al. (2006)), there remains a noticeable lack of research on protecting the summary statistics of shared datasets.

In Lin et al. (2023), a novel privacy framework is introduced, designed to identify and analyze concerns related to summary statistics privacy. Lin et al. (2023) focus solely on the scenario where only one summary statistic is deemed confidential by the data owner. In real-world scenarios, however, multiple summary statistics properties of the disseminated data may be regarded as proprietary information or contain sensitive information. For example, in a web traffic dataset, disclosing the average daily page views of any health-related website can raise privacy concerns (Libert, 2015). 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 Lin et al. (2023) 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' requirements can differ. Some scenarios require no secrets being disclosed, while others may only demand not all secrets being revealed simultaneously. As an example, for a web traffic dataset, revealing any single secret related to health-related websites can give rise to significant privacy concerns. While for the cluster performance traces dataset, only when the proportions of all

server types are disclosed, the business secret about overall deployment of servers is leaked. To this end, we propose a framework to quantify, analyze and protect multi-secret summary statistics privacy under different protection scenarios. The contributions of our paper are shown as follows.

Metric Design (§3, §5) In contrast to the single secret privacy framework, we introduce and analyze several novel 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. This metric is particularly relevant for scenarios where the data holder seeks to conceal all secrets. Subsequently, in §5, we explore three 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) With different privacy metrics, we provide the general lower bounds of the distortion (lower is better) given a certain constraint on the privacy. Those lower bounds are non-trivial extensions of the tradeoff analysis in Lin et al. (2023). The analysis of the lower bound is general, regardless of data distributions and secret types. The bound also reveals how the number of secrets affect the privacy-distortion tradeoffs under different privacy metrics.

2 Related Works

We discuss the related work in detail in App. A. Briefly, previous works on protecting summary statistic secrets can be categorized into four classes.

Heuristics Heuristics, commonly adopted in industries for data sharing (Hundepool et al., 2010), often lack rigorous privacy guarantees and can be vulnerable in real-world scenarios (Elliot & Dale, 1999), with methods like subsetting (Reiss et al., 2012), culling (Reiss et al., 2012), and de-identification (Garfinkel et al., 2015), being susceptible to re-identification threats or unintentional data property leakage (Narayanan & Shmatikov, 2006; Sweeney, 2013; El Emam & Dankar, 2008).

Indistinguishability Methods *Differential privacy* (DP) (Dwork et al., 2006), ensures indistinguishability between neighboring datasets. However, its design is more aligned with protecting individual record contributions rather than overarching distributional statistical properties. Notably, mechanisms like the Laplacian (Dwork et al., 2006) introduce zero-mean noise to samples but often leave certain integral statistics, like means, less affected. Derived from the spirit of DP, methods such as *attribute privacy* (Zhang et al., 2022) aim to safeguard specific dataset properties. However, their applications do not always align with data sharing scenarios as those methods only output certain statistical queries. Similarly, paradigms like *distribution privacy* (Kawamoto & Murakami, 2019) and *distribution inference* (Suri & Evans, 2021) 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), can sometimes be excessive, leading to reduced data utility.

Leakage-Based Methods A set of research 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 (Alvim et al., 2014; Smith, 2015). Various measures, including Shannon entropy (Makhdoumi et al., 2014), min-entropy (Asoodeh et al., 2017), and gain function (M'rio et al., 2012) have been employed to define leakage. A notable advancement in this area is the concept of *maximal leakage* (Issa et al., 2019), which quantifies the increased likelihood of correctly inferring secrets post-data release. However, maximal leakage and its generalizations, such as Gilani et al. (2023), may not be applicable to our context due to their assumption that secrets are not known in advance.

Summary Statistic Privacy The recently introduced summary statistic privacy (Lin et al., 2023) 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 mainly concentrates on safeguarding a singular secret under one-shot attack and confines the data analysis to one dimension, which may not cater comprehensively to practical applications. While a direct

expansion of this framework to guard multiple secrets proves challenging, its foundational principles for formulating a privacy metric resonate with our work.

3 PROBLEM FORMULATION

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

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 ω_{X_θ}. We can express those secrets as d functions $\boldsymbol{g} = [g_1, \cdots, g_d]$, 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 θ through the data release mechanism $\mathcal{M}_g$. The released data distribution parameter θ' satisfies $\theta' \sim \mathcal{M}_g(\theta)$.

Threat Model We assume the attacker knows the parametric family where the original data distribution is from, but does not know the distribution parameter θ. The attacker also knows the released parameter θ' and the mechanism $\mathcal{M}_g$, but does not know the realization of the internal randomness of the mechanism. Based on the released parameter θ', 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 We start by considering the case where the data holder aims to prevent attackers guessing any secret correctly. For example, consider the web traffic dataset with secrets as the average daily page views of health-related websites. Disclosing any secret may cause privacy concerns.

We define the *union privacy* metric $\Pi_{\epsilon,\omega_\Theta}$ as the probability of the attacker guessing any secret to within a tolerance range, ϵ_i for secret g_i, employing the best attack strategy:

$$\Pi_{\epsilon,\omega_\Theta} \triangleq \sup_{\hat{\boldsymbol{g}}} \mathbb{P}\left(\bigcup_{i\in[d]} |\hat{g}_i(\theta') - g_i(\theta)| \leq \epsilon_i \right), \tag{1}$$

where the probability is taken over the randomness of the original data distribution parameter θ, 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 introduced several relaxed privacy metrics.

Union privacy also accommodates to 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 strategies guessing the secret.

Distortion Metric Since the goal of data sharing is to maintain the 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 Δ. Specifically, the distortion of a mechanism is characterized by the worst-case discrepancy between the original distribution and the released distribution:

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

where 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., Korotin et al. (2021)).

Objective The data holder's objective is to choose a data release mechanism that minimizes distortion metric Δ subject to a constraint on privacy $\Pi_{\epsilon,\omega_\Theta}$:

$$\begin{aligned} \min_{\mathcal{M}_g} \quad & \Delta \\ \text{subject to} \quad & \Pi_{\epsilon,\omega_\Theta} \leq T. \end{aligned} \tag{3}$$

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 regardless of the distribution of data and regardless of the secrets $\boldsymbol{g} = [g_1, g_2, \cdots, g_d]$. In App. C, we instantiate this general result on Gaussian distributions with multiple secrets, devise data release mechanisms, and assess their privacy-distortion performance.

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

$$\gamma \triangleq \inf_{\theta_1,\theta_2 \in Supp(\omega_\Theta)} \frac{D\left(X_{\theta_1}, X_{\theta_2}\right)}{R\left(X_{\theta_1}, X_{\theta_2}\right)}. \tag{4}$$

For any $T \in (0,1)$, *when* $\Pi_{\epsilon,\omega_\Theta} \leq T$,

$$\Delta > 2\gamma \cdot \left\lceil \frac{1}{1-(1-T)^{1/d}} - 1 \right\rceil \cdot \left(\prod_{i\in[d]} \epsilon_i \right)^{1/d}. \tag{5}$$

The proof is shown in App. B.1, and we provide the proof sketch as below. From Thm. 4.1, we can observe that the lower bound is proportional to the geometric mean of the tolerance ranges $\epsilon_1, \cdots, \epsilon_d$, and is negatively correlated to the privacy budget T. γ 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., γ) 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.

Proof Sketch We prove the tradeoff lower bound by constructing a sequence of attackers, 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 $g_2(\theta)$. 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 γ, 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. In this section, we relax the privacy metric and propose alternatives that apply to such scenarios. The corresponding case studies and mechanism analysis are shown in App. D.

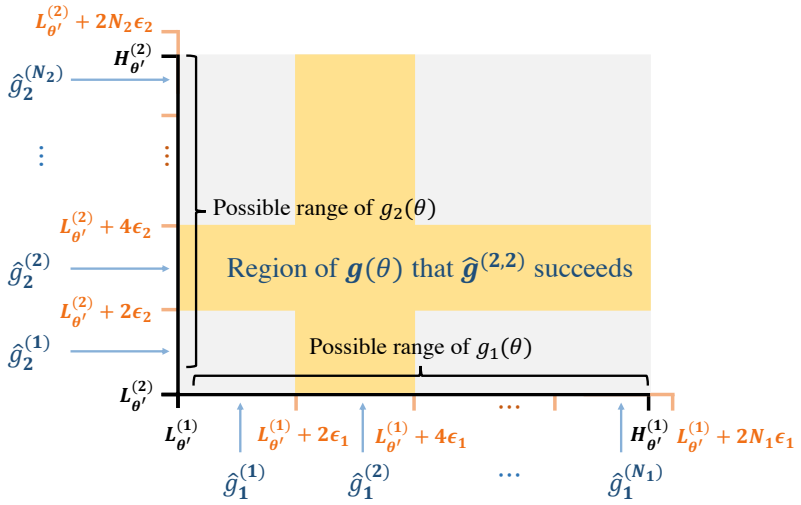

Figure 1: Attacker construction for proof of Thm. 4.1 under the 2-secret case.

5.1 Intersection Summary Statistic Privacy

We first consider the scenario where secrets are severely compromised when the attacker guesses all of them simultaneously. This is for example the case when a data holder is only concerned about an adversary obtaining the full picture of the data rather than specific summary statistics.

We define the *intersection privacy* metric as the probability of attacker guessing all secrets within their respective tolerance ranges, ϵ_i for secret g_i, employing the best attacker strategy:

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

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

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

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

For any $T \in (0,1)$, *when* $\Pi_{\epsilon,\omega_\Theta} \leq T$,

$$\Delta > 2\gamma \cdot \left\lceil \frac{1}{T} \right\rceil^{1/d} \cdot \left(\prod_{i\in[d]} \epsilon_i\right)^{1/d} - 2\gamma \cdot \frac{1}{d}\sum_{i\in[d]} \epsilon_i. \tag{8}$$

(Proof in App. B.2.) From Thm. 5.1, we know that the distortion lower bound is negatively correlated to the privacy budget T. As the secret number d increases, achieving a lower value for the 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, the optimal achievable distortion for intersection privacy 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* Δ_{union} *and* Δ_{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, ϵ_i for secret g_i, adopting the best attack strategy:

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

where the secret index set $\mathcal{I}_b$ satisfies $\mathcal{I}_{b_1} \cap \mathcal{I}_{b_2} = \emptyset$ for any distinct group $b_1, b_2 \in \mathcal{B}$.

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* $D(X_{\theta_1}, X_{\theta_2}) \triangleq \frac{1}{2}\mathfrak{D}\left(\omega_{X_{\theta_1}} \| \omega_{X_{\theta_2}}\right)$*. Further, let* $R(X_{\theta_1}, X_{\theta_2}) \triangleq \frac{1}{d}\sum_{i\in[d]}|g_i(\theta_1) - g_i(\theta_2)|$ *and*

$$\gamma \triangleq \inf_{\theta_1,\theta_2 \in Supp(\omega_\Theta)} \frac{D(X_{\theta_1}, X_{\theta_2})}{R(X_{\theta_1}, X_{\theta_2})}. \tag{9}$$

For any $T \in (0,1)$*, when* $\Pi_{\epsilon,\omega_\Theta} \leq T$*,*

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

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

(Proof in App. B.4.) When $\beta = 1$, group secrets privacy reduces to intersection privacy, the least strict privacy metric. As β grows to d, group secrets privacy transforms into union privacy, the strictest metric. From Thm. 5.3, we can also observe that the distortion lower bound is positively correlated with the group number β.

5.3 l_p NORM SUMMARY STATISTIC PRIVACY

Finally, 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 ε_p, taking the best attack strategy:

$$\Pi_{\epsilon,\omega_\Theta} \triangleq \sup_{\hat{\boldsymbol{g}}} \mathbb{P}\left(\|\hat{\boldsymbol{g}}(\theta') - \boldsymbol{g}(\theta)\|_p \leq \varepsilon_p\right). \tag{10}$$

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

Theorem 5.4 (Lower bound of privacy-distortion tradeoff for l_p norm privacy)**.** *Let* $D(X_{\theta_1}, X_{\theta_2}) \triangleq \frac{1}{2}\mathfrak{D}\left(\omega_{X_{\theta_1}} \| \omega_{X_{\theta_2}}\right)$*. Further, let* $R(X_{\theta_1}, X_{\theta_2}) \triangleq \frac{1}{d}\sum_{i\in[d]}|g_i(\theta_1) - g_i(\theta_2)|$ *and*

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

For any $T \in (0,1)$*, when* $\Pi_{\epsilon,\omega_\Theta} \leq T$*,*

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

(Proof in App. B.6.) From Thm. 5.4, we know that the distortion lower bound is positively correlated to the tolerance range ε_p and negatively correlated to the privacy budget T. As shown in Prop. 5.5, l_p norm privacy metric is less strict than union privacy but stricter than intersection privacy.

Proposition 5.5. *For union and intersection privacy, let $\epsilon_1, \cdots, \epsilon_d$ be the tolerance ranges. Let the tolerance ε_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 Δ_{union}, Δ_{inter}, and Δ_{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. B.7.

6 Acknowledgments

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

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*, pp. 308–322. IEEE, 2014.

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

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

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

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

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*, pp. 265–284. Springer, 2006.

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

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.

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

Alan Gelb and Caroline Decker. Cash at your fingertips: Biometric technology for transfers in developing countries. *Review of Policy Research*, 29(1):91–117, 2012.

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

Atefeh Gilani, Gowtham R Kurri, Oliver Kosut, and Lalitha Sankar. (α, β)-leakage: A unified privacy leakage measure. *arXiv preprint arXiv:2304.07456*, 2023.

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

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.

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

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

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

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.

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

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

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.

Timothy Libert. Privacy implications of health information seeking on the web. *Communications of the ACM*, 58(3):68–77, 2015.

Zinan Lin, Alankar Jain, Chen Wang, Giulia Fanti, and Vyas Sekar. Using gans for sharing networked time series data: Challenges, initial promise, and open questions. In *Proceedings of the ACM Internet Measurement Conference*, pp. 464–483, 2020.

Zinan Lin, Shuaiqi Wang, Vyas Sekar, and Giulia Fanti. Summary statistic privacy in data sharing. *arXiv preprint arXiv:2303.02014*, 2023.

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)*, pp. 501–505. IEEE, 2014.

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*, pp. 265–279. IEEE, 2012.

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

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

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*, pp. 1279–1286. IEEE, 2012.

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

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

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

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

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

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

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

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)*, pp. 620–625. IEEE, 2022.

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

Appendix

CONTENTS

A Related Works

Heuristics While heuristics are widely adopted in industries for data sharing Hundepool et al. (2010), many lack theoretical privacy guarantees and can be vulnerable in real-world scenarios Elliot & Dale (1999). For example, *subsetting* aims to protect sensitive information by only selecting a part of available data to release Reiss et al. (2012). 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 Reiss et al. (2012), but they may excise too much information and are risked from re-identification attacks based on side information or cross-attribute correlations Narayanan & Shmatikov (2006); Sweeney (2013); El Emam & Dankar (2008).

Indistinguishability Methods *Differential privacy* (DP) Dwork et al. (2006) 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 approaches like Laplacian mechanism Dwork et al. (2006); Wasserman & Zhou (2010) would add zero mean noise to each sample. Obfuscating data in such way will not change statistical properties like the expected mean of the distribution.

Motivating by differential privacy, several works proposed approaches aiming to make pairs of datasets or distributions with similar summary statistic secrets indistinguishable Zhang et al. (2022); Ghosh & Kleinberg (2016); Chen & Ohrimenko (2023); Suri & Evans (2021). *Attribute privacy* Zhang et al. (2022) 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 Kifer & Machanavajjhala (2014), 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* Kawamoto & Murakami (2019) and *distribution inference* Suri & Evans (2021); Suri et al. (2023) 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 Alvim et al. (2014); Smith (2015). Leakage can be defined by various of measures, such as Shannon entropy Makhdoumi et al. (2014); Rassouli & Gündüz (2021); Zamani et al. (2022); Calmon et al. (2015), min-entropy Asoodeh et al. (2017; 2018); Smith (2009), and gain function M'rio et al. (2012); Alvim et al. (2014); Liao et al. (2019); Saeidian et al. (2023). One important theme is the development of leakage measures with operational significance Alvim et al. (2014). *Maximal leakage* Issa et al. (2019), 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., Gilani et al. (2023); Kurri et al. (2022)) 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 γ that serves as a linkage between the distributional distance and the distance between secrets.

$$
\begin{aligned}
T &\geq \Pi_{\epsilon,\omega_\Theta} \\
&= \sup_{\hat{\boldsymbol{g}}} \mathbb{P}\left(\bigcup_{i\in[d]} \left|\hat{g}_i\left(\theta'\right) - g_i\left(\theta\right)\right| \leq \epsilon_i\right) \\
&= \sup_{\hat{\boldsymbol{g}}} \mathbb{E}\left(\mathbb{P}\left(\bigcup_{i\in[d]} \left|\hat{g}_i\left(\theta'\right) - g_i\left(\theta\right)\right| \leq \epsilon_i \middle| \theta'\right)\right) \\
&= \mathbb{E}\left(\sup_{\hat{\boldsymbol{g}}} \mathbb{P}\left(\bigcup_{i\in[d]} \left|\hat{g}_i\left(\theta'\right) - g_i\left(\theta\right)\right| \leq \epsilon_i \middle| \theta'\right)\right) \quad , \qquad (11)
\end{aligned}
$$

where Eq. (11) is due to the fact that $\hat{g}$ only depends on θ' and therefore one can devise an attacker that for each θ', performs the optimal attack. It follows from Eq. (11) there exists θ' s.t. $\sup_{\hat{\boldsymbol{g}}} \mathbb{P}\left(\bigcup_{i\in[d]} \left|\hat{g}_i\left(\theta'\right) - g_i\left(\theta\right)\right| \leq \epsilon_i \middle| \theta'\right) \leq T$. 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 θ':

$$
\begin{aligned}
L_{\theta'}^{(i)} &\triangleq \inf_{\theta\in\text{Supp}(\omega_\Theta):\mathcal{M}_g(\theta)=\theta'} g_i\left(\theta\right) \ , \\
H_{\theta'}^{(i)} &\triangleq \sup_{\theta\in\text{Supp}(\omega_\Theta):\mathcal{M}_g(\theta)=\theta'} g_i\left(\theta\right) \ .
\end{aligned}
$$

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

$$
\begin{aligned}
T \cdot \mathcal{N} &\geq \sum_{\boldsymbol{v}} \mathbb{P}\left(\bigcup_{i\in[d]} \left|\hat{g}_i^{[\boldsymbol{v}]}\left(\theta'\right) - g_i\left(\theta\right)\right| \leq \epsilon_i \middle| \theta'\right) \\
&\overset{1}{=} \sum_{\boldsymbol{v}} \sum_{j\in[d]} (-1)^{j-1} \sum_{\substack{i_1<i_2<\cdots<i_j \\ i_1,i_2,\cdots,i_j\in[d]}} \mathbb{P}\left(\bigcap_{i\in\{i_1,i_2,\cdots,i_j\}} \left|\hat{g}_i^{[\boldsymbol{v}]}\left(\theta'\right) - g_i\left(\theta\right)\right| \leq \epsilon_i \middle| \theta'\right) \\
&\overset{2}{\geq} \sum_{j\in[d]} (-1)^{j-1} \sum_{\substack{i_1<i_2<\cdots<i_j \\ i_1,i_2,\cdots,i_j\in[d]}} \frac{\mathcal{N}}{\prod_{k\in\{i_1,i_2,\cdots,i_j\}} N_k}. \qquad (12)
\end{aligned}
$$

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

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

$\overset{2}{\geq}$ is because

$$\begin{aligned}
&\sum_{\boldsymbol{v}}\sum_{j\in[d]}(-1)^{j-1}\sum_{\substack{i_1<i_2<\cdots<i_j\\i_1,i_2,\cdots,i_j\in[d]}}\mathbb{P}\left(\bigcap_{i\in\{i_1,i_2,\cdots,i_j\}}\left|\hat{g}_i^{[\boldsymbol{v}]}\left(\theta'\right)-g_i\left(\theta\right)\right|\leq\epsilon_i\middle|\theta'\right)\\
&\quad=\sum_{j\in[d]}(-1)^{j-1}\sum_{\boldsymbol{v}}\sum_{\substack{i_1<i_2<\cdots<i_j\\i_1,i_2,\cdots,i_j\in[d]}}\mathbb{P}\left(\bigcap_{i\in\{i_1,i_2,\cdots,i_j\}}\left|\hat{g}_i^{[\boldsymbol{v}]}\left(\theta'\right)-g_i\left(\theta\right)\right|\leq\epsilon_i\middle|\theta'\right)\\
&\quad=\sum_{j\in[d]}(-1)^{j-1}\sum_{\substack{i_1<i_2<\cdots<i_j\\i_1,i_2,\cdots,i_j\in[d]}}\sum_{\boldsymbol{v}}\mathbb{P}\left(\bigcap_{i\in\{i_1,i_2,\cdots,i_j\}}\left|\hat{g}_i^{[\boldsymbol{v}]}\left(\theta'\right)-g_i\left(\theta\right)\right|\leq\epsilon_i\middle|\theta'\right)\\
&\quad\geq\sum_{j\in[d]}(-1)^{j-1}\sum_{\substack{i_1<i_2<\cdots<i_j\\i_1,i_2,\cdots,i_j\in[d]}}\prod_{k_1\in[d]\setminus\{i_1,i_2,\cdots,i_j\}}N_{k_1}\\
&\quad=\sum_{j\in[d]}(-1)^{j-1}\sum_{\substack{i_1<i_2<\cdots<i_j\\i_1,i_2,\cdots,i_j\in[d]}}\frac{\mathcal{N}}{\prod_{k\in\{i_1,i_2,\cdots,i_j\}}N_k}.
\end{aligned}$$

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

$$\begin{aligned}
\prod_{i\in[d]}\left(H_{\theta'}^{(i)}-L_{\theta'}^{(i)}\right)&>\prod_{i\in[d]}2\epsilon_i\left(N_i-1\right)\\
&=\prod_{i\in[d]}2\epsilon_i\cdot\prod_{i\in[d]}\left(N_i-1\right)\\
&=\left(\mathcal{N}-\sum_{j\in[d]}(-1)^{j-1}\sum_{\substack{i_1<i_2<\cdots<i_j\\i_1,i_2,\cdots,i_j\in[d]}}\frac{\mathcal{N}}{\prod_{k\in\{i_1,i_2,\cdots,i_j\}}N_k}\right)\cdot\prod_{i\in[d]}2\epsilon_i\\
&\overset{1}{\geq}\lceil(1-T)\mathcal{N}\rceil\cdot\prod_{i\in[d]}2\epsilon_i,
\end{aligned}\tag{13}$$

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

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

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

$$\begin{aligned}
\mathcal{N} &= \prod_{i\in[d]} (a_i + 1) \\
&= 1 + \sum_{j\in[d]} \sum_{\substack{i_1<i_2<\cdots<i_j \\ i_1,i_2,\cdots,i_j\in[d]}} \prod_{k\in\{i_1,i_2,\cdots,i_j\}} a_k \\
&\overset{1}{\geq} \sum_{j\in[d]\cup\{0\}} \binom{d}{j} \cdot \left(\prod_{i\in[d]} a_i\right)^{\frac{j}{d}} \\
&= \left(\left(\prod_{i\in[d]} a_i\right)^{\frac{1}{d}} + 1\right)^d \\
&= \left(\left(\prod_{i\in[d]} (N_i - 1)\right)^{\frac{1}{d}} + 1\right)^d,
\end{aligned}$$

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

$$\begin{aligned}
\sum_{\substack{i_1<i_2<\cdots<i_j \\ i_1,i_2,\cdots,i_j\in[d]}} \prod_{k\in\{i_1,i_2,\cdots,i_j\}} a_k &\geq \binom{d}{j} \cdot \left(\prod_{\substack{i_1<i_2<\cdots<i_j \\ i_1,i_2,\cdots,i_j\in[d]}} \prod_{k\in\{i_1,i_2,\cdots,i_j\}} a_k\right)^{\frac{1}{\binom{d}{j}}} \\
&= \binom{d}{j} \cdot \left(\prod_{i\in[d]} a_i\right)^{\frac{\binom{d-1}{j-1}}{\binom{d}{j}}} \\
&= \binom{d}{j} \cdot \left(\prod_{i\in[d]} a_i\right)^{\frac{j}{d}}.
\end{aligned}$$

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

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

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

$$\begin{aligned} \Delta &= \sup_{\substack{\theta\in\text{Supp}(\omega_\Theta),\\ \theta'\in\text{Supp}(\mathcal{M}_g(\theta))}} \mathfrak{D}\left(\omega_{X_\theta} \| \omega_{X_{\theta'}}\right) \\ &\geq \sup_{\theta_i\in\text{Supp}(\omega_\Theta), i\in\{1,2\}:\mathcal{M}_g(\theta_i)=\theta'} D\left(X_{\theta_1}, X_{\theta_2}\right) \qquad (16) \\ &> 2\gamma \cdot \left\lceil (1-T)^{1/d} \left\lceil \frac{1}{1-(1-T)^{1/d}} \right\rceil \right\rceil \cdot \left(\prod_{i\in[d]} \epsilon_i\right)^{1/d} \qquad (17) \\ &> 2\gamma \cdot \left\lceil \frac{1}{1-(1-T)^{1/d}} - 1 \right\rceil \cdot \left(\prod_{i\in[d]} \epsilon_i\right)^{1/d}, \end{aligned}$$

where in Eq. (16), θ_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 γ. □

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 γ that serves as a linkage between the distributional distance and the distance between secrets.

It follows from Eq. (11) there exists θ' s.t. $\sup_{\hat{g}} \mathbb{P}\left(\bigcap_{i\in[d]} \left|\hat{g}_i\left(\theta'\right) - g_i\left(\theta\right)\right| \leq \epsilon_i \middle| \theta'\right) \leq T$. 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 θ':

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

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

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

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

Therefore, we can get that

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

Hence, we have

$$\begin{aligned}
\Delta &= \sup_{\substack{\theta\in\text{Supp}(\omega_\Theta),\\ \theta'\in\text{Supp}(\mathcal{M}_g(\theta))}} \mathfrak{D}\left(\omega_{X_\theta} \| \omega_{X_{\theta'}}\right) \\
&\geq \sup_{\theta_i\in\text{Supp}(\omega_\Theta), i\in\{1,2\}:\mathcal{M}_g(\theta_i)=\theta'} D\left(X_{\theta_1}, X_{\theta_2}\right) \\
&> 2\gamma \cdot \left\lceil \frac{1}{T} \right\rceil^{1/d} \cdot \left(\prod_{i\in[d]} \epsilon_i \right)^{1/d} - 2\gamma \cdot \frac{1}{d} \sum_{i\in[d]} \epsilon_i .
\end{aligned} \tag{18}$$

□

B.3 Proof of Prop. 5.2

Proof. We first prove that for any fixed distortion budget δ_0, when $\Delta \leq \delta_0$, the achievable lower bound for union privacy, denoted as $\Pi^{\text{uni}}_{\epsilon,\omega_\Theta}$, is no smaller than that for intersection privacy, denoted as $\Pi^{\text{inter}}_{\epsilon,\omega_\Theta}$.

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

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

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

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

which indicates that with a fixed distortion budget δ_0, $\Pi^{\text{inter}}_{\epsilon,\omega_\Theta} \leq \Pi^{\text{uni}}_{\epsilon,\omega_\Theta}$. Hence, we can easily get that with a privacy budget T, the achievable distortion lower bounds for union privacy Δ_{union} and intersection privacy Δ_{inter} satisfy $\Delta_{\text{union}} \geq \Delta_{\text{inter}}$. □

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 γ that serves as a linkage between the distributional distance and the distance between secrets.

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

$$L^{(i)}_{\theta'} \triangleq \inf_{\theta\in\text{Supp}(\omega_\Theta):\mathcal{M}_g(\theta)=\theta'} g_i\left(\theta\right),$$
$$H^{(i)}_{\theta'} \triangleq \sup_{\theta\in\text{Supp}(\omega_\Theta):\mathcal{M}_g(\theta)=\theta'} g_i\left(\theta\right).$$

For each secret g_i, where $i \in [d]$, we partition the range of possible secret values, i.e., $[L^{(i)}_{\theta'}, H^{(i)}_{\theta'}]$, 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 $L^{(i)}_{\theta'} + 2N_i\epsilon_i \geq H^{(i)}_{\theta'} > L^{(i)}_{\theta'} + 2(N_i-1)\epsilon_i$.

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., $\hat{g}^{[\boldsymbol{v}]}_i\left(\theta'\right) = L^{(i)}_{\theta'} + (v_i - 0.5)\cdot 2\epsilon_i$. The number of multi-secret attack strategies, denoted as $\mathcal{N}$, is $\mathcal{N} = \prod_{i\in[d]} N_i$. We can get that

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

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

$$\begin{aligned}
&\sum_{\boldsymbol{v}} \sum_{j\in[\beta]} (-1)^{j-1} \sum_{\substack{b_1\neq b_2\neq\cdots\neq b_j \\ b_1,b_2,\cdots,b_j\in\mathcal{B}}} \mathbb{P}\left(\bigcap_{\substack{i\in\mathcal{I}_b \\ b\in\{b_1,b_2,\cdots,b_j\}}} |\hat{g}_i^{[\boldsymbol{v}]}(\theta') - g_i(\theta)| \leq \epsilon_i \middle| \theta' \right) \\
&= \sum_{j\in[\beta]} (-1)^{j-1} \sum_{\substack{b_1\neq b_2\neq\cdots\neq b_j \\ b_1,b_2,\cdots,b_j\in\mathcal{B}}} \sum_{\boldsymbol{v}} \mathbb{P}\left(\bigcap_{\substack{i\in\mathcal{I}_b \\ b\in\{b_1,b_2,\cdots,b_j\}}} |\hat{g}_i^{[\boldsymbol{v}]}(\theta') - g_i(\theta)| \leq \epsilon_i \middle| \theta' \right) \\
&\geq \sum_{j\in[\beta]} (-1)^{j-1} \sum_{\substack{b_1\neq b_2\neq\cdots\neq b_j \\ b_1,b_2,\cdots,b_j\in\mathcal{B}}} \prod_{k_1\in[d]\setminus\bigcup_{b\in\{b_1,b_2,\cdots,b_j\}}\mathcal{I}_b} N_{k_1} \\
&= \sum_{j\in[\beta]} (-1)^{j-1} \sum_{\substack{b_1\neq b_2\neq\cdots\neq b_j \\ b_1,b_2,\cdots,b_j\in\mathcal{B}}} \frac{\mathcal{N}}{\prod_{b\in\{b_1,b_2,\cdots,b_j\}} \prod_{k\in\mathcal{I}_b} N_k}.
\end{aligned}$$

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

$$\begin{aligned}
\mathcal{N} &= \prod_{b\in\mathcal{B}} (A_b + 1) \\
&= 1 + \sum_{j\in[\beta]} \sum_{\substack{b_1\neq b_2\neq\cdots\neq b_j \\ b_1,b_2,\cdots,b_j\in\mathcal{B}}} \prod_{b\in\{b_1,b_2,\cdots,b_j\}} A_b \\
&\overset{1}{\geq} \sum_{j\in[\beta]\cup\{0\}} \binom{\beta}{j} \cdot \left(\prod_{b\in\mathcal{B}} A_b\right)^{\frac{j}{\beta}} \\
&= \left(\left(\prod_{b\in\mathcal{B}} A_b\right)^{\frac{1}{\beta}} + 1 \right)^{\beta} \\
&= \left(\left(\prod_{b\in\mathcal{B}} \left(\prod_{i\in\mathcal{I}_b} N_i - 1\right)\right)^{\frac{1}{\beta}} + 1 \right)^{\beta}.
\end{aligned}$$

$\overset{1}{\geq}$ 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

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

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

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

Hence, we can get that

$$\begin{aligned} \sum_{i\in[d]} \left(H_{\theta'}^{(i)} - L_{\theta'}^{(i)}\right) &> \sum_{i\in[d]} 2\epsilon_i \left(N_i - 1\right) \\ &\geq 2d \left(\prod_{i\in[d]} \epsilon_i N_i\right)^{1/d} - 2\sum_{i\in[d]} \epsilon_i \\ &\geq 2d \cdot \left\lceil \frac{1}{\left(1-(1-T)^{1/\beta}\right)^{\beta/d}} \right\rceil \cdot \left(\prod_{i\in[d]} \epsilon_i\right)^{1/d} - 2\sum_{i\in[d]} \epsilon_i. \end{aligned}$$

Then we have

$$\begin{aligned} \Delta &= \sup_{\substack{\theta\in\text{Supp}(\omega_\Theta),\\ \theta'\in\text{Supp}(\mathcal{M}_g(\theta))}} \mathfrak{D}\left(\omega_{X_\theta} \| \omega_{X_{\theta'}}\right) \\ &\geq \sup_{\theta_i\in\text{Supp}(\omega_\Theta), i\in\{1,2\}:\mathcal{M}_g(\theta_i)=\theta'} D\left(X_{\theta_1}, X_{\theta_2}\right) \\ &> 2\gamma \cdot \left\lceil \frac{1}{\left(1-(1-T)^{1/\beta}\right)^{\beta/d}} \right\rceil \cdot \left(\prod_{i\in[d]} \epsilon_i\right)^{1/d} - 2\gamma \cdot \frac{1}{d}\sum_{i\in[d]} \epsilon_i. \end{aligned}$$

□

B.5 Comparsion Between Union Privacy and Group Secrets Privacy

When the group size β is equal to d, group secrets privacy transforms into union privacy. As shown in Prop. B.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 B.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 Δ_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 Δ_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

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

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

B.6 Proof of Thm. 5.4

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

$$\begin{aligned}\sup_{\hat{g}}\ \mathbb{P}\left(\left\|\hat{g}\left(\theta'\right)-g\left(\theta\right)\right\|_p\leq\varepsilon_p\right)&\geq\mathbb{P}\left(\left\|\tilde{g}\left(\theta'\right)-g\left(\theta\right)\right\|_p\leq\varepsilon_p\right)\\&\geq\mathbb{P}\left(\bigcap_{i\in[d]}\left|\tilde{g}_i\left(\theta'\right)-g_i\left(\theta\right)\right|\leq\tilde{\epsilon}_i\right)\\&=\sup_{\hat{g}}\ \mathbb{P}\left(\bigcap_{i\in[d]}\left|\hat{g}_i\left(\theta'\right)-g_i\left(\theta\right)\right|\leq\tilde{\epsilon}_i\right)\\&>T,\end{aligned}$$

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

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

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

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

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

□

B.7 Proof of Prop. 5.5 and More Analysis of l_p Norm Privacy

B.7.1 Proof of Prop. 5.5

Proof. We first prove that for any fixed distortion budget δ_0, when $\Delta\leq\delta_0$, the achievable lower bounds for union privacy $\Pi^{\text{uni}}_{\epsilon,\omega_\Theta}$, intersection privacy $\Pi^{\text{inter}}_{\epsilon,\omega_\Theta}$, and l_p norm privacy $\Pi^{l_p}_{\epsilon,\omega_\Theta}$ satisfy $\Pi^{\text{inter}}_{\epsilon,\omega_\Theta}\leq\Pi^{l_p}_{\epsilon,\omega_\Theta}\leq\Pi^{\text{uni}}_{\epsilon,\omega_\Theta}$.

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

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

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

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

which indicates that with a fixed distortion budget δ_0, $\Pi^{\text{inter}}_{\epsilon,\omega_\Theta}\leq\Pi^{l_p}_{\epsilon,\omega_\Theta}\leq\Pi^{\text{uni}}_{\epsilon,\omega_\Theta}$. Therefore, we can easily get that with a privacy budget T, the achievable distortion lower bounds for union privacy Δ_{union}, intersection privacy Δ_{inter}, and l_p norm privacy Δ_{l_p} satisfy $\Delta_{\text{union}}\geq\Delta_{l_p}\geq\Delta_{\text{inter}}$. □

B.7.2 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 B.2. *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 Δ_{l_α} and Δ_{l_τ} 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 δ_0, when $\Delta \leq \delta_0$, the achievable lower bound for l_τ privacy, denoted as $\Pi^{l_\tau}_{\epsilon,\omega_\Theta}$, is no smaller than that for l_α 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 δ_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_α privacy Δ_{l_α} and l_τ privacy Δ_{l_τ} satisfy $\Delta_{l_\alpha} \leq \Delta_{l_\tau}$. □

B.8 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 $\mathcal{X} = \{\boldsymbol{x}_1, \cdots, \boldsymbol{x}_m\}, \mathcal{Y} = \{\boldsymbol{y}_1, \cdots, \boldsymbol{y}_m\}$, 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 $\mathcal{Y}$, satisfies

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

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

For union privacy, we have

$$\begin{aligned}
\tilde{\Delta} &\geq \sqrt{\left(\hat{\mu}_x^{(1)} - \hat{\mu}_y^{(1)}\right)^2 + \left(\hat{\mu}_x^{(2)} - \hat{\mu}_y^{(2)}\right)^2 + \left(\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}\right)^2} \\
&= \sqrt{\epsilon_1^2 \cdot \frac{|\hat{\mu}_x^{(1)} - \hat{\mu}_y^{(1)}|^2}{\epsilon_1^2} + \epsilon_2^2 \cdot \frac{|\hat{\mu}_x^{(2)} - \hat{\mu}_y^{(2)}|^2}{\epsilon_2^2} + \epsilon_3^2 \cdot \frac{|\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}|^2}{\epsilon_3^2}} \\
&\geq \sqrt{\epsilon_1^2 + \epsilon_2^2 + \epsilon_3^2} \cdot \min_{i \in [3]} \left\{ \frac{|\hat{\mu}_x^{(i)} - \hat{\mu}_y^{(i)}|}{\epsilon_i} \right\} \\
&= -\sqrt{\epsilon_1^2 + \epsilon_2^2 + \epsilon_3^2} \cdot \max_{i \in [3]} \left\{ -\frac{|\hat{\mu}_x^{(i)} - \hat{\mu}_y^{(i)}|}{\epsilon_i} \right\} \\
&= -\sqrt{\epsilon_1^2 + \epsilon_2^2 + \epsilon_3^2} \cdot \tilde{\Pi}^{\text{uni}}_{\epsilon, \omega_\Theta}.
\end{aligned}$$

For intersection privacy, we have

$$\begin{aligned}
\tilde{\Delta} &\geq \sqrt{\left(\hat{\mu}_x^{(1)} - \hat{\mu}_y^{(1)}\right)^2 + \left(\hat{\mu}_x^{(2)} - \hat{\mu}_y^{(2)}\right)^2 + \left(\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}\right)^2} \\
&= \sqrt{\epsilon_1^2 \cdot \frac{|\hat{\mu}_x^{(1)} - \hat{\mu}_y^{(1)}|^2}{\epsilon_1^2} + \epsilon_2^2 \cdot \frac{|\hat{\mu}_x^{(2)} - \hat{\mu}_y^{(2)}|^2}{\epsilon_2^2} + \epsilon_3^2 \cdot \frac{|\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}|^2}{\epsilon_3^2}} \\
&\geq \min\{\epsilon_1, \epsilon_2, \epsilon_3\} \cdot \max_{i \in [3]} \left\{ \frac{|\hat{\mu}_x^{(i)} - \hat{\mu}_y^{(i)}|}{\epsilon_i} \right\} \\
&= -\min\{\epsilon_1, \epsilon_2, \epsilon_3\} \cdot \min_{i \in [3]} \left\{ -\frac{|\hat{\mu}_x^{(i)} - \hat{\mu}_y^{(i)}|}{\epsilon_i} \right\} \\
&= -\min\{\epsilon_1, \epsilon_2, \epsilon_3\} \tilde{\Pi}^{\text{inter}}_{\epsilon, \omega_\Theta}.
\end{aligned}$$

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

$$\begin{aligned}
\tilde{\Delta} &\geq \sqrt{\left(\hat{\mu}_x^{(1)} - \hat{\mu}_y^{(1)}\right)^2 + \left(\hat{\mu}_x^{(2)} - \hat{\mu}_y^{(2)}\right)^2 + \left(\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}\right)^2} \\
&= \sqrt{\epsilon_1^2 \cdot \frac{|\hat{\mu}_x^{(1)} - \hat{\mu}_y^{(1)}|^2}{\epsilon_1^2} + \epsilon_2^2 \cdot \frac{|\hat{\mu}_x^{(2)} - \hat{\mu}_y^{(2)}|^2}{\epsilon_2^2} + \epsilon_3^2 \cdot \frac{|\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}|^2}{\epsilon_3^2}} \\
&\geq \sqrt{\min\{\epsilon_1^2, \epsilon_2^2\} \cdot \max_{i \in [2]} \left\{ \frac{|\hat{\mu}_x^{(i)} - \hat{\mu}_y^{(i)}|^2}{\epsilon_i^2} \right\} + \epsilon_3^2 \cdot \frac{|\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}|^2}{\epsilon_3^2}} \\
&\geq \sqrt{\min\{\epsilon_1^2, \epsilon_2^2\} + \epsilon_3^2} \cdot \min \left\{ \max_{i \in [2]} \left\{ \frac{|\hat{\mu}_x^{(i)} - \hat{\mu}_y^{(i)}|}{\epsilon_i} \right\}, \frac{|\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}|}{\epsilon_3} \right\} \\
&= -\sqrt{\min\{\epsilon_1^2, \epsilon_2^2\} + \epsilon_3^2} \cdot \max \left\{ \min_{i \in [2]} \left\{ -\frac{|\hat{\mu}_x^{(i)} - \hat{\mu}_y^{(i)}|}{\epsilon_i} \right\}, -\frac{|\hat{\mu}_x^{(3)} - \hat{\mu}_y^{(3)}|}{\epsilon_3} \right\} \\
&= -\sqrt{\min\{\epsilon_1^2, \epsilon_2^2\} + \epsilon_3^2} \cdot \tilde{\Pi}^{\text{group}}_{\epsilon, \omega_\Theta}.
\end{aligned}$$

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

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

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

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

C Case Studies under Union Privacy

In this section, we instantiate the general result from §4 on Gaussian distributions with multiple secrets. For each distribution setting, we establish the distortion lower bound, devise a data release mechanism, and assess its privacy-distortion performance. In App. C.4, we demonstrate how to extend the data release mechanism to accommodate dataset input/output when the data holder does not know distribution parameters.

C.1 Secrets = Mean and Standard Deviation, Distribution = 1-Dimensional Gaussian

As a starting point, we show how to protect mean μ and standard deviation (SD) σ of a one-dimensional Gaussian distribution with $\theta = (\mu, \sigma)$. Note that for the 1D Gaussian distribution, as it can be entirely characterized by parameters μ and σ, protecting both parameters is equivalent to protecting all statistical properties of the distribution. We instantiate the privacy-distortion tradeoff lower bound in Prop. C.1.

Proposition C.1. *For 1-dimensional Gaussian distribution with $\theta = (\mu, \sigma)$, consider the secrets $g_1(\theta) = \mu,\ g_2(\theta) = \sigma$. For any $T \in (0, 1)$, when $\Pi_{\epsilon,\omega_\Theta} \leq T$,*

$$\Delta > \sqrt{2} \cdot \left\lceil \frac{1}{1 - \sqrt{1 - T}} - 1 \right\rceil \cdot \sqrt{\epsilon_1 \epsilon_2}.$$

The proof is shown in App. C.5.1. We then design a data release mechanism to approximate the tradeoff lower bound. Intuitively, we partition the ranges of possible values of μ and σ into intervals of lengths s_μ and s_σ respectively. The mechanism then outputs the midpoints of the respective intervals into which the original μ and σ fit. Precisely, the designed mechanism is shown in Alg. 1.

For the mechanism privacy-distortion analysis, we consider the case where the prior distributions of parameters μ and σ are uniform.

Proposition C.2 (Mechanism privacy-distortion tradeoff)**.** *Under the assumption that parameters μ, σ follow the uniform distribution, Alg. 1 has*

$$\begin{aligned}\Pi_{\epsilon,\omega_\Theta} &= \frac{2\epsilon_1}{s_\mu} + \frac{2\epsilon_2}{s_\sigma} - \frac{2\epsilon_1}{s_\mu} \cdot \frac{2\epsilon_2}{s_\sigma}, \\ \Delta &= \frac{1}{2}\sqrt{s_\mu^2 + s_\sigma^2} < c_{\epsilon,s} \cdot \Delta_{opt},\end{aligned}$$

Algorithm 1: Data release mechanism for 1-dimensional Gaussian with secrets as mean and SD.

Input: $\theta = (\mu, \sigma)$, lower bound $\underline{\mu}$ of μ, lower bound $\underline{\sigma}$ for σ, quantization intervals s_μ, s_σ.

$\mu' \leftarrow \underline{\mu} + \left(\lfloor \frac{\mu - \underline{\mu}}{s_\mu} \rfloor + 0.5 \right) \cdot s_\mu$;

$\sigma' \leftarrow \underline{\sigma} + \left(\lfloor \frac{\sigma - \underline{\sigma}}{s_\sigma} \rfloor + 0.5 \right) \cdot s_\sigma$;

Output Gaussian distribution with $\theta' = (\mu', \sigma')$.

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

The proof is shown in App. C.5.2. Prop. C.2 shows that Alg. 1 achieves order-optimal privacy-distortion performance with a constant multiplication factor.

C.2 Secrets = {Mean, SD}^{d}, Distribution = Multivariate Gaussian with Dimensionally Independent Variables

In practice, data often exhibits high dimensionality. In this section, we focus on k-dimensional Gaussian distribution ($k \in \mathbb{Z}^+$) with dimensionally 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 general analysis of multivariate Gaussian distribution in App. C.3. 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 in Prop. C.3.

Proposition C.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 $\Pi_{\epsilon,\omega_\Theta} \leq T$,*

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

The proof is shown in App. C.5.3. Next, we provide a data release mechanism that approximates the tradeoff lower bound. Similar to Alg. 1, we design quantization mechanism to divide the range of possible secret values into intervals with lengths s_{g_i} for each secret g_i, $i \in [d]$. The mechanism outputs the midpoints of the intervals within which the original secrets reside. Precisely, we provide the mechanism in Alg. 2.

Algorithm 2: 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}, $\forall i \in [d]$.

for each $i \in [d]$: $g_i'(\theta) \leftarrow \underline{g_i} + \left(\lfloor \frac{g_i(\theta) - \underline{g_i}}{s_{g_i}} \rfloor + 0.5 \right) \cdot s_{g_i}$;

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 assume that the prior distributions of secret distribution parameters $g_1, \cdots, g_d$ are uniform.

Proposition C.4 (Mechanism privacy-distortion tradeoff)**.** *Under the assumption that secret distribution parameters $g_1, \cdots, g_d$ follow the uniform distribution, Alg. 2 has*

$$\Pi_{\epsilon,\omega_\Theta} = 1 - \prod_{i\in[d]} \left(1 - \frac{2\epsilon_i}{s_{g_i}}\right),$$
$$\Delta = \frac{1}{2}\sqrt{\sum_{i\in[d]} {s_{g_i}}^2} < c_{\epsilon,s} \cdot \Delta_{opt}.$$

where $c_{\epsilon,s}$ is a constant depending on tolerance ranges and the interval lengths of the mechanism, and Δ_{opt} is the optimal achievable distortion under the privacy achieved by Alg. 2.

The proof is shown in App. C.5.4. From Prop. C.4 we know that Alg. 2 is order-optimal with constant multiplication factor.

C.3 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. C.5.

Proposition C.5. *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 $\Pi_{\epsilon,\omega_\Theta} \leq T$,*

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

The proof is shown in App. C.5.5. We then design a quantization data release mechanism to approximate the tradeoff lower bound. Intuitively, if the secret is a mean μ_i ($i \in \{1, 2\}$), we partition the range of possible values of it into intervals of lengths s_{μ_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. 3. 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.

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 C.6 (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. 3 has*

$$\Pi_{\epsilon,\omega_\Theta} \leq P_\mu + P_\sigma - P_\mu P_\sigma,$$
$$\Delta = \frac{1}{2}\sqrt{\sum_{i:\mu_i\in\mathcal{G}} s_{\mu_i}^2 + \mathbb{1}_{\{\sigma_1,\sigma_2\}\cap\mathcal{G}\neq\emptyset} \cdot (s_a^2 + s_b^2)},$$

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

Algorithm 3: 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 $\mathcal{G}$.

for each $i \in \{1, 2\}$:
  if $\mu_i \in \mathcal{G}$: $\mu_i' \leftarrow \underline{\mu_i} + \left(\lfloor \frac{\mu_i - \underline{\mu_i}}{s_{\mu_i}} \rfloor + 0.5\right) \cdot s_{\mu_i}$;
  else: $\mu_i' \leftarrow \mu_i$;
if $\{\sigma_1, \sigma_2\} \cap \mathcal{G} \neq \emptyset$:
  $a' \leftarrow \underline{a} + \left(\lfloor \frac{a - \underline{a}}{s_a} \rfloor + 0.5\right) \cdot s_a$;
  $b' \leftarrow \underline{b} + \left(\lfloor \frac{b - \underline{b}}{s_b} \rfloor + 0.5\right) \cdot s_b$;
else: $a' \leftarrow a$, $b' \leftarrow b$;

Output: Gaussian distribution with parameter $\theta' = \left(\mu_1', \mu_2', a'^2, b'^2, \alpha\right)$.

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

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

The proof is shown in App. C.5.9.

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. 3, we design a quantization data release mechanism. If a secret is mean μ_i ($i \in [k]$), we partition the range of possible values of it into intervals of lengths s_{μ_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. 4.

C.4 Extending Data Release Mechanisms to Accommodate Dataset Input/Output

In practice, the data holder may only possess the dataset without knowing the distribution parameters. Similar to Lin et al. (2023), our data release mechanisms can be easily extended for dataset input/output. Briefly, the data holder estimates the parameters θ from the data and maps them to corresponding intervals. Once the released parameters θ' are determined, each sample is adjusted to conform to the distribution characterized by θ'.

We take Alg. 1 as an example to demonstrate the extension process. For a dataset $\mathcal{X} = \{x_1, \ldots, x_m\}$, the concrete steps of the extended mechanism are:

Algorithm 4: 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 $\mathcal{G}$.

for each $i \in [k]$:
  if $\mu_i \in \mathcal{G}$: $\mu_i' \leftarrow \underline{\mu_i} + \left(\lfloor \frac{\mu_i - \underline{\mu_i}}{s_{\mu_i}} \rfloor + 0.5\right) \cdot s_{\mu_i}$;
  else: $\mu_i' \leftarrow \mu_i$;
if $\{\sigma_1, \cdots, \sigma_k\} \cap \mathcal{G} \neq \emptyset$:
  for each $i \in [k]$: $a_i' \leftarrow \underline{a_i} + \left(\lfloor \frac{a_i - \underline{a_i}}{s_{a_i}} \rfloor + 0.5\right) \cdot s_{a_i}$;
else: **for** each $i \in [k]$: $a_i' \leftarrow a_i$;

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

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: $\mu_r = \underline{\mu} + \left(i + \frac{1}{2}\right) \cdot s_\mu$, $\sigma_r = \underline{\sigma} + \left(j + \frac{1}{2}\right) \cdot s_\sigma$.
4. Modify each sample x_i as $x_i' = \frac{\sigma_r}{\hat{\sigma}}(x_i - \hat{\mu}) + \mu_r$, and release the dataset $\mathcal{X}' = \{x_1', \ldots, x_m'\}$.

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

C.5 Proofs

C.5.1 Proof of Prop. C.1

Proof. Define $\theta' = (\mu', \sigma')$. For the 1-dimensional Gaussian, we have

$$D(X_\theta, X_{\theta'}) = \frac{1}{2}\mathfrak{D}\left(\omega_{X_\theta} \| \omega_{X_{\theta'}}\right) = \frac{1}{2}\sqrt{(\mu - \mu')^2 + (\sigma - \sigma')^2}.$$

We can get that

$$\begin{aligned}
\frac{D(X_\theta, X_{\theta'})}{R(X_\theta, X_{\theta'})} &= \frac{\sqrt{(\mu - \mu')^2 + (\sigma - \sigma')^2}}{2\sqrt{(\mu - \mu')(\sigma - \sigma')}} \\
&= \frac{1}{2}\sqrt{\frac{\mu - \mu'}{\sigma - \sigma'} + \frac{\sigma - \sigma'}{\mu - \mu'}} \\
&\geq \frac{\sqrt{2}}{2}.
\end{aligned}$$

Hence, we have

$$\gamma = \inf_{\theta, \theta' \in \text{Supp}(\omega_\Theta)} \frac{D(X_\theta, X_{\theta'})}{R(X_\theta, X_{\theta'})} = \frac{\sqrt{2}}{2}.$$

Based on Thm. 4.1, we can get that

$$\Delta > \sqrt{2} \cdot \left[\frac{1}{1 - \sqrt{1 - T}} - 1\right] \cdot \sqrt{\epsilon_1 \epsilon_2}.$$

□

C.5.2 PROOF OF PROP. C.2

Proof. We can easily can get that the distortion Δ of Alg. 1 is

$$\Delta = \sqrt{\left(\frac{s_\mu}{2}\right)^2 + \left(\frac{s_\sigma}{2}\right)^2} = \frac{1}{2}\sqrt{s_\mu^2 + s_\sigma^2}.$$

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

$$\begin{aligned}
\Pi_{\epsilon,\omega_\Theta} &= \sup_{\hat{\boldsymbol{g}}} \mathbb{P}\left(\bigcup_{i\in[2]} \left|\hat{g}_i\left(\theta'\right) - g_i\left(\theta\right)\right| \leq \epsilon_i\right) \\
&= 1 - \sup_{\hat{\boldsymbol{g}}} \mathbb{P}\left(\bigcap_{i\in[2]} \left|\hat{g}_i\left(\theta'\right) - g_i\left(\theta\right)\right| > \epsilon_i\right) \\
&= 1 - \sup_{\hat{\boldsymbol{g}}} \prod_{i\in[2]} \mathbb{P}\left(\left|\hat{g}_i\left(\theta'\right) - g_i\left(\theta\right)\right| > \epsilon_i\right) \\
&= 1 - \prod_{i\in[2]}\left(1 - \frac{2\epsilon_i}{s_{g_i}}\right) \\
&= \frac{2\epsilon_1}{s_\mu} + \frac{2\epsilon_2}{s_\sigma} - \frac{2\epsilon_1}{s_\mu}\cdot\frac{2\epsilon_2}{s_\sigma}.
\end{aligned}$$

From Prop. C.3, we know that the optimal achievable distortion Δ_{opt} satisfy

$$\begin{aligned}
\Delta_{opt} &> \sqrt{2}\cdot\left\lceil \frac{1}{1-\sqrt{1-\Pi_{\epsilon,\omega_\Theta}}} - 1\right\rceil \cdot \sqrt{\epsilon_1\epsilon_2} \\
&= \sqrt{2}\cdot\left\lceil \frac{1}{1-\prod_{i\in[2]}\left(1-\frac{2\epsilon_i}{s_{g_i}}\right)^{1/2}} - 1\right\rceil \cdot \sqrt{\epsilon_1\epsilon_2}.
\end{aligned}$$

Let $k = \frac{\Delta}{\Delta_{opt}}$, $x_i = \frac{\epsilon_i}{s_{g_i}}, \forall i \in [2]$, $c_1 = \min\{x_1, x_2\}$, and $c_2 = \max\{x_1, x_2\}$, we have

$$\begin{aligned}
k &< \frac{\sqrt{s_\mu^2 + s_\sigma^2}}{2\sqrt{2}\cdot\left\lceil \frac{1}{1-\prod_{i\in[2]}\left(1-\frac{2\epsilon_i}{s_{g_i}}\right)^{1/2}} - 1\right\rceil \cdot \sqrt{\epsilon_1\epsilon_2}} \\
&= \frac{\sqrt{\left(\frac{\epsilon_1}{x_1}\right)^2 + \left(\frac{\epsilon_2}{x_2}\right)^2}}{2\sqrt{2}\cdot\left\lceil \frac{1}{1-\prod_{i\in[2]}(1-2x_i)^{1/2}} - 1\right\rceil \cdot \sqrt{\epsilon_1\epsilon_2}} \\
&\leq \frac{\sqrt{\epsilon_1^2+\epsilon_2^2}\cdot c_2}{c_1(1-2c_2)\sqrt{2\epsilon_1\epsilon_2}} \\
&= \frac{\sqrt{\epsilon_1^2+\epsilon_2^2}}{\sqrt{2\epsilon_1\epsilon_2}}\cdot\frac{c_2}{c_1(1-2c_2)}.
\end{aligned}$$

Let $c_\epsilon = \frac{\sqrt{\epsilon_1^2+\epsilon_2^2}}{\sqrt{2\epsilon_1\epsilon_2}}$, a constant depending on the values of tolerance ranges. Denoting $c_{\epsilon,s} = \frac{c_\epsilon c_2}{c_1(1-2c_2)}$, we can finally get that

$$\Delta = k\Delta_{opt} < c_{\epsilon,s}\Delta_{opt},$$

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

Specifically, when $\epsilon_1 = \epsilon_2$, and the designed data released mechanism satisfies $\frac{\epsilon_1}{s_\mu} = \frac{\epsilon_2}{s_\sigma} \leq \frac{1}{4}$, we can get that $\Delta < 2\Delta_{opt}$.

□

C.5.3 PROOF OF PROP. C.3

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

Lemma C.7. *$D\left(X_\theta, X_{\theta'}\right)$ 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. C.5.3.

Based on Lemma C.7, we can get that

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

Therefore, we have

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

Based on Thm. 4.1, we can get that

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

□

Proof of Lemma C.7

Proof. From Givens & Shortt (1984), we have

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

where diagonal covariance matrices Σ, Σ' 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

$$\Sigma + \Sigma' - 2\left(\Sigma^{\frac{1}{2}}\Sigma'\Sigma^{\frac{1}{2}}\right)^{\frac{1}{2}} = \begin{bmatrix} {\sigma_1}^2 + {\sigma'_1}^2 & & & \\ & {\sigma_2}^2 + {\sigma'_2}^2 & & \\ & & \ddots & \\ & & & {\sigma_k}^2 + {\sigma'_k}^2 \end{bmatrix} - 2\begin{bmatrix} {\sigma_1}^2{\sigma'_1}^2 & & & \\ & {\sigma_2}^2{\sigma'_2}^2 & & \\ & & \ddots & \\ & & & {\sigma_k}^2{\sigma'_k}^2 \end{bmatrix}^{\frac{1}{2}}$$
$$= \begin{bmatrix} (\sigma_1 - \sigma'_1)^2 & & & \\ & (\sigma_2 - \sigma'_2)^2 & & \\ & & \ddots & \\ & & & (\sigma_k - \sigma'_k)^2 \end{bmatrix}.$$

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

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

□

C.5.4 Proof of Prop. C.4

Proof. Based on Lemma C.7, we can easily can get that the distortion Δ of Alg. 2 is

$$\Delta = \frac{1}{2}\sqrt{\sum_{i\in[d]} {s_{g_i}}^2}.$$

Since the secret distribution parameters are independent of each other and follow the uniform distributions, we can get that the privacy of Alg. 2 is

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

From Prop. C.3, we know that the optimal achievable distortion Δ_{opt} satisfy

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

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

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

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

$$\Delta=k\Delta_{opt}<c_{\epsilon,s}\Delta_{opt},$$

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 $\frac{\epsilon_1}{s_{g_1}}=\cdots=\frac{\epsilon_g}{s_{g_d}}\le\frac{1}{4}$, we can get that $\Delta<2\Delta_{opt}$. □

C.5.5 Proof of Prop. C.5

Proof. Let $\theta'=(\mu_1',\mu_2',\lambda_1',\lambda_2',\alpha')$. From Givens & Shortt (1984), we have

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

We provide a lower bound on $\mathfrak{D}\left(\omega_{X_\theta}\|\omega_{X_{\theta'}}\right)$ in Lemma C.8.

Lemma C.8. *$\mathfrak{D}\left(\omega_{X_\theta}\|\omega_{X_{\theta'}}\right)^2$ can be lower bounded as*

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

The proof is shown in App. C.5.6.

Based on Lemma C.8, we can get that

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

□

C.5.6 Proof of Lemma C.8

Proof. To proof Lemma C.8, we first provide two lemmas as follows.

Lemma C.9. $\mathfrak{D}\left(\omega_{X_\theta}\|\omega_{X_{\theta'}}\right)^2$ *can be derived as:*

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

The proof is shown in App. C.5.7.

Lemma C.10.

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

The proof is in App. C.5.8

Based on Lemma C.9 and Lemma C.10, we have

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

□

C.5.7 Proof of Lemma C.9

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

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

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

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

Therefore, we have

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

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

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

Therefore, we have

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

Hence,

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

□

C.5.8 Proof of Lemma C.10

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

$$\begin{aligned}B &\triangleq \sqrt{\left(\lambda_1\lambda_1' + \lambda_2\lambda_2'\right)\cos^2\left(\alpha-\alpha'\right) + \left(\lambda_1\lambda_2' + \lambda_2\lambda_1'\right)\sin^2\left(\alpha-\alpha'\right) + 2\sqrt{\lambda_1\lambda_1'\lambda_2\lambda_2'}}\\ &= \sqrt{\left(a\tilde{a} + b\tilde{b}\right)^2\cos^2\left(\alpha-\alpha'\right) + \left(a\tilde{b} + b\tilde{a}\right)^2\sin^2\left(\alpha-\alpha'\right)}.\end{aligned}$$

We then can derive that

$$\begin{aligned}A^2 - B^2 &= 2\sqrt{\left(a^2\cos^2\alpha + b^2\sin^2\alpha\right)\left(\tilde{a}^2\cos^2\alpha' + \tilde{b}^2\sin^2\alpha'\right)\left(a^2\sin^2\alpha + b^2\cos^2\alpha\right)\left(\tilde{a}^2\sin^2\alpha' + \tilde{b}^2\cos^2\alpha'\right)}\\ &\quad - 2a\tilde{a}b\tilde{b} - 2\cos\alpha\cos\alpha'\sin\alpha\sin\alpha'\left(a^2\tilde{a}^2 + b^2\tilde{b}^2 - a^2\tilde{b}^2 - b^2\tilde{a}^2\right).\end{aligned}$$

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

$$\begin{aligned}
C^2 &= a^2\tilde{a}^2b^2\tilde{b}^2\left(\cos^4\alpha + \sin^4\alpha\right)\left(\cos^4\alpha' + \sin^4\alpha'\right) + a^4\tilde{a}^2\tilde{b}^2\cos^2\alpha\sin^2\alpha\left(\cos^4\alpha' + \sin^4\alpha'\right) \\
&\quad + a^2b^2\tilde{b}^4\cos^2\alpha'\sin^2\alpha'\left(\cos^4\alpha + \sin^4\alpha\right) + \tilde{a}^2b^4\tilde{b}^2\cos^2\alpha\sin^2\alpha\left(\cos^4\alpha' + \sin^4\alpha'\right) \\
&\quad + a^2\tilde{a}^4b^2\cos^2\alpha'\sin^2\alpha'\left(\cos^4\alpha + \sin^4\alpha\right) \\
&= a^2\tilde{a}^2b^2\tilde{b}^2\left(1 - 2\cos^2\alpha\sin^2\alpha\right)\left(1 - 2\cos^2\alpha'\sin^2\alpha'\right) + \left(a^4 + b^4\right)\tilde{a}^2\tilde{b}^2\cos^2\alpha\sin^2\alpha\left(1 - 2\cos^2\alpha'\sin^2\alpha'\right) \\
&\quad + \left(\tilde{a}^4 + \tilde{b}^4\right)a^2b^2\cos^2\alpha'\sin^2\alpha'\left(1 - 2\cos^2\alpha\sin^2\alpha\right),
\end{aligned}$$

and

$$\begin{aligned}
D^2 &= a^2\tilde{a}^2b^2\tilde{b}^2\left(1 + 4\cos^2\alpha\cos^2\alpha'\sin^2\alpha\sin^2\alpha'\right) + 2\cos\alpha\cos\alpha'\sin\alpha\sin\alpha'a\tilde{a}b\tilde{b}\left(a^2\tilde{a}^2 + b^2\tilde{b}^2 - a^2\tilde{b}^2 - b^2\tilde{a}^2\right) \\
&\quad - 2\cos^2\alpha\cos^2\alpha'\sin^2\alpha\sin^2\alpha'\left(\left(a^4 + b^4\right)\tilde{a}^2\tilde{b}^2 + \left(\tilde{a}^4 + \tilde{b}^4\right)a^2b^2\right).
\end{aligned}$$

Then we have

$$\begin{aligned}
C^2 - D^2 &= \cos^2\alpha\sin^2\alpha\left(a^4 + b^4\right)\tilde{a}^2\tilde{b}^2 + \cos^2\alpha'\sin^2\alpha'\left(\tilde{a}^4 + \tilde{b}^4\right)a^2b^2 - 2a^2\tilde{a}^2b^2\tilde{b}^2\left(\cos^2\alpha\sin^2\alpha + \cos^2\alpha'\sin^2\alpha'\right) \\
&\quad - 2\cos\alpha\cos\alpha'\sin\alpha\sin\alpha'a\tilde{a}b\tilde{b}\left(a^2\tilde{a}^2 + b^2\tilde{b}^2 - a^2\tilde{b}^2 - b^2\tilde{a}^2\right) \\
&= \cos^2\alpha\sin^2\alpha\left(a^2 - b^2\right)^2\tilde{a}^2\tilde{b}^2 + \cos^2\alpha'\sin^2\alpha'\left(\tilde{a}^2 - \tilde{b}^2\right)^2a^2b^2 - 2\cos\alpha\cos\alpha'\sin\alpha\sin\alpha'a\tilde{a}b\tilde{b}\left(a^2 - b^2\right)\left(\tilde{a}^2 - \right. \\
&\geq 2\sqrt{\cos^2\alpha\sin^2\alpha\cos^2\alpha'\sin^2\alpha'\tilde{a}^2\tilde{b}^2a^2b^2\left(a^2 - b^2\right)^2\left(\tilde{a}^2 - \tilde{b}^2\right)^2} - 2\cos\alpha\cos\alpha'\sin\alpha\sin\alpha'a\tilde{a}b\tilde{b}\left(a^2 - b^2\right)\left(\tilde{a}^2 - \right. \\
&= 0
\end{aligned}$$

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.,

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

□

C.5.9 Proof of Prop. C.6

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

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

Therefore, we have

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

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

Lemma C.11. *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* $a, b \geq 0$, *we have*

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

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

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* $a \geq \delta'_{\sigma_1,\alpha}, b \geq \delta'_{\sigma_1,\beta}$, *we have*

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

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* $a \geq \delta'_{\sigma_2,\alpha}, b \geq \delta'_{\sigma_2,\beta}$, *we have*

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

The proof is shown in App. C.5.10.

Suppose the parameters Alg. 3 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

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

The probability of the attacker guessing the secret σ_1 within the tolerance range is:

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

Based on Lemma C.11, we have

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

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

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

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

$$\begin{aligned}
\mathbb{P}\left(|\hat{g}_{\sigma_1}(\theta') - g_{\sigma_1}(\theta)| \leq \epsilon_{\sigma_1}\right) &= \mathbb{P}\Bigg[\left(\sqrt{a^2\cos^2\alpha + b^2\sin^2\alpha} \geq \sqrt{\hat{a}^2\cos^2\alpha + \hat{b}^2\sin^2\alpha} - \epsilon_{\sigma_1}\right) \cup \\
&\qquad \left(\sqrt{a^2\cos^2\alpha + b^2\sin^2\alpha} \leq \sqrt{\hat{a}^2\cos^2\alpha + \hat{b}^2\sin^2\alpha} + \epsilon_{\sigma_1}\right)\Bigg] \\
&\leq \sup_{\hat{a},\hat{b}} \Big(1 - \max\left\{t_a s_a - \delta'_{\sigma_1,\alpha}, 0\right\}\cdot\max\left\{t_b s_b - \delta'_{\sigma_1,\beta}, 0\right\}/s_a s_b \\
&\qquad - \max\left\{(1-t_a)\,s_a - \delta_{\sigma_1,\alpha}, 0\right\}\cdot\max\left\{(1-t_b)\,s_b - \delta_{\sigma_1,\beta}, 0\right\}/s_a s_b\Big).
\end{aligned}$$

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

$$\begin{aligned}
\mathbb{P}\left(|\hat{g}_{\sigma_1}(\theta') - g_{\sigma_1}(\theta)| \le \epsilon_{\sigma_1}\right) &\le \sup_{x,y}\Big(1 - \max\{x,0\}\cdot\max\{y,0\}/s_a s_b \\
&\qquad - \max\left\{s_a - \delta_{\sigma_1,\alpha} - \delta'_{\sigma_1,\alpha} - x, 0\right\}\cdot\max\left\{s_b - \delta_{\sigma_1,\beta} - \delta'_{\sigma_1,\beta} - y, 0\right\}/s_a s_b\Big) \\
&= 1 - \frac{1}{2}\max\left\{s_a - \delta_{\sigma_1,\alpha} - \delta'_{\sigma_1,\alpha}, 0\right\}\cdot\max\left\{s_b - \delta_{\sigma_1,\beta} - \delta'_{\sigma_1,\beta}, 0\right\}/s_a s_b \\
&= \begin{cases} 1, & L^{(\alpha)}_{\sigma_1} \le 0 \text{ or } L^{(\beta)}_{\sigma_1} \le 0 \\ 1 - \frac{1}{2}L^{(\alpha)}_{\sigma_1}L^{(\beta)}_{\sigma_1}/s_a s_b, & \text{otherwise} \end{cases} \\
&= P_{\sigma_1}.
\end{aligned}$$

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

$$\begin{aligned}
\mathbb{P}\left(|\hat{g}_{\sigma_2}(\theta') - g_{\sigma_2}(\theta)| \le \epsilon_{\sigma_2}\right) &\le \sup_{\hat{a},\hat{b}}\Big(1 - \max\left\{t_a s_a - \delta'_{\sigma_2,\alpha}, 0\right\}\cdot\max\left\{t_b s_b - \delta'_{\sigma_2,\beta}, 0\right\}/s_a s_b \\
&\qquad - \max\left\{(1-t_a)s_a - \delta_{\sigma_2,\alpha}, 0\right\}\cdot\max\left\{(1-t_b)s_b - \delta_{\sigma_2,\beta}, 0\right\}/s_a s_b\Big) \\
&= \begin{cases} 1, & L^{(\alpha)}_{\sigma_2} \le 0 \text{ or } L^{(\beta)}_{\sigma_2} \le 0 \\ 1 - \frac{1}{2}L^{(\alpha)}_{\sigma_2}L^{(\beta)}_{\sigma_2}/s_a s_b, & \text{otherwise} \end{cases} \\
&= P_{\sigma_2}.
\end{aligned}$$

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

$$\begin{aligned}
&\mathbb{P}\left(|\hat{g}_{\sigma_1}(\theta') - g_{\sigma_1}(\theta)| \le \epsilon_{\sigma_1} \cup |\hat{g}_{\sigma_2}(\theta') - g_{\sigma_2}(\theta)| \le \epsilon_{\sigma_2}\right) \\
&\quad\le \sup_{\hat{a},\hat{b}}\Big(1 - \max\left\{t_a s_a - \max\left\{\delta'_{\sigma_1,\alpha}, \delta'_{\sigma_2,\alpha}\right\}, 0\right\}\cdot\max\left\{t_b s_b - \max\left(\delta'_{\sigma_1,\beta}, \delta'_{\sigma_2,\beta}\right), 0\right\}/s_a s_b \\
&\qquad\quad - \max\left\{(1-t_a)s_a - \max\left(\delta_{\sigma_1,\alpha}, \delta_{\sigma_2,\alpha}\right), 0\right\}\cdot\max\left\{(1-t_b)s_b - \max\left(\delta_{\sigma_1,\beta}, \delta_{\sigma_2,\beta}\right), 0\right\}/s_a s_b\Big) \\
&\quad= \begin{cases} 1, & L^{(\alpha)}_{\sigma_1,\sigma_2} \le 0 \text{ or } L^{(\beta)}_{\sigma_1,\sigma_2} \le 0 \\ 1 - \frac{1}{2}L^{(\alpha)}_{\sigma_1,\sigma_2}L^{(\beta)}_{\sigma_1,\sigma_2}/s_a s_b, & \text{otherwise} \end{cases} \\
&\quad= P_{\sigma_1,\sigma_2}.
\end{aligned}$$

Besides, we have

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

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. 3 satisfies

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

□

C.5.10 PROOF OF LEMMA C.11

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

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

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

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

Similarly, we can get that

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

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

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

□

D 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 1-dimensional Gaussian and multivariate Gaussian with dimensionally independent variables, and analyze the performance of Algs. 1 and 2.

D.1 INTERSECTION PRIVACY

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

Proposition D.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 $\Pi_{\epsilon,\omega_\Theta} \leq T$,*

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

The proof is shown in App. D.1.1. We then analyze the performance of Alg. 2 under intersection privacy as follows.

Proposition D.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. 2 has*

$$\Pi_{\epsilon,\omega_\Theta} = \prod_{i\in[d]} \frac{2\epsilon_i}{s_{g_i}},$$
$$\Delta = \frac{1}{2}\sqrt{\sum_{i\in[d]} {s_{g_i}}^2} < c_{\epsilon,s} \cdot \Delta_{opt}.$$

where $c_{\epsilon,s}$ is a constant depending on tolerance ranges and the interval lengths of the mechanism, and Δ_{opt} is the optimal achievable distortion under the privacy achieved by Alg. 2.

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

For the 1-dimensional Gaussian scenario, with similar analysis, we can easily get that the privacy-distortion lower bound and the performance of Alg. 1 are consistent with the results presented in Prop. D.1 and Prop. D.2 (with $d = 2$).

D.1.1 Proof of Prop. D.1

Define $\theta' = (\mu'_1, \cdots, \mu'_k, \sigma'_1, \cdots, \sigma'_k)$. Based on Lemma C.7, 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

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

Based on Thm. 5.1, we can get that

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

D.1.2 PROOF OF PROP. D.2

Proof. Based on Lemma C.7, we can easily can get that the distortion Δ of Alg. 2 is

$$\Delta = \frac{1}{2}\sqrt{\sum_{i\in[d]} {s_{g_i}}^2}.$$

Since the secret distribution parameters are independent of each other and follow the uniform distributions, we can get that the privacy of Alg. 2 is

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

From Prop. D.1, we know that the optimal achievable distortion Δ_{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

$$\begin{aligned}k &< \frac{\sqrt{\sum_{i\in[d]} {s_{g_i}}^2}}{\sqrt{d}\cdot\left(\prod_{i\in[d]} s_{g_i}\right)^{1/d} - \frac{2}{\sqrt{d}}\sum_{i\in[d]}\epsilon_i} \\ &= \frac{\sqrt{\sum_{i\in[d]}\left(\frac{\epsilon_i}{x_i}\right)^2}}{\sqrt{d}\cdot\left(\prod_{i\in[d]}\frac{\epsilon_i}{x_i}\right)^{1/d} - \frac{2}{\sqrt{d}}\sum_{i\in[d]}\epsilon_i} \\ &\le \frac{c_2\sqrt{\sum_{i\in[d]}\epsilon_i^2}}{c_1\sqrt{d}\cdot\left(\prod_{i\in[d]}\epsilon_i\right)^{1/d} - \frac{2c_1c_2}{\sqrt{d}}\sum_{i\in[d]}\epsilon_i} \\ &= \frac{c_2\sqrt{\sum_{i\in[d]}\epsilon_i^2/d}}{c_1\left(\prod_{i\in[d]}\epsilon_i\right)^{1/d} - 2c_1c_2\sum_{i\in[d]}\epsilon_i/d} \\ &\triangleq c_{\epsilon,s}.\end{aligned}$$

Therefore, we can get that

$$\Delta = k\Delta_{opt} < c_{\epsilon,s}\Delta_{opt},$$

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 $\frac{\epsilon_1}{s_{g_1}} = \cdots = \frac{\epsilon_g}{s_{g_d}} \le \frac{1}{4}$, we can get that $\Delta < 2\Delta_{opt}$. □

D.2 GROUP SECRETS PRIVACY

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

Proposition D.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 $\Pi_{\epsilon,\omega_\Theta} \leq T$,*

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

The proof is shown in App. D.2.1. We then analyze the performance of Alg. 2 under group secrets privacy as follows.

Proposition D.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. 2 has*

$$\Pi_{\epsilon,\omega_\Theta} = 1 - \prod_{b\in\mathcal{B}} \left(1 - \prod_{i\in\mathcal{I}_b} \frac{2\epsilon_i}{s_{g_i}}\right),$$
$$\Delta = \frac{1}{2}\sqrt{\sum_{i\in[d]} {s_{g_i}}^2} < c_{\epsilon,s,\mathcal{B}} \cdot \Delta_{opt}.$$

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 $\mathcal{B}$. Δ_{opt} is the optimal achievable distortion under the privacy achieved by Alg. 2.

The proof is shown in App. D.2.2. From Prop. D.4 we know that Alg. 2 is order-optimal with a constant multiplication factor.

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

D.2.1 PROOF OF PROP. D.3

Define $\theta' = (\mu'_1, \cdots, \mu'_k, \sigma'_1, \cdots, \sigma'_k)$. Based on Lemma C.7, we can get that

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

Therefore, we have

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

Based on Thm. 5.3, we can get that

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

D.2.2 Proof of Prop. D.4

Proof. Based on Lemma C.7, we can easily can get that the distortion Δ of Alg. 2 is

$$\Delta = \frac{1}{2}\sqrt{\sum_{i\in[d]} {s_{g_i}}^2}.$$

Since the secret distribution parameters are independent of each other and follow the uniform distributions, we can get that the privacy of Alg. 2 is

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

From Prop. D.3, we know that the optimal achievable distortion Δ_{opt} satisfy

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

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

$$\begin{aligned}
k &< \frac{\sqrt{\sum_{i\in[d]}\left(\frac{\epsilon_i}{x_i}\right)^2}}{2\sqrt{d}\left\lceil \frac{1}{\left(1-\left[\prod_{b\in\mathcal{B}}\left(1-\prod_{i\in\mathcal{I}_b}2x_i\right)\right]^{1/\beta}\right)^{\beta/d}} \right\rceil \left(\prod_{i\in[d]}\epsilon_i\right)^{1/d} - \frac{2}{\sqrt{d}}\sum_{i\in[d]}\epsilon_i} \\
&\le \frac{\sqrt{\sum_{i\in[d]}\epsilon_i^2}}{2c_1\sqrt{d}\cdot\frac{1}{\left(1-\left[\prod_{b\in\mathcal{B}}\left(1-(2c_2)^{|b|}\right)\right]^{1/\beta}\right)^{\beta/d}}\cdot\left(\prod_{i\in[d]}\epsilon_i\right)^{1/d} - \frac{2c_1}{\sqrt{d}}\sum_{i\in[d]}\epsilon_i} \\
&= \frac{\sqrt{\sum_{i\in[d]}\epsilon_i^2/d}}{\frac{2c_1}{\left(1-\left[\prod_{b\in\mathcal{B}}\left(1-(2c_2)^{|b|}\right)\right]^{1/\beta}\right)^{\beta/d}}\left(\prod_{i\in[d]}\epsilon_i\right)^{1/d} - 2c_1\sum_{i\in[d]}\epsilon_i/d} \\
&\triangleq c_{\epsilon,s,\mathcal{B}}.
\end{aligned}$$

Therefore, we can get that

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

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 $\Delta < 2\Delta_{opt}$ 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 $\frac{\epsilon_1}{s_{g_1}} = \cdots = \frac{\epsilon_g}{s_{g_d}} \leq \frac{1}{4}$. □

D.3 l_p NORM PRIVACY

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

Proposition D.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 $\Pi_{\epsilon,\omega_\Theta} \leq T$,*

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

The proof is shown in App. D.3.1. We then analyze the performance of Alg. 2 under l_p norm privacy as follows.

Proposition D.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. 2 has*

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

The proof is shown in App. D.3.2. From Prop. D.6 we know that Alg. 2 is order-optimal with a constant multiplication factor.

For the 1-dimensional Gaussian scenario, with similar analysis, we can easily get that the privacy-distortion lower bound and the performance of Alg. 1 are consistent with the results presented in Prop. D.5 and Prop. D.6 (with $d = 2$).

D.3.1 PROOF OF PROP. D.5

Define $\theta' = (\mu'_1, \cdots, \mu'_k, \sigma'_1, \cdots, \sigma'_k)$. Based on Lemma C.7, 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

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

Based on Thm. 5.4, we can get that

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

D.3.2 Proof of Prop. D.6

Proof. Based on Lemma C.7, we can easily can get that the distortion Δ of Alg. 2 is

$$\Delta = \frac{1}{2} \sqrt{\sum_{i \in [d]} {s_{g_i}}^2}.$$

We denote $\Pi^{\text{uni}}_{\epsilon,\omega_\Theta}$ as the union privacy metric with tolerance ranges $\epsilon_1, \cdots, \epsilon_d$. From App. B.7.1, we know that $\Pi_{\epsilon,\omega_\Theta} \leq \Pi^{\text{uni}}_{\epsilon,\omega_\Theta}$ when $\left(\sum_{i\in[d]} \epsilon_i^p\right)^{1/p} = \varepsilon_p$. Therefore, we can get that

$$\begin{aligned} \Pi_{\epsilon,\omega_\Theta} &\leq \min_{\substack{\epsilon_1,\cdots,\epsilon_d: \\ \left(\sum_{i\in[d]} \epsilon_i^p\right)^{1/p} = \varepsilon_p}} \Pi^{\text{uni}}_{\epsilon,\omega_\Theta} \\ &= \min_{\substack{\epsilon_1,\cdots,\epsilon_d: \\ \left(\sum_{i\in[d]} \epsilon_i^p\right)^{1/p} = \varepsilon_p}} 1 - \prod_{i\in[d]} \left(1 - \frac{2\epsilon_i}{s_{g_i}}\right). \end{aligned}$$

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

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

□