Differentially Private Conditional Independence Testing

Iden Kalemaj[*]
Boston Unviersity
ikalemaj@bu.edu

Shiva Prasad Kasiviswanathan
Amazon
kasivisw@gmail.com

Aaditya Ramdas
Carnegie Mellon University
aramdas@cmu.edu

Abstract

Conditional independence (CI) tests are widely used in statistical data analysis, e.g., they are the building block of many algorithms for causal graph discovery. The goal of a CI test is to accept or reject the null hypothesis that $X \perp\!\!\!\perp Y \mid Z$, where $X \in \mathbb{R}, Y \in \mathbb{R}, Z \in \mathbb{R}^d$. In this work, we investigate conditional independence testing under the constraint of differential privacy. We design two private CI testing procedures: one based on the generalized covariance measure of Shah and Peters (2020) and another based on the conditional randomization test of Candès et al. (2016) (under the model-X assumption). We provide theoretical guarantees on the performance of our tests and validate them empirically. These are the first private CI tests that work for the general case when Z is continuous.

1 Introduction

Conditional independence (CI) tests are a powerful tool in statistical data analysis, e.g., they are building blocks for graphical models, causal inference, and causal graph discovery Dawid [1979], Koller and Friedman [2009], Pearl [2000]. These analyses are frequently performed on sensitive data, such as clinical datasets and demographic datasets, where concerns for privacy are foremost. For example, in clinical trials, CI tests are used to answer fundamental questions such as "After accounting for (conditioning on) a set of patient covariates Z (e.g., age or gender), does a treatment X lead to better patient outcomes Y?". Formally, given three random variables (X, Y, Z) where $X \in \mathbb{R}$, $Y \in \mathbb{R}$, and $Z \in \mathbb{R}^d$, denote the conditional independence of X and Y given Z by $X \perp\!\!\!\perp Y \mid Z$. Our problem is that of testing

$$H_0 \text{ (null)} : X \perp\!\!\!\perp Y \mid Z \text{ vs. } H_1 \text{ (alternate) } : X \not\perp\!\!\!\perp Y \mid Z$$

given data drawn i.i.d. from a joint distribution of (X, Y, Z). CI testing is a much harder problem than (unconditional) independence testing, where the variable Z is omitted. Indeed, Shah and Peters [2020] showed that CI testing is a statistically impossible task for continuous random variables.[1] Thus, techniques for independence testing do not directly extend to the CI testing problem.

When the underlying data is sensitive and confidential, publishing statistics (such as the value of a CI independence test statistic or the corresponding p-value) can leak private information about individuals in the data. For instance, Genome-Wide Association Studies (GWAS) involve finding (causal) relations between Single Nucleotide Polymorphisms (SNPs) and diseases. CI tests are building blocks for establishing these relations, and the existence of a link between a specific SNP and a rare disease may indicate the presence of a minority patient. *Differential privacy* Dwork et al. [2016] is a widely studied and deployed formal privacy guarantee for data analysis. The output distributions of a differentially private algorithm must look nearly indistinguishable for any two input datasets that differ only in the data of a single individual. In this work, we design the first differentially private (DP) CI tests that can handle continuous variables $X \in \mathbb{R}, Y \in \mathbb{R}, Z \in \mathbb{R}^d$.

Our Contributions. We design two private CI tests, each based on a different set of assumptions about the data-generating distribution. They are the *first* private CI tests with rigorous type-I error and power guarantees. Given the aforementioned impossibility results for non-private CI testing, to obtain a CI test with meaningful theoretical guarantees, some assumptions are necessary; in particular we must restrict the space of possible null distributions. In

[*]This work was conducted during an internship at Amazon.

[1]Any test that uniformly controls the type-I error (false positive rate) for all absolutely continuous triplets (X, Y, Z) such that $X \perp\!\!\!\perp Y \mid Z$, even asymptotically, does not have nontrivial power against *any* alternative.

designing our private tests, we start with non-private CI tests that provide rigorous guarantees on type-I error control. In Appendix A.1 we discuss other non-private CI tests that provide weaker guarantees.

Our first test (Section 2) is a private version of the generalized covariance measure (GCM) by Shah and Peters [2020]. The type-I error guarantees of the GCM rely on the fairly weak assumption that the conditional means $\mathbb{E}[X \mid Z]$ and $\mathbb{E}[Y \mid Z]$ can be estimated sufficiently well given the dataset size. The test statistic of the GCM is a normalized sum of the product of the residuals of (nonlinearly) regressing X on Z and Y on Z. This test statistic has *unbounded* sensitivity, thus a more careful way of adding and analyzing the impact of the privacy noise is needed. Our private GCM test adds appropriately scaled, zero-mean noise to the residual products, and calculates the same statistic on the noisy residual products. We show that even with the added noise, the GCM score converges asymptotically to a standard Gaussian distribution under the null hypothesis. The magnitude of the noise added to the residuals is constant (it does not vanish with increasing sample size n), thus showing asymptotic convergence results in the presence of such noise is nontrivial. Even more care is needed to show our stronger *uniform* convergence results, to bound how the noise variables interact with the noise from the estimation of the residuals. Our asymptotic guarantees imply that our test achieves the same power as the non-private GCM test with a $O(1/\varepsilon^2)$-factor of the dataset size. Recall, as mentioned earlier, that finite sample guarantees on type-I error and power are impossible even for the task of non-private CI testing Shah and Peters [2020]. In addition, the privacy-preserving noise added to our GCM test offers an extra advantage: it can maintain type-I error control even when the non-private GCM test fails to do so. This occurs in scenarios where the regression methods used to estimate the conditional means either underfit or overfit. Thus, the noise added for privacy purposes can provide benefits beyond safeguarding data confidentiality during analysis.

Our second test (Section 3) relies on the *model-X assumption* that the conditional distribution of $X \mid Z$ is known or can be well-approximated. Recently introduced by Candès et al. [2016], this assumption is useful in settings where one has access to abundant unlabeled data, such as in GWAS, but labeled data are scarce. The model-X assumption is also satisfied in experimental settings where a randomization mechanism is known or designed by the experimenter. CI tests utilizing this assumption provide exact, non-asymptotic, type-I error control [Candès et al., 2016, Berrett et al., 2019], thus bypassing the hardness result of Shah and Peters [2020]. While this assumption has spurred a lot of recent research in (non-private) CI testing, there are no prior private tests in the literature that are designed to work under this assumption. In this work, we focus on the conditional randomization test (CRT) [Candès et al., 2016]. We design a private CRT and provide theoretical guarantees on the accuracy of its p-value. We adopt a popular framework for obtaining DP algorithms, known as Report Noisy Max (or the exponential mechanism), which requires defining a problem-specific score function of low sensitivity. The score function we design is novel and can be used for solving a more general problem: given a set of queries on a dataset, estimate privately the rank of a particular query amongst the rest of the queries. To obtain good utility, our score function exploits the specific distribution of intermediate statistics calculated by the CRT.

We present a detailed empirical evaluation of the proposed tests, justifying their practicality across a wide range of settings. Our experiments confirm that our private CI tests provide the critical type-I error control, and can in fact do so more reliably than their non-private counterparts. As expected, our private tests achieve lower power due to the noise injected for privacy, which can be compensated for with a larger dataset size.

1.1 Related Work

Private Conditional Independence Testing. Wang et al. [2020] is the only work, prior to ours, to explicitly study private CI testing, motivated by an application to causal discovery. Their tests (obtained from Kendall's τ and Spearman's ρ score) are designed for categorical Z. While these tests could be adapted to work for continuous Z via binning or clustering, in practice this method does not seem to control type-I error, as we show in our experiments (Fig. 1). The problem worsens with higher-dimensional Z. Additionally, while Wang et al. [2020] bound the excess type-I and type-II error introduced by the privacy noise, there are no results on the type-I error and power of the tests overall, which we provide for our private GCM test. Our techniques also differ from those of Wang et al. [2020], who obtain their tests by bounding the sensitivity of non-private CI scores and adding appropriately scaled noise to the true value of the score. They state two open problems: obtaining private CI tests for continuous Z and obtaining private tests from scores of unbounded sensitivity (as is the case with the GCM score). We solve both open problems, and manage to privatize the GCM score by instead adding noise to an intermediate statistic, the residuals of fitting X to Z and Y to Z.

Another line of work Smith [2011], Kazan et al. [2023], Peña and Barrientos [2023] has utilized the "subsample and aggregate" framework of differential privacy Nissim et al. [2007] to obtain private versions of existing hypothesis tests in a black-box fashion. In this approach, the dataset is partitioned into k smaller equally-sized datasets; the non-private hypothesis test is evaluated on the smaller datasets; and finally, the results are privately aggregated. Smith [2011] analyzed the asymptotic properties of this strategy and showed that for a large family of statistics, one can obtain a corresponding DP statistic with the same asymptotic distribution as the original statistic. In particular, one could apply the result of Smith [2011] to obtain a DP version of the GCM statistic. However, compared to our results on the private GCM, (a) an additional assumption on bounded third moments of the GCM statistic is required to obtain the desired asymptotic convergence, (b) only a weaker notion of privacy, known as *approximate* DP, would be guaranteed, and (c) it is not clear how to obtain a trade-off between the power of the private test and its non-private counterpart in terms of the input parameters. Kazan et al. [2023] propose a test-of-tests (ToT) framework for constructing a private version of any known (non-private) hypothesis test and show guarantees on the power of their test based on finite-sample guarantees of the power of the non-private hypothesis test. Since finite-sample guarantees are impossible for the task of CI testing (Shah and Peters [2020]), their results do not apply for our particular task. We emphasize that while our asymptotics justify the threshold for rejecting the null, our private GCM test controls type-I error very well at finite n, as we demonstrate in experiments. In Fig. 1 we compare the type-I error control of our tests with the ToT framework. Finally, the test of Peña and Barrientos [2023] only outputs a binary accept/reject decision and not a p-value as our tests provide, and was empirically outperformed by the test of Kazan et al. [2023].

Private (non-conditional) Independence Testing. A line of work on private independence testing has focused on privatizing the chi-squared statistic Vu and Slavkovic [2009], Johnson and Shmatikov [2013], Uhler et al. [2013], Yu et al. [2014], Wang et al. [2015], Gaboardi et al. [2016], Rogers and Kifer [2017]. These tests operate with categorical X and Y. Earlier works obtained private hypothesis tests by adding noise to the histogram of the data Johnson and Shmatikov [2013], but it was later pointed out that this approach does not provide reliable type-I error control at small sample sizes Fienberg et al. [2010]. Motivated by this issue, later works use numerical approaches to obtain the distribution of the noisy statistic and calculate p-values with that distribution Uhler et al. [2013], Yu et al. [2014], Wang et al. [2015], Gaboardi et al. [2016], whereas Rogers and Kifer [2017] obtain new statistics for chi-squared tests whose distribution after the privacy noise can be derived analytically. In this light, one important feature of our private GCM test is that its type-I error control can be more reliable than for the non-private GCM, even at small n, as our experiments demonstrate. For continuous X and Y, Kusner et al. [2016] obtained DP versions of several dependence scores (Kendall's τ, Spearman's ρ, HSIC), however, they do not provide type-I error or power guarantees. Note that CI testing is a much harder task than independence testing, and techniques for the latter do not necessarily translate to CI testing. Our work is part of the broader literature on private hypothesis testing Barrientos et al. [2017], Campbell et al. [2018], Swanberg et al. [2019], Couch et al. [2019], Wang et al. [2018], Awan and Slavkovic [2018], Brenner and Nissim [2014], Ding et al. [2021], Vepakomma et al. [2022].

1.2 Preliminaries

Notation. If $(V_{P,n})_{n\in\mathbb{N},P\in\mathcal{P}}$ is a family of sequences of random variables whose distributions are determined by $P \in \mathcal{P}$, we say $V_{P,n} = o_{\mathcal{P}}(1)$ if for all $\delta > 0$, $\sup_{P\in\mathcal{P}} \Pr_P[|V_{P,n}| > \delta] \to 0$. Similarly, $V_{P,n} = O_{\mathcal{P}}(1)$ if for all $\delta > 0$, $\exists M > 0$ such that $\sup_{n\in\mathbb{N}} \sup_{P\in\mathcal{P}} \Pr_P[|V_{P,n}| > M] < \delta$.

The notion of neighboring datasets is central to differential privacy. In this work, we consider datasets $\mathbf{D} = (\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ of n datapoints $\{(x_i, y_i, z_i)\}_{i=1}^n$, drawn i.i.d. from a joint distribution P on some domain $\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$. Let $\mathcal{D}$ denote the universe of datasets. A dataset $\mathbf{D'} \in \mathcal{D}$ is a neighbor of $\mathbf{D}$ if it can be obtained from $\mathbf{D}$ by replacing at most one datapoint $(x_i, y_i, z_i) \in \mathbf{D}$ with an arbitrary entry $(x'_i, y'_i, z'_i) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$, for some $i \in [n]$.

Definition 1.1 (Dwork et al. [2016]). A randomized algorithm Alg is ε-DP if for all neighboring datasets $\mathbf{D}, \mathbf{D'}$ and all events $\mathcal{R}$ in the output space of Alg, it holds $\Pr[\mathrm{Alg}(\mathbf{D}) \in \mathcal{R}] \le \exp(\varepsilon) \cdot \Pr[\mathrm{Alg}(\mathbf{D'}) \in \mathcal{R}]$, where the probability is over the randomness of the algorithm.

We provide additional background on differential privacy in Appendix A.2. In our algorithms and experiments, we use kernel ridge regression (KRR) as a procedure for regressing $\mathbf{X}$ and $\mathbf{Y}$ on $\mathbf{Z}$, and rely on the following result by Kusner et al. [2016] about the sensitivity of the residuals of KRR.[2]

Theorem 1.2 (Restated Theorem 5 of Kusner et al. [2016]). *Let $(\mathbf{U}, \mathbf{V})$ be a dataset of n datapoints (u_i, v_i), $i \in [n]$ from the domain $\mathcal{U} \times \mathcal{V} \subset \mathbb{R} \times \mathbb{R}^d$. Suppose that $|\mathcal{U}| \le 1$. Given a Hilbert space $\mathcal{H}$, let $\mathbf{w}$ be the vector that minimizes the kernel ridge regression objective $(\lambda/2)\|\mathbf{w}\|_{\mathcal{H}}^2 + (1/n)\sum_{i=1}^n (u_i - \mathbf{w}^\top \phi(v_i))^2$, for kernel $\phi\colon \mathbb{R}^d \to \mathcal{H}$ with $\|\phi(v)\|_{\mathcal{H}} \le 1$*

[2] One could also use other regression techniques within our private GCM and private CRT frameworks, and theoretical guarantees continue to hold if similar ($\approx O(1/n)$) bounds on the sensitivity of the residuals are true.

for all $v \in \mathcal{V}$. Define $\mathbf{w}'$ analogously for a neighboring dataset $(\mathbf{U}', \mathbf{V}')$ that is obtained by replacing one datapoint in $(\mathbf{U}, \mathbf{V})$. Then $\|\mathbf{w}\|_{\mathcal{H}} \leq \sqrt{2/\lambda}$ and for all $v \in \mathbf{V}$ it holds: $|\mathbf{w}^\top \phi(v) - \mathbf{w}'^\top \phi(v)| \leq 8\sqrt{2}/(\lambda^{3/2} n) + 8/(\lambda n)$.

2 Private Generalized Covariance Measure

In this section, we propose our private GCM test. Missing proofs are collected in Appendix B.

GCM Test. We first describe the non-private GCM test of Shah and Peters [2020]. Given a joint distribution P of the random variables (X, Y, Z), the GCM tests the implications of *weak conditional independence*.[3] For the variables X and Y we can always write:

$$X = f_P(Z) + \chi_P, \quad Y = g_P(Z) + \xi_P,$$

where $f_P(z) = \mathbb{E}_P[X|Z = z]$, $g_P(z) = \mathbb{E}_P[Y|Z = z]$, $\chi_P = X - f_P(z)$, and $\xi_P = Y - g_P(z)$.

Let $\mathbf{D} = (\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ be a dataset of n i.i.d. samples from P. Let $\hat{f}$ and $\hat{g}$ be approximations to the conditional expectations f_P and g_P, obtained by fitting $\mathbf{X}$ to $\mathbf{Z}$ and $\mathbf{Y}$ to $\mathbf{Z}$, respectively. We consider the products of the residuals from the fitting procedure:

$$R_i = ((x_i - \hat{f}(z_i))(y_i - \hat{g}(z_i)) \text{ for } i \in [n]. \tag{1}$$

The GCM test statistic T is defined as the normalized mean of the residual products, i.e.,

$$T(R_1, \ldots, R_n) = \frac{\frac{1}{\sqrt{n}} \sum_{i=1}^n R_i}{(\frac{1}{n} \sum_{i=1}^n R_i^2 - (\frac{1}{n} \sum_{k=1}^n R_k)^2)^{1/2}}. \tag{2}$$

The normalization plays a critical role in ensuring that the asymptotic distribution of T follows a standard normal distribution. However, it also leads to the unbounded sensitivity of the statistic T.

Private GCM Test. To construct a DP version of the GCM test, we focus on the vector of residual products, $\mathbf{R} = (R_1, \ldots, R_n)$. Let Δ denote the ℓ_1-sensitivity of $\mathbf{R}$. Given Δ, we use the Laplace mechanism (Lemma A.2) to add scaled Laplace noise to $\mathbf{R}$ and then compute T on the noisy residual products. The private GCM test we present (in Algorithm 1) can be used with any fitting procedure, as long as a bound on the sensitivity of the residuals for that procedure is known.

Algorithm 1 Private Generalized Covariance Measure

1: **Input:** Dataset $(\mathbf{X}, \mathbf{Y}, \mathbf{Z}) = \{(x_i, y_i, z_i)\}_{i=1}^n$, privacy parameter $\varepsilon > 0$, fitting procedure $\mathcal{F}$, bound $\Delta > 0$ on the sensitivity of residual products of $\mathcal{F}$.
2: Let $\hat{f} = \mathcal{F}(\mathbf{Z}, \mathbf{X})$ and $\hat{g} = \mathcal{F}(\mathbf{Z}, \mathbf{Y})$ $\;i = 1, \ldots, n$
3: $r_{X,i} \leftarrow x_i - \hat{f}(z_i)$, $r_{Y,i} \leftarrow y_i - \hat{g}(z_i)$
4: $R_i \leftarrow r_{X,i} \cdot r_{Y,i}$
5: $W_i \sim \text{Lap}(0, \Delta/\varepsilon)$
6: Calculate $T^{(n)} \leftarrow T(R_1 + W_1, \ldots, R_n + W_n)$ {see (2)}
7: Output p-value $= 2 \cdot (1 - \Phi(|T^{(n)}|)$

We now focus on the guarantees of this private CI test. Firstly, we show that as with the GCM test of Shah and Peters [2020], the private counterpart has uniformly asymptotic level.[4]

We start with some definitions. Let $\mathcal{E}_0$ be the set of distributions for (X, Y, Z) that are absolutely continuous with respect to the Lebesgue measure. Define $\mathcal{P}_0 \subset \mathcal{E}_0$ as the subset of distributions for which $X \perp\!\!\!\perp Y \mid Z$. Given $P \in \mathcal{P}$, let P' be the joint distribution of variables (X, Y, Z, W) where $W \sim \text{Lap}(\Delta/\varepsilon)$ is independent of (X, Y, Z). For a set of distributions $\mathcal{P}$, let $\mathcal{P}'$ denote the set of distributions P' for all $P \in \mathcal{P}$. Denote by Φ the CDF of the standard normal

[3] It states that for all relationships where $X \perp\!\!\!\perp Y \mid Z$ then $\text{cov}(X, Y \mid Z) = 0$. This implication does not hold in the reverse direction, i.e., there are always alternatives where $\text{cov}(X, Y \mid Z) = 0$ and $X \not\perp\!\!\!\perp Y \mid Z$.

[4] Given a level $\alpha \in (0, 1)$ and null hypothesis $\mathcal{P}_0$, a test ψ_n has uniformly asymptotic level if its asymptotic type-I error is bounded by α over all distributions in $\mathcal{P}_0$, i.e., $\lim_{n\to\infty} \sup_{P \in \mathcal{P}_0} \Pr_P[\psi_n \text{ rejects null}] \leq \alpha$.

distribution. Consider $u_P(z) = \mathbb{E}_P[\chi_P^2 \mid Z = z]$, $v_P(z) = \mathbb{E}_P[\xi_P^2 \mid Z = z]$, and the following error quantities:

$$A_f = \frac{1}{n}\sum_{i=1}^{n}(f_P(z_i) - \hat{f}(z_i))^2, \qquad B_f = \frac{1}{n}\sum_{i=1}^{n}(f_P(z_i) - \hat{f}(z_i))^2 v_P(z_i),$$
$$A_g = \frac{1}{n}\sum_{i=1}^{n}(g_P(z_i) - \hat{g}(z_i))^2, \qquad B_g = \frac{1}{n}\sum_{i=1}^{n}(g_P(z_i) - \hat{g}(z_i))^2 u_P(z_i). \tag{3}$$

Type-I Error Control. In Theorem 2.1, we establish assumptions on the error terms defined above, under which $T^{(n)}$ from Algorithm 1 converges uniformly to the standard normal distribution. While the original GCM test of Shah and Peters [2020] does not require the input variables to be bounded, we assume bounded random variables X and Y to obtain bounds on the sensitivity Δ of the residual products. For the rest of this section, we assume publicly known bounds a and b on the domain $\mathcal{X}$ of X and $\mathcal{Y}$ of Y, (i.e., $|x| \le a, \forall x \in \mathcal{X}$ and $|y| \le b, \forall y \in \mathcal{Y}$).[5] Note that we do not assume such bounds on the domain of Z, which is important as Z could be high-dimensional.

Theorem 2.1. (Type-I Error Control of Private GCM) *Let a and b be known bounds on the domains of X and Y, respectively. Given a dataset $\mathbf{D} = (\mathbf{X}, \mathbf{Y}, \mathbf{Z})$, let $(\hat{\mathbf{X}}, \hat{\mathbf{Y}}, \mathbf{Z})$ be the rescaled dataset obtained by setting $\hat{\mathbf{X}} = \mathbf{X}/a$ and $\hat{\mathbf{Y}} = \mathbf{Y}/b$. Consider $R_i, i \in [n]$, as defined in (1), for the rescaled dataset $(\hat{\mathbf{X}}, \hat{\mathbf{Y}}, \mathbf{Z})$. Let $W_i \sim \mathrm{Lap}(0, \Delta/\varepsilon)$ for $i \in [n]$, where $\Delta, \varepsilon > 0$ are constants. Then $T^{(n)} = T(R_1 + W_1, \ldots, R_n + W_n)$, defined in Algorithm 1, satisfies:*

1. *For $P \in \mathcal{P}_0$ such that $A_f A_g = o_P(n^{-1}), B_f = o_P(1), B_g = o_P(1)$, and $\mathbb{E}[\chi_P^2 \xi_P^2] < \infty$, then*
$$\lim_{n\to\infty} \sup_{t\in\mathbb{R}} |\Pr_{P'}[T^{(n)} \le t] - \Phi(t)| = 0.$$
2. *Let $\mathcal{P} \subset \mathcal{P}_0$ be a set of distributions such that $A_f A_g = o_{\mathcal{P}}(n^{-1}), B_f = o_{\mathcal{P}}(1)$ and $B_g = o_{\mathcal{P}}(1)$. If in addition $\sup_{P\in\mathcal{P}} \mathbb{E}[|\chi_P \xi_P|^{2+\eta}] \le c$, for some constants $c, \eta > 0$, then*
$$\lim_{n\to\infty} \sup_{P'\in\mathcal{P}'} \sup_{t\in\mathbb{R}} |\Pr_{P'}[T^{(n)} \le t] - \Phi(t)| = 0. \tag{4}$$

Theorem 2.1 implies that the CI test in Algorithm 1 has uniformly asymptotic level. It also satisfies a weaker pointwise asymptotic level guarantee that holds under slightly weaker assumptions (see Theorem 2.1). Note that this always holds, independent of the bound on $|X|$ and $|Y|$. The assumptions in Theorem 2.1 are similar to those of Shah and Peters [2020] for guaranteeing uniformly asymptotic level of the GCM. The only difference is that we do not require a lower bound on the variance $\mathbb{E}[\chi_P^2 \xi_P^2]$ of the true residuals. This requirement is no longer necessary as we add finite-variance noise to the residual products.

Noise Addition Leads to Better Type-I Error Control. A beneficial consequence of the privacy noise is that there are scenarios, under the null hypothesis, where the non-private GCM fails to provide type-I error control, but our private GCM does. If the functions $\hat{f}$ and $\hat{g}$ fail to fit the data (i.e., the conditions on A_f, A_g, B_f, B_g in Theorem 2.1 are violated), private GCM can still provide type-I error control. We show in Section 4 one such scenario, when the learned model underfits the data. Consider on the other hand the case when the model overfits, and more extremely, when the model interpolates asymptotically, i.e. $\hat{f}(z_i) \to x_i$ and $\hat{g}(z_i) \to y_i$ as $n \to \infty$ for all $i \in [n]$ Liang and Rakhlin [2020]. It is not too hard to show that (4) still holds for the private GCM, and thus type-I error control is provided. Instead, the rejection rate of the non-private GCM converges to 1 when the model interpolates.

Power of the Private GCM. Next, we show a result on the power of our private GCM test. Following Shah and Peters [2020], to facilitate the theoretical analysis of power, we separate the model fitting step from the calculation of the residuals. We calculate $\hat{f}$ and $\hat{g}$ on the first half of the dataset and calculate the residuals $R_i, i \in [n]$ on the second half.

Theorem 2.2. (Power of Private GCM). *Consider the setup of Theorem 2.1. Let A_f, A_g, B_f, B_g be as defined in (3), with the difference that $\hat{f}$ and $\hat{g}$ are estimated on the first half of the dataset $(\hat{\mathbf{X}}, \hat{\mathbf{Y}}, \mathbf{Z})$, and $R_i, i \in [n/2, n]$ are calculated on the second half. Define the "signal" (ρ_P) and "noise" (σ_P) of the true residuals χ_P, ξ_P as:*

$$\rho_P = \mathbb{E}_P[\mathrm{cov}(X, Y \mid Z)], \sigma_P = \sqrt{\mathrm{Var}_P(\chi_P \xi_P)}.$$

[5]These bounds can also be replaced with high probability bounds, but the privacy guarantees of our CI test would be replaced with what is known as *approximate differential privacy*.

1. *If for $P \in \mathcal{E}_0$ we have $A_f A_g = o_P(n^{-1}), B_f = o_P(1), B_g = o_P(1)$ and $\sigma_P < \infty$, then*

$$\lim_{n\to\infty} \sup_{t\in\mathbb{R}} \Big| \Pr_{P'} \Big[T^{(n)} - \frac{\sqrt{n}\rho_P}{\sigma'_P} \le t \Big] - \Phi(t) \Big| = 0, \text{ where } \sigma'_P = \sqrt{\sigma_P^2 + (\frac{\sqrt{2}ab\Delta}{\varepsilon})^2}. \tag{5}$$

2. *Let $\mathcal{P} \subset \mathcal{E}_0$ such that $A_f A_g = o_{\mathcal{P}}(n^{-1}), B_f = o_{\mathcal{P}}(1)$ and $B_g = o_{\mathcal{P}}(1)$. If in addition $\sup_{P\in\mathcal{P}} \mathbb{E}[|\chi_P \xi_P|^{2+\eta}] \le c$, for some constants $c, \eta > 0$, then (5) holds over $\mathcal{P}'$ uniformly.*

Discussion on Power. Theorem 2.2 implies that $T^{(n)}$ has uniform (asymptotic) power of 1 if $\rho_P \neq 0$. See Corollary B.3 for a short proof. In Theorem 2.2, we also show a pointwise (asymptotic) power guarantee, under weaker assumptions. We remark that the bounds a and b on $|X|$ and $|Y|$ could depend on the dataset size n. Algorithm 1 has uniform asymptotic power of 1 as long as $a \cdot b = o(\sqrt{n})$.

Shah and Peters [2020] show a similar result on the power of the (non-private) GCM, but with $\sigma'_P = \sigma_P$. Suppose $\sigma_P = 1$. Then, Theorem 2.2 states that a $(\frac{ab\Delta}{\varepsilon})^2$-factor of the dataset size used in the non-private case is required to obtain the same power in the private case. A blow-up in the sample size is typical in DP analyses [Dwork and Roth, 2014]. On the other hand, we do not require a lower bound on the variance $\mathbb{E}[\chi_P^2 \xi_P^2]$ of the true residuals, but Shah and Peters [2020] do.

Private GCM with Kernel Ridge Regression (PrivGCM). To obtain a bound on the sensitivity of the vector of residual products, we use kernel ridge regression (KRR) as the model for regressing X on Z and Y on Z, respectively. Let PrivGCM denote Algorithm 1 with KRR as the fitting procedure and the bound on Δ.

The vector of residual products has ℓ_1-sensitivity $O_\lambda(1)$ as formally shown in Lemma 2.3 using Theorem 1.2.

Lemma 2.3. (Sensitivity of residual products). *Let $\mathbf{R}$ be the vector of residual products, as defined in* (1)*, of fitting a KRR model of $\mathbf{X}$ to $\mathbf{Z}$ and $\mathbf{Y}$ to $\mathbf{Z}$ with regularization parameter $\lambda > 0$. If $|x_i|, |y_i| \le 1$ for all $i \in [n]$, then $\Delta_{\mathbf{R}} \le C$ where $C = 4(1 + \frac{\sqrt{2}}{\sqrt{\lambda}})(1 + \frac{\sqrt{2}}{\sqrt{\lambda}} + \frac{4\sqrt{2}}{\lambda^{3/2}} + \frac{4}{\lambda})$.*

Along with Lemma A.2, this implies that PrivGCM is ε-DP. In addition, as shown by Shah and Peters [2020], the requirements on A_f, A_g, B_f, B_g are satisfied when using KRR. If the additional conditions listed in Theorems 2.1 and 2.2 are also satisfied, then PrivGCM has uniformly asymptotic level and uniform asymptotic power of 1 (see Corollary B.4).

3 Private Conditional Randomized Testing

In this section, we propose a private version of the conditional randomization test (CRT), which uses access to the distribution $X \mid Z$ as a key assumption. Missing proofs can be found in Appendix C.

CRT. As before, consider a dataset $(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ of n i.i.d. samples $(x_i, y_i, z_i), i \in [n]$ from the joint distribution P. For ease of notation, denote the original $\mathbf{X}$ as $\mathbf{X}^{(0)}$. The key idea of CRT is to sample m copies of $\mathbf{X}^{(0)}$ from $X \mid Z$, where Z is fixed to the values in $\mathbf{Z}$. That is, for $j \in [m]$ and $i \in [n]$, a new datapoint $x_i^{(j)}$ is sampled from $X \mid Z = z_i$. Then $\mathbf{X}^{(j)} = (x_1^{(j)}, \dots, x_n^{(j)})$.

Under the null hypothesis, the triples $(\mathbf{X}^{(0)}, \mathbf{Y}, \mathbf{Z}), \dots, (\mathbf{X}^{(m)}, \mathbf{Y}, \mathbf{Z})$ are identically distributed. Thus, for every statistic T chosen independently of the data, the random variables $T(\mathbf{X}^{(0)}, \mathbf{Y}, \mathbf{Z}), \dots, T(\mathbf{X}^{(m)}, \mathbf{Y}, \mathbf{Z})$ are also identically distributed. Denote these random variables by $T_0, \dots, T_m$. The p-value is computed by ranking T_0, obtained by using the original $\mathbf{X}^{(0)}$ vector, against $T_1, \dots, T_m$, obtained from the resamples:

$$\text{p-value} = \frac{1 + \sum_{j=1}^m \mathbf{1}(T_j \ge T_0)}{m+1}.$$

For every choice of T, the p-value is uniformly distributed and finite-sample type-I error control is guaranteed.

Private CRT. Let $\mathbf{D} = (\mathbf{X}^{(0)}, \dots, \mathbf{X}^{(m)}, \mathbf{Y}, \mathbf{Z})$ denote the aggregated dataset. We say $\mathbf{D}'$ is a neighbor of $\mathbf{D}$ if they differ in at most one row. By defining $\mathbf{D}$ to include the resamples $\mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)}$, we also protect the privacy of the data obtained in the resampling step.

Our private CRT test is shown in Algorithm 2: it obtains a private estimate of the rank of T_0 amongst the statistics $T_1, \dots, T_m$, sorted in decreasing order. Using the Laplace mechanism to privately estimate the rank is not a viable option, since the rank has high sensitivity: changing one point in $\mathbf{D}$ could change all the values $T_0, \dots, T_m$ and change the rank of T_0 by $O(m)$. Another straightforward approach is to employ the widely used Sparse Vector Technique Dwork et al. [2009], Dwork and Roth [2014] to privately answer questions "Is $T_i > T_0$?" for all $i \in [m]$. However, this algorithm pays a privacy price for each T_i that is above the "threshold" T_0, which under the null is $\Omega(m)$, thus resulting in lower utility of the algorithm. Instead, we define a new score function and algorithm which circumvents this problem by intuitively only incurring a cost for the queries T_i that are very close to T_0 in value.

Our key algorithmic idea is to define an appropriate score function of bounded sensitivity. It assigns a score to each rank $c \in [0, m]$ that indicates how well c approximates the true rank of T_0. The score of a rank c equals the negative absolute difference between T_0 and the statistic at rank c. The true rank of T_0 has the highest score (equal to 0), whereas all other ranks have negative scores. We show that this score function has bounded sensitivity for statistics T of bounded sensitivity. The rank with the highest score is privately selected using Report Noisy Max, a popular DP selection algorithm [Dwork and Roth, 2014]. To obtain good utility, the design of the score function exploits the fact that for CRTs, the values T_i are distributed in a very controlled fashion, as explained in the remark following Theorem 3.7.

Algorithm 2 Private Conditional Randomization Test

Input: Dataset $(\mathbf{X}^{(0)}, \mathbf{Y}, \mathbf{Z})$, privacy parameter ε, bound Δ_T on the sensitivity of T, number of resamples m.
$T_0 \leftarrow T(\mathbf{X}^{(0)}, \mathbf{Y}, \mathbf{Z})$, $s_0 \leftarrow 0$. $i = 1, \dots, m$
  Sample $\mathbf{X}^{(i)} \mid \mathbf{Z}$ from $X \mid Z$.
  $T_i \leftarrow T(\mathbf{X}^{(i)}, \mathbf{Y}, \mathbf{Z})$.
Let $Q_0, \dots, Q_m$ denote the values $\{T_i\}_{i\in[0,m]}$ sorted in decreasing order. $i = 0, 1 \dots, m$
  $s_i \leftarrow -\frac{|Q_i - T_0|}{2\Delta_T}$.
$\hat{c} \leftarrow \texttt{ReportNoisyMax}(\{s_i\}_{i\in[0,m]}, \varepsilon)$. {Theorem 3.3}
Output p-value $\hat{p} = \frac{1+\hat{c}}{m+1}$.

Definition 3.1 (Score function for rank of query)**.** Let $\{T_i\}_{i\in[0,m]}$ be $m + 1$ queries of sensitivity at most Δ_T on a dataset $\mathbf{D}$. Let $Q_0, \dots, Q_m$ denote the values $\{T_i\}_{i\in[0,m]}$ sorted in decreasing order. Let $k \in [0, m]$ be the index of the query whose rank we wish to know. Then for all $c \in [0, m]$, define

$$s_k(c, \mathbf{D}) = -\frac{|Q_c - T_k|}{2\Delta_T}.$$

We bound the sensitivity of the score function in Lemma 3.2.

Lemma 3.2. (Sensitivity of the score function). *Let $\{T_i\}_{i\in[0,m]}$ be the values of $m + 1$ queries of sensitivity at most Δ_T on a dataset $\mathbf{D}$. Let $\{T_i'\}_{i\in[B]}$ be the values of the same queries on a neighboring dataset $\mathbf{D}'$. Let $Q_0, \dots, Q_m$ (respectively $Q_0', \dots, Q_m'$) denote the values $\{T_i\}_{i\in[0,m]}$ (respectively $\{T_i'\}_{i\in[0,m]}$) sorted in decreasing order. Then $|Q_c - Q_c'| \leq \Delta_T$ for all $c \in [0, m]$. As a result, the score function $s_k(c, \mathbf{D})$ has sensitivity at most 1 for all $c \in [0, m]$.*

Theorem 3.3 (Report Noisy Max [Dwork and Roth, 2014, McKenna and Sheldon, 2020, Ding et al., 2021])**.** *Let $\varepsilon > 0$. Given scores $s_i \in \mathbb{R}$, $i \in [B]$ of sensitivity at most 1, the algorithm* `ReportNoisyMax` *samples $Z_1, \dots, Z_B \sim \mathrm{Exp}(2/\varepsilon)$ and returns $\hat{\imath} = \arg\max_{i\in[B]}(s_i + Z_i)$. This algorithm is ε-DP and for $\delta \in (0, 1)$, with probability at least $1 - \delta$, it holds $s_{\hat{\imath}} \geq s^* - 2\log(B/\delta)\varepsilon^{-1}$, where $s^* = \max_{i\in[B]} s_i$.*

Statistic T and its Sensitivity. The statistic T that we use to obtain our private CRT test is defined as the numerator of the GCM statistic. The residuals of $\mathbf{Y}$ with respect to $\mathbf{Z}$ are calculated by fitting a KRR model of $\mathbf{Y}$ to $\mathbf{Z}$. Denote such residuals $r_{Y,i}$, for $i \in [n]$. The residuals of $\mathbf{X}$ with respect to $\mathbf{Z}$ are exact, since we have access to the distribution $X \mid Z$. Denote such residuals $r_{X,i}$ for $i \in [n]$. The residual products are calculated as $R_i = r_{X,i} r_{Y,i}$ for $i \in [n]$.

Definition 3.4 (Statistic T for the private CRT)**.** Given a dataset $(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ of n points, let $(R_1, \dots, R_n)$ be the vector of residual products of the exact residuals of $\mathbf{X}$ with respect to $\mathbf{Z}$ and the residuals of fitting a kernel ridge regression model of $\mathbf{Y}$ to $\mathbf{Z}$. Define $T(\mathbf{X}, \mathbf{Y}, \mathbf{Z}) = \sum_{i=1}^{n} R_i$.

We obtain a bound of $O_\lambda(1)$ on the ℓ_1-sensitivity of the statistic T by bounding the sensitivity of the R_i. To bound the sensitivity of the $r_{Y,i}$ we assume that the domain of the variable Y is bounded and use the result of Theorem 1.2. We assume a known bound on the magnitude of the residuals $r_{X,i}$, motivated by the fact that we have access to the distribution $X \mid Z$. This differs from the assumptions for our PrivGCM test, where we assumed bounds on both X and Y. Assuming a bound on the residuals $r_{X,i}$ gives a tighter sensitivity bound for T.

Lemma 3.5. (Sensitivity of T). *Consider two neighboring datasets* $\mathbf{D} = (\mathbf{X}^{(0)}, \ldots, \mathbf{X}^{(m)}, \mathbf{Y}, \mathbf{Z})$ *and* $\mathbf{D}' = (\mathbf{X}'^{(0)}, \ldots, \mathbf{X}'^{(m)}, \mathbf{Y}', \mathbf{Z}')$. *For* $j \in [0, m]$, *let* $T_j = T(\mathbf{X}^{(j)}, \mathbf{Y}, \mathbf{Z})$. *Define* T'_j *analogously. If* $|y_i|, |y'_i| \leq 1$ *for all* $i \in [n]$ *and* $|r^{(j)}_{X,i}|, |r'^{(j)}_{X,i}| \leq 1$[6] *for all* $i \in [n], j \in [0, m]$, *then* $|T_j - T'_j| \leq C'$, *where* $C' = 4 \cdot (1 + \frac{\sqrt{2}}{\sqrt{\lambda}} + \frac{2\sqrt{2}}{\lambda^{3/2}} + \frac{2}{\lambda})$.

Accuracy of the Private CRT. We define the accuracy of Algorithm 2 in terms of the difference between the private p-value it outputs and its non-private counterpart.

Definition 3.6 ((γ, δ)-accuracy)**.** Let $G_\gamma = |\{i \in [m] \mid |T_i - T_0| \leq \gamma\}|$. Let c^* be the rank of T_0 given statistics $T_i, i \in [0, m]$, and $p^* = (1 + c^*)/(m + 1)$ be the non-private p-value. We say Algorithm 2 is (γ, δ)-accurate if with probability at least $1 - \delta$ it holds $|\hat{p} - p^*| \leq \frac{G_\gamma}{m+1}$.

Define PrivCRT as Algorithm 2 where T is the statistic from Definition 3.4.

Theorem 3.7. PrivCRT *is* ε*-DP and* (γ, δ)*-accurate for* $\gamma = O\left(\frac{1}{\varepsilon} \log\left(\frac{m}{\delta}\right)\right)$.

Remark on the Accuracy. Under the null hypothesis, the T_i's are uniformly distributed, thus G_γ only grows linearly with γ. From Theorem 4.7, $\gamma = O(\log m)$, so $|\hat{p} - p^*| \to 0$ as $m \to \infty$. Empirically, we observe that, under the null, the p-values output by PrivCRT are uniformly distributed (Fig. 9), and thus the test provides type-I error control. Under the alternate, T_0 is much larger (or smaller) than all the other values $T_i, i \geq 1$ and thus G_γ is small. However, the power of PrivCRT can be affected if we increase m, as this can increase the value of G_γ (see Fig. 8). It is an interesting open question whether the dependence on m in the accuracy of a private CRT is avoidable. For now, we recommend using $m = O(1/\alpha)$, where α is the rejection level.

4 Empirical Evaluation

Setup. We use a setup similar to that of Shah and Peters [2020] proposed for evaluating the performance of GCM. Fix an RKHS $\mathcal{H}$ that corresponds to a Gaussian kernel. The function $f_s(z) = \exp(-s^2/2)\sin(sz)$ satisfies $f_s \in \mathcal{H}$. $Z = (Z_1, \ldots, Z_d)$ is a d-dimensional variable, where $d \in \{1, 5\}$. The distribution of (X, Y, Z) is as follows:

$$Z_1, \ldots, Z_d \sim N_Z, \quad X = f_s(Z_1) + N_X, \quad Y = -f_s(Z_1) + N_Y + \beta \cdot N_X,$$

where $N_Z \sim \mathcal{N}(0, 4)$, $N_X \sim \mathcal{N}(0, 1)$, $N_Y \sim \mathcal{N}(0, 1)$, and $\beta \geq 0$ is a constant controlling the strength of dependence between X and Y. If $\beta = 0$, then $X \perp\!\!\!\perp Y \mid Z$, but not otherwise. For experiments with PrivGCM, the dataset $(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ consists of n points sampled as above. For experiments with PrivCRT, we additionally sample m copies $\mathbf{X}^{(j)}$, $j \in [m]$, by fixing $\mathbf{Z}$. We study how varying β, s, and n affects the rejection rate of our tests (averaged over 500 resampled datasets). Shaded error bars represent 95% confidence intervals. We set type-I error level $\alpha = 0.05$.

We rescale X and Y so that all datapoints x_i and y_i satisfy $|x_i| \leq 1, |y_i| \leq 1$ (recall that we assume known bounds for the data; for this simulation, standard Gaussian concentration implies $\max_{i \leq n} X_i \leq \sqrt{2 \log n}$ with very high probability, so choosing $\sqrt{C \log n}$ suffices here for a sufficiently large constant C). We then fit a KRR model with a Gaussian kernel of $\mathbf{X}$ to $\mathbf{Z}$ and $\mathbf{Y}$ to $\mathbf{Z}$. The best model is chosen via 5-fold cross-validation and grid search over the regularization parameter λ and the parameter of the Gaussian kernel. The choice of λ requires balancing the performance of the fitting step of the algorithm with the magnitude of noise added (see Lemma 2.3), and thus some lower bound on λ is needed. We enforce $\lambda \geq 10$ and find that this does not hurt the performance of the fitting step even with increasing n. See Fig. 6 for an example dataset.

Comparison to the Private Kendall CI test [Wang et al., 2020] and Test-of-Tests [Kazan et al., 2023]. We start with a comparison to two other private CI tests in the literature. The first is the private Kendall's CI test, proposed by Wang et al. [2020] for categorical variables. The second, which we call PrivToT, is obtained from the Test-of-Tests framework of Kazan et al. [2023] and uses the non-private GCM as a black-box. See Appendix D for details on the implementations of these two tests. In Fig. 1, we compare the performance of these two tests with our private tests under the null hypothesis. We vary s, the model complexity from 1 to 32, and use a sample size $n = 10^4$ and privacy parameter $\varepsilon = 2$. The larger s, the harder it is to learn the function f_s. As the model complexity increases, the private Kendall test and PrivToT cannot control type-I error, even with a large sample size ($n = 10^4$). They perform even worse when Z is 5-dimensional. On the other hand, both PrivGCM and PrivCRT have consistent type-I error control across model complexity and dimensionality of Z. This experiment motivates the need for tests with rigorous theoretical type-I error guarantees, as we derive.[7]

[6] The bound of 1 can be replaced by any constant.

[7] Note that for tests without the desired type-I error control, statements about power are vacuous.

Figure 1: Type-I error control of PrivToT, private Kendall, PrivGCM, and PrivCRT (under the null): the first two fail to control Type-I error.

Next, we compare our private CI tests with their non-private counterparts. We fix $s = 2$ for f_s.

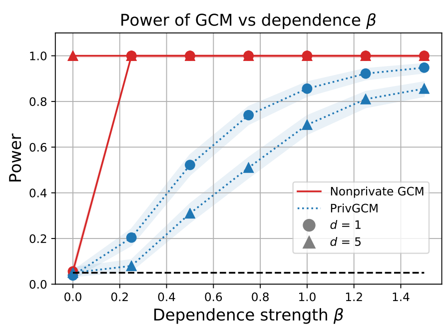

Figure 2: Comparison of the power of private and nonprivate GCM tests as the dependence strength β increases. At $d = 5$, the (nonprivate) GCM fails to provide type-I error control when $\beta = 0$.

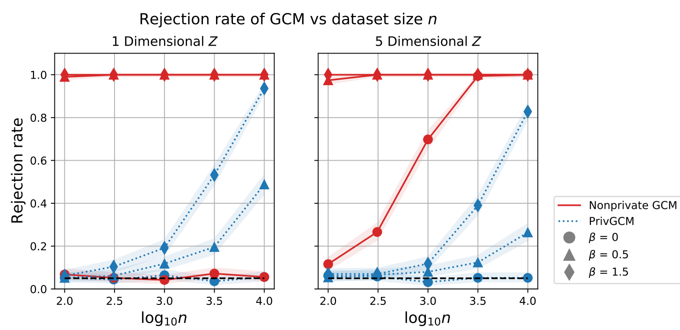

Figure 3: Comparison of the type-I error and power of private and nonprivate GCM tests as the dataset size n increases. Again, at $d = 5$ with $\beta = 0$, the (nonprivate) GCM fails to provide type-I error control even at large n (in fact, its type-I error gets worse with n).

Performance of PrivGCM. In Fig. 2, we vary β, the strength of the dependence between X and Y from 0 to 1.5 and compare the rejection rate of PrivGCM with the (non-private) GCM. We set $n = 10^4$ and privacy parameter $\varepsilon = 7$. In the one-dimensional case, i.e., when $d = 1$, the rejection rate of both tests goes from 0.05 to 1, with the rejection rate of GCM converging faster to 1 than for PrivGCM, as a consequence of the noise added for privacy. Crucially though, when $d = 5$, the privacy noise helps PrivGCM provide the critical type-I error control at $\beta = 0$, which non-private GCM fails at. The failure of (non-private) GCM to provide type-I error control is better examined in Fig. 3, where we vary the dataset size n from 10^2 to 10^4, and plot the rejection rate of PrivGCM and GCM for $\beta = 0$ and $\beta > 0$. When $d = 5$, the KRR model fails to fit the data (it returns a predicted function that is nearly-zero). In this case, for $\beta = 0$, the GCM statistic converges to a Gaussian of standard deviation 1, but whose mean is removed from zero. The larger n, the further the mean of the Gaussian is from zero, and the worse the type-I error. The noise added for privacy brings the mean close to zero since the standard deviation of the noisy residuals, σ'_P, is much larger than σ_P (see (5)).

In Fig. 3, for $\beta > 0$, we see that PrivGCM needs a higher dataset size to achieve the same power as GCM, concordant with our discussion following Theorem 2.2.

Performance of PrivCRT. We study the performance of PrivCRT in Figs. 4-5. PrivCRT achieves better power than PrivGCM for our setup, so we use a smaller privacy parameter of $\varepsilon = 2$ and set $m = 19$ (an extreme, but valid choice).

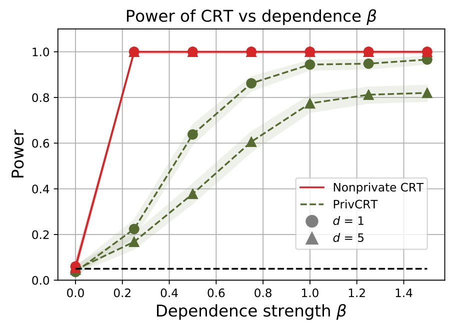

Figure 4: Comparison of power of private and nonprivate CRT tests as we increase dependence strength β.

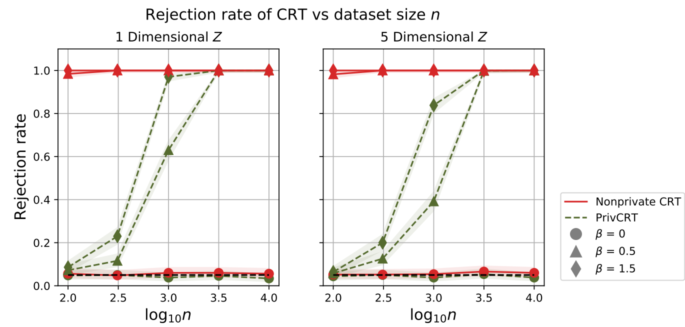

Figure 5: Comparison of the type-I error and power of private and nonprivate CRT tests as we increase the dataset size n.

In Fig. 4, we vary β, the dependence strength between X and Y, from 0 to 1.5, using $n = 10^3$. Both non-private CRT and PrivCRT provide type-I error control. Also, the power of both PrivCRT and (non-private) CRT converges to 1, with a faster convergence for the non-private test. In Fig. 5, we vary the dataset size n and $\beta \in \{0, 0.5, 1.5\}$.

Finally, in Fig. 7 (Appendix D), we compare the performance of PrivCRT with PrivGCM for different privacy parameters $\varepsilon \in [2^{-3}, 2^3]$. Both tests control type-I error, but PrivCRT achieves better power than PrivGCM for all privacy parameters ε. Therefore, PrivCRT appears preferable to PrivGCM when dataholders have access to the distribution $X \mid Z$. This result is consistent with the non-private scenario where the CRT has higher power because it does not have to learn $\mathbb{E}[X \mid Z]$.

5 Concluding Remarks

This work studies the fundamental statistical task of conditional independence testing under privacy constraints. We design the first DP conditional independence tests that support the general case of continuous variables and have strong theoretical guarantees on both statistical validity and power. Our experiments support our theoretical results and additionally demonstrate that our private tests have more robust type-I error control than their non-private counterparts.

We envision two straightforward generalizations of our private GCM test. First, our test can be generalized to handle multivariate X and Y, following Shah and Peters [2020], who obtain the test statistic from the residual products of fitting each variable in X and each variable in Y to Z. A natural extension would be to compute the same statistic on our noisy residual products. Secondly, following Scheidegger et al. [2022], a private version of the weighted GCM would allow the test to achieve power against a wider class of alternatives than the unweighted version. Finally, constructing private versions of other model-X based tests, such as the Conditional Permutation Test [Berrett et al., 2019], could be another interesting direction.

Acknowledgements

We would like to thank Patrick Blöbaum for helpful initial discussions surrounding this project.

References

Jordan Awan and Aleksandra B. Slavkovic. Differentially private uniformly most powerful tests for binomial data. In *Advances in Neural Information Processing Systems (NeurIPS)*, pages 4212–4222, 2018.

Andrés F. Barrientos, Jerome P. Reiter, Ashwin Machanavajjhala, and Yan Chen. Differentially private significance tests for regression coefficients. *Journal of Computational and Graphical Statistics*, 28:440 – 453, 2017.

Thomas B. Berrett, Yi Wang, Rina Foygel Barber, and Richard J. Samworth. The conditional permutation test for independence while controlling for confounders. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 82, 2019.

Hai Brenner and Kobbi Nissim. Impossibility of differentially private universally optimal mechanisms. *SIAM Journal on Computing (SICOMP)*, 43(5):1513–1540, 2014.

Zachary Campbell, Andrew Bray, Anna M. Ritz, and Adam Groce. Differentially private ANOVA testing. In *International Conference on Data Intelligence and Security*, pages 281–285, 2018.

Emmanuel J. Candès, Yingying Fan, Lucas Janson, and Jinchi Lv. Panning for gold: 'model-X' knockoffs for high dimensional controlled variable selection. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 80, 2016.

Simon Couch, Zeki Kazan, Kaiyan Shi, Andrew Bray, and Adam Groce. Differentially private nonparametric hypothesis testing. In *Proceedings of the ACM Conference on Computer and Communications Security, CCS*, pages 737–751, 2019.

A Philip Dawid. Conditional independence in statistical theory. *Journal of the Royal Statistical Society: Series B (Methodological)*, 41(1):1–15, 1979.

Zeyu Ding, Daniel Kifer, Sayed M. Saghaian N. E., Thomas Steinke, Yuxin Wang, Yingtai Xiao, and Danfeng Zhang. The permute-and-flip mechanism is identical to report-noisy-max with exponential noise. *arXiv 2105.07260*, 2021.

Cynthia Dwork and Aaron Roth. The algorithmic foundations of differential privacy. *Found. Trends Theor. Comput. Sci.*, 9(3-4):211–407, 2014.

Cynthia Dwork, Moni Naor, Omer Reingold, Guy N. Rothblum, and Salil P. Vadhan. On the complexity of differentially private data release: efficient algorithms and hardness results. In *Proceedings, ACM Symposium on Theory of Computing (STOC)*, pages 381–390, 2009.

Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam D. Smith. Calibrating noise to sensitivity in private data analysis. *Journal of Privacy and Confidentiality*, 7(3):17–51, 2016.

Stephen E. Fienberg, Alessandro Rinaldo, and Xiaolin Yang. Differential privacy and the risk-utility tradeoff for multi-dimensional contingency tables. In *Privacy in Statistical Databases*, volume 6344 of *Lecture Notes in Computer Science*, pages 187–199. Springer, 2010.

Kenji Fukumizu, Arthur Gretton, Xiaohai Sun, and Bernhard Schölkopf. Kernel measures of conditional dependence. *Advances in Neural Information Processing Systems (NeurIPS)*, 20, 2007.

Marco Gaboardi, Hyun-Woo Lim, Ryan M. Rogers, and Salil P. Vadhan. Differentially private Chi-Squared hypothesis testing: Goodness of fit and independence testing. In *Proceedings, International Conference on Machine Learning (ICML)*, volume 48, 2016.

Aaron Johnson and Vitaly Shmatikov. Privacy-preserving data exploration in genome-wide association studies. In *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 1079–1087, 2013.

Zeki Kazan, Kaiyan Shi, Adam Groce, and Andrew Bray. The test of tests: A framework for differentially private hypothesis testing. *CoRR*, abs/2302.04260, 2023.

Daphne Koller and Nir Friedman. *Probabilistic graphical models: principles and techniques*. MIT Press, 2009.

Matt J. Kusner, Yu Sun, Karthik Sridharan, and Kilian Q. Weinberger. Private causal inference. In *Proceedings, International Conference on Artificial Intelligence and Statistics (AISTATS)*, volume 51, pages 1308–1317, 2016.

Tengyuan Liang and Alexander Rakhlin. Just interpolate: Kernel "ridgeless" regression can generalize. *The Annals of Statistics*, 48(3):1329 – 1347, 2020.

Ryan McKenna and Daniel Sheldon. Permute-and-flip: A new mechanism for differentially private selection. In *Advances in Neural Information Processing Systems (NeurIPS)*, 2020.

Kobbi Nissim, Sofya Raskhodnikova, and Adam D. Smith. Smooth sensitivity and sampling in private data analysis. In *Proceedings, ACM Symposium on Theory of Computing (STOC)*, pages 75–84. ACM, 2007.

Judea Pearl. Models, reasoning and inference. *Cambridge, UK: Cambridge University Press*, 19(2), 2000.

Víctor Peña and Andrés F. Barrientos. Differentially private hypothesis testing with the subsampled and aggregated randomized response mechanism. *CoRR*, abs/2208.06803, 2023.

Ryan Rogers and Daniel Kifer. A new class of private chi-square hypothesis tests. In *Proceedings, International Conference on Artificial Intelligence and Statistics (AISTATS)*, volume 54, pages 991–1000, 2017.

Cyrill Scheidegger, Julia Hörrmann, and Peter Bühlmann. The weighted generalised covariance measure. *Journal of Machine Learning Research*, 23(273):1–68, 2022.

Rajen D. Shah and Jonas Peters. The hardness of conditional independence testing and the generalised covariance measure. *The Annals of Statistics*, 48(3), 2020.

Adam Smith. Privacy-preserving statistical estimation with optimal convergence rates. In *Proceedings, ACM Symposium on Theory of Computing (STOC)*, pages 813–822, 2011.

Eric V Strobl, Kun Zhang, and Shyam Visweswaran. Approximate kernel-based conditional independence tests for fast non-parametric causal discovery. *Journal of Causal Inference*, 7(1), 2019.

Marika Swanberg, Ira Globus-Harris, Iris Griffith, Anna M. Ritz, Adam Groce, and Andrew Bray. Improved differentially private analysis of variance. *Proc. Priv. Enhancing Technol.*, 2019(3):310–330, 2019.

Caroline Uhler, Aleksandra B. Slavkovic, and Stephen E. Fienberg. Privacy-preserving data sharing for genome-wide association studies. *J. Priv. Confidentiality*, 5(1), 2013.

Praneeth Vepakomma, Mohammad Mohammadi Amiri, Clément L. Canonne, Ramesh Raskar, and Alex Pentland. Private independence testing across two parties. *CoRR*, abs/2207.03652, 2022.

Duy Vu and Aleksandra B. Slavkovic. Differential privacy for clinical trial data: Preliminary evaluations. In *ICDM Workshops*, pages 138–143, 2009.

Lun Wang, Qi Pang, and Dawn Song. Towards practical differentially private causal graph discovery. In *Advances in Neural Information Processing Systems (NeurIPS)*, 2020.

Yue Wang, Jaewoo Lee, and Daniel Kifer. Revisiting differentially private hypothesis tests for categorical data. *arXiv 1511.03376*, 2015.

Yue Wang, Daniel Kifer, Jaewoo Lee, and Vishesh Karwa. Statistical approximating distributions under differential privacy. *J. Priv. Confidentiality*, 8(1), 2018.

Fei Yu, Stephen E. Fienberg, Aleksandra B. Slavkovic, and Caroline Uhler. Scalable privacy-preserving data sharing methodology for genome-wide association studies. *J. Biomed. Informatics*, 50:133–141, 2014.

Kun Zhang, Jonas Peters, Dominik Janzing, and Bernhard Schölkopf. Kernel-based conditional independence test and application in causal discovery. In *Proceedings of the Conference on Uncertainty in Artificial Intelligence (UAI)*, pages 804–813, 2011.

A Missing Details from Section 1

A.1 Additional Related Work

Conditional Independence Testing. A popular category of CI tests are kernel-based tests, obtained by extending the Hilbert-Schmidt independence criterion to the conditional setting Fukumizu et al. [2007], Zhang et al. [2011], Strobl et al. [2019]. However, these tests only provide a weaker *pointwise* asymptotic validity guarantee. It is widely acknowledged that for a statistical test to be useful in practice, it needs to provide the stronger guarantees of either valid level at finite sample size or *uniformly* asymptotic level. Our private GCM test provides the latter guarantee.

One way of getting around the hardness result of Shah and Peters [2020] is through the model-X assumption, where the conditional distribution of $X \mid Z$ is assumed to be accessible. Tests based on this assumption, such as CRT (conditional randomization test) [Candès et al., 2016] and CPT (conditional permutation test) [Berrett et al., 2019], provide a general framework for conditional independence testing, where one can use their test statistic of choice and exactly (non-asymptotically) control the type-I error regardless of the data dimensionality.

A.2 Background on Differential Privacy

Definition A.1 (ℓ_1-sensitivity)**.** For a function $f : \mathcal{D} \to \mathbb{R}^d$, its ℓ_1-sensitivity Δ_f is defined as $\Delta_f = \max_{\mathbf{D},\mathbf{D}'\text{neighbors}} \|f(\mathbf{D}) - f(\mathbf{D}')\|_1$.

Lemma A.2 (Laplace Mechanism [Dwork et al., 2016])**.** *Let $\varepsilon > 0$ and $f : \mathcal{D} \to \mathbb{R}^d$ be a function with ℓ_1-sensitivity Δ_f. Let $W \sim \mathrm{Lap}(0, \Delta_f/\varepsilon)$ be a noise vector from the Laplace distribution with scale parameter Δ_f/ε. The Laplace Mechanism that, on input $\mathbf{D}$ and ε, outputs $f(\mathbf{D}) + W$ is ε-DP.*

Lemma A.3 (Post-Processing Dwork et al. [2016])**.** *If the algorithm $\mathcal{A}$ is ε-differentially private, and g is any randomized function, then the algorithm $g(\mathcal{A}(x))$ is ε-differentially private.*

B Proofs of Section 2

B.1 Proof of Theorem 2.1

The first part of Theorem 2.1 gives the pointwise asymptotic level guarantee, whereas the second part shows the more desirable uniform asymptotic level guarantee under a slightly stronger condition.

Theorem 2.1. (Type-I Error Control of Private GCM) *Let a and b be known bounds on the domains of X and Y, respectively. Given a dataset $\mathbf{D} = (\mathbf{X}, \mathbf{Y}, \mathbf{Z})$, let $(\hat{\mathbf{X}}, \hat{\mathbf{Y}}, \mathbf{Z})$ be the rescaled dataset obtained by setting $\hat{\mathbf{X}} = \mathbf{X}/a$ and $\hat{\mathbf{Y}} = \mathbf{Y}/b$. Consider $R_i, i \in [n]$, as defined in (1), for the rescaled dataset $(\hat{\mathbf{X}}, \hat{\mathbf{Y}}, \mathbf{Z})$. Let $W_i \sim \mathrm{Lap}(0, \Delta/\varepsilon)$ for $i \in [n]$, where $\Delta, \varepsilon > 0$ are constants. Then $T^{(n)} = T(R_1 + W_1, \ldots, R_n + W_n)$, defined in Algorithm 1, satisfies:*

1. *For $P \in \mathcal{P}_0$ such that $A_f A_g = o_P(n^{-1}), B_f = o_P(1), B_g = o_P(1)$, and $\mathbb{E}[\chi_P^2 \xi_P^2] < \infty$, then*

$$\lim_{n\to\infty} \sup_{t\in\mathbb{R}} |\Pr_{P'}[T^{(n)} \le t] - \Phi(t)| = 0.$$

2. *Let $\mathcal{P} \subset \mathcal{P}_0$ be a set of distributions such that $A_f A_g = o_{\mathcal{P}}(n^{-1}), B_f = o_{\mathcal{P}}(1)$ and $B_g = o_{\mathcal{P}}(1)$. If in addition $\sup_{P\in\mathcal{P}} \mathbb{E}[|\chi_P \xi_P|^{2+\eta}] \le c$, for some constants $c, \eta > 0$, then*

$$\lim_{n\to\infty} \sup_{P'\in\mathcal{P}'} \sup_{t\in\mathbb{R}} |\Pr_{P'}[T^{(n)} \le t] - \Phi(t)| = 0. \tag{4}$$

Proof. Let $\sigma_P = \sqrt{\mathrm{Var}(\chi_P \xi_P)}$, $\sigma_{\text{priv}} = \Delta/\varepsilon$, and $\sigma_{\text{joint}} = \sqrt{\frac{\sigma_P^2}{a^2 b^2} + 2\sigma_{\text{priv}}^2}$. Denote by τ_N the numerator of $T^{(n)}$ and by τ_D the denominator. We sometimes omit P from the notation for ease of presentation.

We first show Item 1. Specifically, we show that $\tau_N \to \mathcal{N}(0, \sigma^2_{\text{joint}})$ and $\tau_D \to \sigma_{\text{joint}}$, which, by Slutsky's lemma (Lemma B.5), would imply that $T^{(n)} \to \mathcal{N}(0,1)$. For $i \in [n]$, let $\chi_i = x_i - f(z_i)$ and $\xi_i = y_i - g(z_i)$. Note that

$$\begin{aligned}\tau_N &= \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (R_i + W_i) \\ &= \frac{1}{ab\sqrt{n}} \sum_{i=1}^{n} (f(z_i) - \hat{f}(z_i))(g(z_i) - \hat{g}(z_i)) + \frac{1}{ab\sqrt{n}} \sum_{i=1}^{n} (f(z_i) - \hat{f}(z_i))\xi_i \\ &+ \frac{1}{ab\sqrt{n}} \sum_{i=1}^{n} (g(z_i) - \hat{g}(z_i))\chi_i + \frac{1}{\sqrt{n}} \sum_{i=1}^{n} \left(\frac{\chi_i \xi_i}{ab} + W_i\right) \end{aligned} \tag{6}$$

We use the following claim obtained from the proof of Theorem 6 of Shah and Peters [2020].

Claim B.1 (Shah and Peters [2020]). *Under the assumptions listed in Item 1 of Theorem 2.1, the following hold*

1. $\frac{1}{\sqrt{n}} \sum_{i=1}^{n} (f(z_i) - \hat{f}(z_i))(g(z_i) - \hat{g}(z_i)) \xrightarrow{P} 0.$
2. $\frac{1}{\sqrt{n}} \sum_{i=1}^{n} (f(z_i) - \hat{f}(z_i))\xi_i \xrightarrow{P} 0.$
3. $\frac{1}{\sqrt{n}} \sum_{i=1}^{n} (g(z_i) - \hat{g}(z_i))\chi_i \xrightarrow{P} 0.$
4. $\frac{1}{n} \sum_{i=1}^{n} R_i \xrightarrow{P} 0.$
5. $\frac{1}{n} \sum_{i=1}^{n} R_i^2 \xrightarrow{P} \frac{\sigma_P^2}{a^2 b^2}.$

Additionally, under the assumptions of Item 2, all convergence statements above are uniform over $\mathcal{P}$.

By Claim B.1, Items 1-3, the first three terms of the sum in (6) are $o_P(1)$. We show that the last term of the sum converges to $\mathcal{N}(0, \sigma^2_{\text{joint}})$. Note that $\mathbb{E}[\frac{\chi_i \xi_i}{ab} + W_i] = 0$ and $\text{Var}(\frac{\chi_i \xi_i}{ab} + W_i) = \text{Var}(\chi_i \xi_i) + \text{Var}(W_i) = \sigma^2_{\text{joint}}$. Since σ_{priv} is a constant and $\sigma_P < \infty$, we can apply the Central Limit Theorem to obtain the desired convergence to a Gaussian. By Slutsky's lemma, we obtain that $\tau_N \to \mathcal{N}(0, \sigma^2_{\text{joint}})$.

We now consider τ_D. Since $\mathbb{E}[W_i] = 0$ for all $i \in [n]$, by the Weak Law of Large Numbers it holds that $\frac{1}{n} \sum_{i=1}^{n} W_i \to 0$. From Item 4 of Claim B.1, we obtain $\frac{1}{n} \sum_{i=1}^{n} (R_i + W_i) \xrightarrow{P} 0$. It remains to show that $\frac{1}{n} \sum_{i=1}^{n} (R_i + W_i)^2 \xrightarrow{P} \sigma_P$. We have

$$\frac{1}{n} \sum_{i=1}^{n} (R_i + W_i)^2 = \frac{1}{n} \sum_{i=1}^{n} R_i^2 + \frac{2}{n} \sum_{i=1}^{n} R_i W_i + \frac{1}{n} \sum_{i=1}^{n} W_i^2.$$

Since R_i and W_i are independent, we have $\mathbb{E}[R_i W_i] = \mathbb{E}[R_i]\mathbb{E}[W_i] = 0$. Another application of the Weak Law of Large Numbers yields $\frac{2}{n} \sum_{i=1}^{n} R_i W_i \xrightarrow{P} 0$. Finally, let $B^{(n)} = \frac{1}{n} \sum_{i=1}^{n} W_i^2$. We have $\mathbb{E}[W_i^2] = \text{Var}[W_i] = 2\sigma^2_{\text{priv}}$. The Weak Law of Large numbers gives that $B^{(n)} \to 2\sigma^2_{\text{priv}}$. By Item 5 of Claim B.1 and Slutsky's lemma, we obtain that $\tau_D \to \sigma_{\text{joint}}$, as desired. This concludes the proof of Item 1.

Turning to Item 2, the proof follows similarly to that of Item 1, but more care is needed to replace statements of convergence with statements of uniform convergence. We first show that τ_N converges to $\mathcal{N}(0, \sigma^2_{\text{joint}})$ uniformly. Consider again the sum in (6). By Claim B.1, Items 1-3, the first three terms of the sum in (6) are $o_{\mathcal{P}}(1)$, and as a consequence, $o_{\mathcal{P}'}(1)$. We show that

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} \left(\frac{\chi_i \xi_i}{ab} + W_i\right) \to \mathcal{N}\left(0, \sigma^2_{\text{joint}}\right) \text{ uniformly over } \mathcal{P}'. \tag{7}$$

Then, applying Item 1 of Lemma B.8 we would obtain the desired convergence of τ_N. We prove (7) by showing that the random variables $\frac{\chi_i \xi_i}{ab} + W_i, i \in [n]$ satisfy the conditions of Lemma B.6. Recall that $\mathbb{E}[\frac{\chi_i \xi_i}{ab} + W_i] = 0$ and

$\mathbb{E}[(\frac{\chi_i\xi_i}{ab}+W_i)^2] = \mathrm{Var}(\frac{\chi_i\xi_i}{ab}+W_i) = \sigma^2_{\text{joint}}$, which is a constant. It remains to bound the $(2+\eta)$-absolute moment of $\frac{\chi_i\xi_i}{ab}+W_i$. By Claim B.10 and our assumption on $\chi_i\xi_i$, we have

$$\mathbb{E}\Big[\Big|\frac{\chi_i\xi_i}{ab}+W_i\Big|^{2+\eta}\Big] \le 2^{1+\eta}\Big(\mathbb{E}\Big[\Big|\frac{\chi_i\xi_i}{ab}\Big|^{2+\eta}\Big]+\mathbb{E}[|W_i|^{2+\eta}]\Big) \le 2^{(1+\eta)}\cdot\Big(\frac{c}{(ab)^{2+\eta}}+c'\Big)$$

where c' is the (constant) bound on $\mathbb{E}[|W_i|^{2+\eta}])$ given by Claim B.11. Thus, all the conditions of Lemma B.6 are satisfied, and (7) holds. This concludes our argument on the convergence of τ_N.

We now show that τ_D converges uniformly over $\mathcal{P}'$ to σ_{joint}. We first show that $n^{-1}\sum_{i=1}^n(R_i+W_i) = o_{\mathcal{P}'}(1)$. By Item 4 of Claim B.1, we have that $n^{-1}\sum_{i=1}^n R_i = o_{\mathcal{P}'}(1)$. We also showed that $\frac{1}{n}\sum_{i=1}^n W_i = o_{\mathcal{P}'}(1)$. Applying Lemma B.8, we obtain that $n^{-1}\sum_{i=1}^n(R_i+W_i) = o_{\mathcal{P}'}(1)$.

Next, we show that $n^{-1}\sum_{i=1}^n R_iW_i = o_{\mathcal{P}'}(1)$. Note that

$$\begin{aligned}\frac{1}{n}\sum_{i=1}^n R_iW_i &= \frac{1}{ab}\Big(\frac{1}{n}\sum_{i=1}^n(f(z_i)-\hat{f}(z_i)+\chi_i)(g(z_i)-\hat{g}(z_i)+\xi_i)W_i\Big)\\ &= \frac{1}{ab}\Big(\frac{1}{n}\sum_{i=1}^n(f(z_i)-\hat{f}(z_i))(g(z_i)-\hat{g}(z_i))W_i+\frac{1}{n}\sum_{i=1}^n(f(z_i)-\hat{f}(z_i))\xi_iW_i\\ &\quad+\frac{1}{n}\sum_{i=1}^n(g(z_i)-\hat{g}(z_i))\chi_{P,i}W_i+\frac{1}{n}\sum_{i=1}^n\chi_i\xi_iW_i\Big)\end{aligned} \tag{8}$$

We show that each of the terms of the sum in (8) is $o_{\mathcal{P}'}(1)$, starting with $n^{-1}\sum_{i=1}^n\chi_i\xi_iW_i$. We do so by showing that the conditions of Lemma B.7 hold for the random variables $\chi_i\xi_iW_i$. More precisely, we need to show that for all $P'\in\mathcal{P}'$ it holds that $\mathbb{E}_{P'}[|\chi_i\xi_iW_i|^{1+\eta}] < c_2$ for some $c_2,\eta>0$. By the assumptions in Item 2, we know $\mathbb{E}_{P'}[|\chi_P\xi_P|^{1+\eta}] \le \mathbb{E}_{P'}[|\chi_P\xi_P|^{2+\eta}] \le c$. By the independence of $\chi_i\xi_i$ and W_i we have

$$\mathbb{E}_{P'}[|\chi_i\xi_iW_i|^{1+\eta}] = \mathbb{E}_{P'}[|\chi_P\xi_P|^{1+\eta}]\mathbb{E}_{P'}[|W_i|^{1+\eta}] \le c\cdot c',$$

where c' is a bound on $\mathbb{E}_{P'}[|W_i|^{1+\eta}]$ given by Claim B.11. Therefore, we have that the variables $\chi_i\xi_iW_i$ satisfy all properties listed in Lemma B.7, and thus

$$n^{-1}\sum_{i=1}^n\chi_i\xi_iW_i = o_{\mathcal{P}}(1). \tag{9}$$

Next, we show that

$$\frac{1}{n}\sum_{i=1}^n(f(z_i)-\hat{f}(z_i))(g(z_i)-\hat{g}(z_i))W_i = o_{\mathcal{P}'}(1). \tag{10}$$

Denote the term in the LHS of (10) by b. We have

$$|b| \le \max_{i\in[n]}|W_i|\cdot\Big(\frac{1}{n}\sum_{i=1}^n(f(z_i)-\hat{f}(z_i))(g(z_i)-\hat{g}(z_i))\Big) \tag{11}$$

We show that $\max_{i\in[n]}|W_i| = O_{\mathcal{P}'}(\log n)$ in Claim B.9. By Item 1 of Claim B.1, the other term in the product in the RHS of (11) is $o_{\mathcal{P}}(n^{-1/2})$. As a result, $b = o_{\mathcal{P}'}(1)$. By a similar proof, and using Claim B.1, the other terms in the sum in (8) are equal to $o_{\mathcal{P}'}(1)$.

By Item 5 of Claim B.1, we have that $\frac{1}{n}\sum_{i=1}^n R_i^2$ converges uniformly over $\mathcal{P}'$ to $\frac{\sigma_P^2}{a^2b^2}$. In addition, we showed that $\frac{1}{n}\sum_{W_i}^2$ converges uniformly over $\mathcal{P}'$ to $2\sigma^2_{\text{priv}}$. Applying Lemma B.8 we obtain that τ_D converges uniformly over $\mathcal{P}'$ to σ_{joint}. One final application of Lemma B.8 yields that $T^{(n)}$ converges uniformly over $\mathcal{P}'$ to $\mathcal{N}(0,1)$. □

B.2 Proof of Theorem 2.2

The first part of Theorem 2.2. gives the pointwise power guarantee, whereas the second part shows the uniform power guarantee under a slightly stronger condition.

Theorem 2.2. (Power of Private GCM). *Consider the setup of Theorem 2.1. Let A_f, A_g, B_f, B_g be as defined in (3), with the difference that $\hat{f}$ and $\hat{g}$ are estimated on the first half of the dataset $(\hat{\mathbf{X}}, \hat{\mathbf{Y}}, \mathbf{Z})$, and $R_i, i \in [n/2, n]$ are calculated on the second half. Define the "signal" (ρ_P) and "noise" (σ_P) of the true residuals χ_P, ξ_P as:*

$$\rho_P = \mathbb{E}_P[\mathrm{cov}(X, Y \mid Z)], \sigma_P = \sqrt{\mathrm{Var}_P(\chi_P \xi_P)}.$$

1. *If for $P \in \mathcal{E}_0$ we have $A_f A_g = o_P(n^{-1}), B_f = o_P(1), B_g = o_P(1)$ and $\sigma_P < \infty$, then*

$$\lim_{n\to\infty} \sup_{t\in\mathbb{R}} \Big| \Pr_{P'}\Big[T^{(n)} - \frac{\sqrt{n}\rho_P}{\sigma'_P} \le t\Big] - \Phi(t) \Big| = 0, \text{ where } \sigma'_P = \sqrt{\sigma_P^2 + (\frac{\sqrt{2}ab\Delta}{\varepsilon})^2}. \tag{5}$$

2. *Let $\mathcal{P} \subset \mathcal{E}_0$ such that $A_f A_g = o_{\mathcal{P}}(n^{-1}), B_f = o_{\mathcal{P}}(1)$ and $B_g = o_{\mathcal{P}}(1)$. If in addition $\sup_{P\in\mathcal{P}} \mathbb{E}[|\chi_P \xi_P|^{2+\eta}] \le c$, for some constants $c, \eta > 0$, then (5) holds over $\mathcal{P}'$ uniformly.*

Proof. Note that $\mathbb{E}[\frac{\chi_P \xi_P}{ab}] = \frac{\rho}{ab}$ and $\sqrt{\mathrm{Var}(\frac{\chi_P \xi_P}{ab})} = \frac{\sigma_P}{ab}$. The proof is similar to that of Theorem 2.1, using the following result from Shah and Peters [2020].

Claim B.2. *Under the assumptions listed in Theorem 2.2, as $n \to \infty$, the following hold.*

1. $\frac{1}{\sqrt{n}} \sum_{i=1}^n (f(z_i) - \hat{f}(z_i))(g(z_i) - \hat{g}(z_i)) \xrightarrow{P} 0.$
2. $\frac{1}{\sqrt{n}} \sum_{i=1}^n (f(z_i) - \hat{f}(z_i))\xi_i \xrightarrow{P} 0.$
3. $\frac{1}{\sqrt{n}} \sum_{i=1}^n (g(z_i) - \hat{g}(z_i))\chi_i \xrightarrow{P} 0.$
4. $\frac{1}{n} \sum_{i=1}^n R_i \xrightarrow{P} 0.$
5. $\frac{1}{n} \sum_{i=1}^n R_i^2 \xrightarrow{P} \frac{\sigma_P^2}{a^2 b^2}.$

Additionally, under the assumptions in Item 2 of Theorem 2.2, all convergence statements above are uniform over $\mathcal{P}$.

□

Corollary B.3. *Under the assumptions of Theorem 2.2, Algorithm 1 has asymptotic power of 1 if $\rho_P \neq 0$.*

Proof. Note that Algorithm 1 has asymptotic power of 1 if, for all $M > 0$, it holds $\Pr_P[T^{(n)} > M] \to 1$ as $n \to \infty$. Given $M > 0$, note that

$$\Pr[T^{(n)} \le M] = \Pr_{P'}\Big[T^{(n)} - \frac{\sqrt{n}\rho_P}{\sigma'_P} \le M - \frac{\sqrt{n}\rho_P}{\sigma'_P}\Big] \to \Phi\Big(M - \frac{\sqrt{n}\rho_P}{\sigma'_P}\Big),$$

where the convergence statement follows from Theorem 2.2. Since $\rho_P \neq 0$ and σ'_P is a constant, then $M - \frac{\sqrt{n}\rho_P}{\sigma'_P} \to -\infty$ as $n \to \infty$. Therefore $\Phi\Big(M - \frac{\sqrt{n}\rho_P}{\sigma'_P}\Big) \to 0$, and as a result $\Pr[T^{(n)} \le M] \to 0$, as desired. □

B.3 Guarantees of PrivGCM

Lemma 2.3. (Sensitivity of residual products). *Let* $\mathbf{R}$ *be the vector of residual products, as defined in* (1)*, of fitting a KRR model of* $\mathbf{X}$ *to* $\mathbf{Z}$ *and* $\mathbf{Y}$ *to* $\mathbf{Z}$ *with regularization parameter* $\lambda > 0$*. If* $|x_i|, |y_i| \le 1$ *for all* $i \in [n]$*, then* $\Delta_{\mathbf{R}} \le C$ *where* $C = 4(1 + \frac{\sqrt{2}}{\sqrt{\lambda}})(1 + \frac{\sqrt{2}}{\sqrt{\lambda}} + \frac{4\sqrt{2}}{\lambda^{3/2}} + \frac{4}{\lambda})$.

Proof. Consider two neighboring datasets $(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ and $(\mathbf{X}', \mathbf{Y}', \mathbf{Z}')$. For $i \in [n]$, let $r_{X,i}, r_{Y,i}$ denote the residuals of fitting a kernel ridge regression model of $\mathbf{X}$ to $\mathbf{Z}$ and $\mathbf{Y}$ to $\mathbf{Z}$, respectively. Suppose without loss of generality that $(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ and $(\mathbf{X}', \mathbf{Y}', \mathbf{Z}')$ differ only in the last datapoint, i.e., $(x_i, y_i, z_i) = (x'_i, y'_i, z'_i)$ for $i \in [n-1]$. Then, by Theorem 1.2, for $i \in [n-1]$, we have

$$|r_{X,i} - r'_{X,i}| = |(x_i - \mathbf{w}^\top \phi(z_i)) - (x'_i - \mathbf{w}'^\top \phi(z'_i))| = |\mathbf{w}^\top \phi(z_i) - \mathbf{w}'^\top \phi(z_i)| \le \frac{8\sqrt{2}}{\lambda^{3/2} n} + \frac{8}{\lambda n}.$$

For the last datapoint we have

$$\begin{aligned} |r_{X,n} - r'_{X,n}| &= |(x_n - \mathbf{w}^\top \phi(z_n)) - (x'_n - \mathbf{w}'^\top \phi(z'_n))| \\ &\le |x_n - x'_n| + \|\mathbf{w}'\|_{\mathcal{H}} |\phi(z'_n) - \phi(z_n)| + |\mathbf{w}'^\top \phi(z_n) - \mathbf{w}^\top \phi(z_n)| \\ &\le 2 + \frac{2\sqrt{2}}{\sqrt{\lambda}} + \frac{8\sqrt{2}}{\lambda^{3/2} n} + \frac{8}{\lambda n}. \end{aligned}$$

Finally, note that for all $i \in [n]$, we have$|r_{X,i}| \le |x_i| + \|\mathbf{w}\|_{\mathcal{H}} \|\phi(z_i)\|_{\mathcal{H}} \le 1 + \frac{\sqrt{2}}{\sqrt{\lambda}}$. The same bound holds for $|r_{Y,i}|$. Let $c_1 = 2 + \frac{2\sqrt{2}}{\sqrt{\lambda}}$ and $c_2 = \frac{8\sqrt{2}}{\lambda^{3/2}} + \frac{8}{\lambda}$. This gives us that for all $i \in [n-1]$:

$$|R_i - R'_i| \le |r_{X,i}||r_{Y,i} - r'_{Y,i}| + |r'_{Y,i}||r_{X,i} - r'_{X,i}| \le 2\Big(1 + \frac{\sqrt{2}}{\sqrt{\lambda}}\Big)\Big(\frac{8\sqrt{2}}{\lambda^{3/2} n} + \frac{8}{\lambda n}\Big) = \frac{c_1 c_2}{n}.$$

For $i = n$ we have

$$|R_n - R'_n| \le 2\Big(1 + \frac{\sqrt{2}}{\sqrt{\lambda}}\Big)\Big(2 + \frac{2\sqrt{2}}{\sqrt{\lambda}} + \frac{8\sqrt{2}}{\lambda^{3/2} n} + \frac{8}{\lambda n}\Big) = c_1(c_1 + \frac{c_2}{n}).$$

Finally,

$$\|\mathbf{R} - \mathbf{R}'\|_1 = \sum_{i=1}^{n} |R_i - R'_i| \le (n-1) \cdot \frac{c_1 c_2}{n} + c_1(c_1 + \frac{c_2}{n}) = c_1^2 + c_1 c_2,$$

as desired. □

Corollary B.4. *Let* a *and* b *be known bounds on the domains of* X *and* Y*, respectively. Given a dataset* $\mathbf{D} = (\mathbf{X}, \mathbf{Y}, \mathbf{Z})$*, let* $(\hat{\mathbf{X}}, \hat{\mathbf{Y}}, \mathbf{Z})$ *be the rescaled dataset obtained by setting* $\hat{\mathbf{X}} = \mathbf{X}/a$ *and* $\hat{\mathbf{Y}} = \mathbf{Y}/b$*. Let PrivGCM be the algorithm which runs Algorithm 1 with kernel ridge regression as the fitting procedure* $\mathcal{F}$ *and sensitivity bound* $\Delta = C$*, where* C *is the constant from Lemma 2.3. Algorithm PrivGCM is* ε*-differentially private.*

The statistic $T^{(n)} = T(R_1 + W_1, \ldots, R_n + W_n)$*, defined in Algorithm 1, satisfies the following.*

1. *Let* $\mathcal{P} \subset \mathcal{P}_0$ *be a family of distributions such that* $A_f A_g = o_{\mathcal{P}}(n^{-1}), B_f = o_{\mathcal{P}}(1), B_g = o_{\mathcal{P}}(1)$*. If in addition* $\sup_{P \in \mathcal{P}} \mathbb{E}[|\chi_P \xi_P|^{2+\eta}] \le c$*, for some constants* $c, \eta > 0$*, then*

$$\lim_{n\to\infty} \sup_{P' \in \mathcal{P}'} \sup_{t \in \mathbb{R}} |\Pr_{P'}[T^{(n)} \le t] - \Phi(t)| = 0.$$

2. *Define* $\rho_P = \mathbb{E}_P[\mathrm{cov}(X, Y \mid Z)]$ *and* $\sigma_P = \sqrt{\mathrm{Var}_P(\chi_P \xi_P)}$*. Let* $\mathcal{P} \subset \mathcal{E}_0$ *be a family of distributions such that* $A_f A_g = o_{\mathcal{P}}(n^{-1}), B_f = o_{\mathcal{P}}(1)$ *and* $B_g = o_{\mathcal{P}}(1)$*. If in addition we have* $\sup_{P \in \mathcal{P}} \mathbb{E}[|\chi_P \xi_P|^{2+\eta}] \le c$*, for some constants* $c, \eta > 0$*, then*

$$\lim_{n\to\infty} \sup_{P' \in \mathcal{P}'} \sup_{t \in \mathbb{R}} \Big| \Pr_{P'}\Big[T^{(n)} - \frac{\sqrt{n}\rho_P}{\sigma'_P} \le t\Big] - \Phi(t) \Big| = 0,$$

where $\sigma'_P = \sqrt{\sigma_P^2 + (\frac{\sqrt{2}ab \cdot C}{\varepsilon})^2}$.

Proof. The fact that PrivGCM is ε-differentially private follows from Lemmas A.2 and 2.3. Note that if the regularization parameter λ is chosen adaptively based on the data, then obtaining the value of the constant C by plugging in λ might not be ε-differentially private. This can be resolved by setting an a priori lower bound on λ, independent of the data, e.g., $\lambda \geq 1$, and plugging that lower bound to obtain C.

Item 1 follows from Theorem 2.1 and Lemma 2.3. Item 2 follows from Theorem 2.2 and Lemma 2.3 □

B.4 Auxiliary Lemmas

Lemma B.5 (Slutsky's Lemma)**.** *Let A_n, B_n be sequences of random variables. If A_n converges in distribution to A and B_n converges in probability to a constant c, then (1) $A_n + B_n \to A + c$, (2) $A_n \cdot B_n \to c \cdot A$, and (3) $A_n/B_n \to A/c$.*

Lemma B.6 (Uniform version of the Central Limit Theorem (Lemma 18 of Shah and Peters [2020]))**.** *Let $\mathcal{P}$ be a family of distributions for a random variable ζ such that for all $P \in \mathcal{P}$ it holds $\mathbb{E}_P[\zeta] = 0$, $\mathbb{E}_P[\zeta^2] = 1$, and $\mathbb{E}_P[|\zeta|^{2+\eta}] < c$ for some $\eta, c > 0$. Let $(\zeta_i)_{i\in\mathbb{N}}$ be i.i.d copies of ζ. For $n \in \mathbb{N}$, define $S_n = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} \zeta_i$. Then*

$$\lim_{n\to\infty} \sup_{P\in\mathcal{P}} \sup_{t\in\mathbb{R}} |\Pr_P[S_n \leq t] - \Phi(t)| = 0.$$

Lemma B.7 (Uniform version of the Weak Law of Large Numbers (Lemma 19 of Shah and Peters [2020]))**.** *Let $\mathcal{P}$ be a family of distributions for a random variable ζ such that for all $P \in \mathcal{P}$ it holds $\mathbb{E}_P[\zeta] = 0$ and $\mathbb{E}_P[|\zeta|^{1+\eta}] < c$ for some $\eta, c > 0$. Let $(\zeta_i)_{i\in\mathbb{N}}$ be i.i.d copies of ζ. For $n \in \mathbb{N}$, define $S_n = \frac{1}{n} \sum_{i=1}^{n} \zeta_i$. Then for all $\delta > 0$ it holds*

$$\lim_{n\to\infty} \sup_{P\in\mathcal{P}} \Pr_P[|S_n| > \delta] = 0.$$

Lemma B.8 (Uniform version of Slutsky's Lemma (Lemma 20 of Shah and Peters [2020]))**.** *Let $\mathcal{P}$ be a family of distributions that determines the law of sequences $(A_n)_{n\in\mathbb{N}}$ and $(B_n)_{n\in N}$ of random variables.*

1. *If A_n converges uniformly over $\mathcal{P}$ to $\mathcal{N}(0, 1)$, and $B_n = o_{\mathcal{P}}(1)$, then $A_n + B_n$ converges uniformly over $\mathcal{P}$ to $\mathcal{N}(0, 1)$.*
2. *If A_n converges uniformly over $\mathcal{P}$ to $\mathcal{N}(0, 1)$, and $B_n = 1 + o_{\mathcal{P}}(1)$, then A_n/B_n converges uniformly over $\mathcal{P}$ to $\mathcal{N}(0, 1)$.*
3. *If $A_n = M + o_{\mathcal{P}}(1)$ for some $M > 0$ and $B_n = o_{\mathcal{P}}(1)$, then $A_n + B_n = M + o_{\mathcal{P}}(1)$.*
4. *If $A_n = o_{\mathcal{P}}(1)$ and $B_n = o_{\mathcal{P}}(1)$, then $A_n + B_n = o_{\mathcal{P}}(1)$.*

Claim B.9. *Let $(W_i)_{i\in\mathbb{N}}$ be i.i.d copies of $W \sim \mathrm{Lap}(0, \sigma)$. Let $S_n = \max_{i\in[n]} |W_i|$. Then $\mathbb{E}[S_n] \leq \sigma(1 + \ln n)$.*

Proof. If $W_i \sim \mathrm{Lap}(0, \sigma)$, then $|W_i| \sim \mathrm{Exponential}(\sigma^{-1})$. It is a known fact that $\mathbb{E}[\max |W_1|, \ldots, |W_n|] = \sigma \cdot H(n)$, where $H(n)$ is the harmonic number $H(n) = \sum_{i=1}^{n} 1/i$. The claim follows from the fact that $H(n) \leq \ln(n) + 1$. □

Claim B.10. *Let A and B be random variables and $p > 1$. Then $\mathbb{E}[|A + B|^p] \leq 2^{p-1}(\mathbb{E}[|A|^p] + \mathbb{E}[|B|^p])$.*

Claim B.11. *Let $W \sim \mathrm{Laplace}(0, \sigma)$. Then for $n \in \mathrm{N}$ we have $\mathbb{E}[|W|^n] = \frac{n!}{\sigma^n}$.*

Proof. This claim follows from the fact that $|W| \sim \mathrm{Exponential}(\sigma^{-1})$. □

C Proofs of Section 3

Lemma 3.2. (Sensitivity of the score function). *Let $\{T_i\}_{i\in[0,m]}$ be the values of $m + 1$ queries of sensitivity at most Δ_T on a dataset $\mathbf{D}$. Let $\{T'_i\}_{i\in[B]}$ be the values of the same queries on a neighboring dataset $\mathbf{D}'$. Let $Q_0, \ldots, Q_m$ (respectively $Q'_0, \ldots, Q'_m$) denote the values $\{T_i\}_{i\in[0,m]}$ (respectively $\{T'_i\}_{i\in[0,m]}$) sorted in decreasing order. Then $|Q_c - Q'_c| \leq \Delta_T$ for all $c \in [0, m]$. As a result, the score function $s_k(c, \mathbf{D})$ has sensitivity at most 1 for all $c \in [0, m]$.*

Proof. Fix $c \in [0, m]$. First, we bound the sensitivity of Q_c. Suppose by contradiction that $|Q_c - Q'_c| > \Delta_T$. Consider the case when $Q_c > Q'_c$. Then $Q_c > Q'_c + \Delta_T$. Let $\texttt{Above}_c = \{i \in [0, m] \mid T_i \geq Q_c\}$. Define $\texttt{Above}'_c$ similarly. Then, for all $i \in \texttt{Above}_c$, we have

$$T'_i \geq T_i - \Delta_T \geq Q_c - \Delta_T > Q'_c, \tag{12}$$

where the first inequality holds since the values T_i have sensitivity at most Δ_T, the second inequality holds from $i \in \texttt{Above}_c$, and the last inequality holds from our assumption by contradiction. Thus $i \in \texttt{Above}'_c$, and as a result $\texttt{Above}_c \subseteq \texttt{Above}'_c$. Moreover, for j such that $T'_j = Q'_c$ we have that $j \notin \texttt{Above}_c$ since it does not satisfy (12). Therefore $|\texttt{Above}'_c| > |\texttt{Above}_c|$, a contradiction.

For the case when $Q_c < Q'_c$ we obtain a contradiction by a symmetric argument. This concludes the proof on the sensitivity of Q_c. Next, we bound the sensitivity of the score function. We have,

$$|s_k(c, \mathbf{D}) - s_k(c, \mathbf{D})| \leq \frac{\Big||Q_c - T_k| - |Q'_c - T'_k|\Big|}{2\Delta_T} \leq \frac{|Q_c - Q'_c| + |T_k - T'_k|}{2\Delta_T}.$$

We just showed that $|Q_c - Q'_c| \leq \Delta_T$. Since the queries T_i have sensitivity at most Δ_T, we also have $|T_k - T'_k| \leq \Delta_T$. We obtain that $|s(c, \mathbf{D}) - s(c, \mathbf{D})| \leq 1$ for all neighboring datasets $\mathbf{D}, \mathbf{D}'$. □

Lemma 3.5. (Sensitivity of T). *Consider two neighboring datasets $\mathbf{D} = (\mathbf{X}^{(0)}, \ldots, \mathbf{X}^{(m)}, \mathbf{Y}, \mathbf{Z})$ and $\mathbf{D}' = (\mathbf{X}'^{(0)}, \ldots, \mathbf{X}'^{(m)}, \mathbf{Y}', \mathbf{Z}')$. For $j \in [0, m]$, let $T_j = T(\mathbf{X}^{(j)}, \mathbf{Y}, \mathbf{Z})$. Define T'_j analogously. If $|y_i|, |y'_i| \leq 1$ for all $i \in [n]$ and $|r^{(j)}_{X,i}|, |r'^{(j)}_{X,i}| \leq 1$[8] for all $i \in [n], j \in [0, m]$, then $|T_j - T'_j| \leq C'$, where $C' = 4 \cdot (1 + \frac{\sqrt{2}}{\sqrt{\lambda}} + \frac{2\sqrt{2}}{\lambda^{3/2}} + \frac{2}{\lambda})$.*

Proof. Suppose that $\mathbf{D}$ and $\mathbf{D}'$ differ in the last row. In the following, we assume that $j \in [m]$ is fixed. To ease notation, we remove the superscript (j) from all $r^{(j)}_{X,i}, r^{(j)}_{Y,i}$ and $R^{(j)}_i$. Since we know $\mathbb{E}[X \mid Z]$ exactly, we have $r_{X,i} = x_i - \mathbb{E}[X \mid Z = z_i]$ for $i \in [n], j \in [m]$. Then for $i \in [n]$ we have

$$|r_{X,i} - r'_{X,i}| = |(x_i - \mathbb{E}[X \mid Z = z_i]) - (x'_i - \mathbb{E}[X \mid Z = z'_i])|.$$

If $i \in [n-1]$, then $x_i = x'_i$ and $z_i = z'_i$, so that $|r_{X,i} - r_{X,i}| = 0$. For $i = n$, we have $|r_{X,n} - r_{X,n}| \leq 2$ by the triangle inequality and since $|r_{X,n}| \leq 1$.

Let $c_1 = 2 + \frac{2\sqrt{2}}{\sqrt{\lambda}}$ and $c_2 = \frac{8\sqrt{2}}{\lambda^{3/2}} + \frac{8}{\lambda}$. Turning to the residuals of fitting $\mathbf{Y}$ to $\mathbf{Z}$, by the same argument as in Lemma 2.3 we have, for all $i \in [n-1]$,

$$|r_{Y,i} - r'_{Y,i}| \leq \frac{8\sqrt{2}}{\lambda^{3/2} n} + \frac{8}{\lambda n} = \frac{c_2}{n}.$$

For the last datapoint it holds

$$|r_{Y,n} - r'_{Y,n}| \leq 2 + \frac{2\sqrt{2}}{\sqrt{\lambda}} + \frac{8\sqrt{2}}{\lambda^{3/2} n} + \frac{8}{\lambda n} = c_1 + \frac{c_2}{n}.$$

Additionally, $|r_{Y,i}| \leq c_1/2$ for all $i \in [n]$.

We can now bound the sensitivity of the residual products $R_i = r_{X,i} r_{Y,i}$. For $i \in [n-1]$, we have

$$|R_i - R'_i| \leq |r_{X,i}|||r_{Y,i} - r'_{Y,i}| + |r'_{Y,i}||r_{X,i} - r'_{X,i}| \leq \frac{c_2}{n} + 0.$$

For $i = n$ we have

$$|R_n - R'_n| \leq \left(c_1 + \frac{c_2}{n}\right) + \frac{c_1}{2} \cdot 2 = 2c_1 + \frac{c_2}{n}.$$

Finally,

$$|T_j - T'_j| = \Big|\sum_{i=1}^{n} R_i - \sum_{i=1}^{n} R'_i\Big| \leq \sum_{i=1}^{n} |R_i - R'_i| \leq (n-1) \cdot \frac{c_2}{n} + 2c_1 + \frac{c_2}{n} = 2c_1 + c_2.$$

□

[8]The bound of 1 can be replaced by any constant.

Theorem 3.7. PrivCRT *is ε-DP and (γ, δ)-accurate for* $\gamma = O\left(\frac{1}{\varepsilon}\log\left(\frac{m}{\delta}\right)\right)$.

Proof. We first show that PrivCRT is ε-differentially private. The scores $T_i, i \in [0, m]$ have sensitivity at most $\Delta_T = O(1)$ by Lemma 3.5. Therefore, the scores $s_i, i \in [0, m]$ have sensitivity at most 1 by Lemma 3.2. Finally, by Theorem 3.3 we have that outputting $\hat{c}$ is ε-DP. Therefore, PrivCRT is ε-DP. Note that if the regularization parameter λ is chosen adaptively based on the data, then obtaining the value of the constant C' by plugging in λ might not be ε-differentially private. This can be resolved by setting an a priori lower bound on λ, independent of the data, e.g., $\lambda \geq 1$, and plugging that lower bound to obtain C'.

Next, we analyze the accuracy of PrivCRT. Let c^* be the true rank of T_0 amongst the statistics $\{T_i\}_{i\in[0,m]}$, sorted in decreasing order. Then $p^* = (1 + c^*)/(m + 1)$. Note that $s_{c^*} = 0$. By Theorem 3.3, with probability at least $1 - \delta$, it holds

$$s_{\hat{c}} \geq -\frac{2\log(m/\delta)}{\varepsilon}.$$

As a result,

$$|Q_{\hat{c}} - T_0| = -2\Delta_T \cdot s_{\hat{c}} \leq \frac{4\Delta_T \log(m/\delta)}{\varepsilon}.$$

Let $\gamma = \frac{4\Delta_T \log(m/\delta)}{\varepsilon}$. The rank c^* of T_0 cannot differ from $\hat{c}$ by more than G_γ, since $Q_{\hat{c}}$ is within distance γ of T_0. Therefore, $|\hat{p} - p^*| \leq \frac{G_\gamma}{m+1}$, and since $\Delta_T = O(1)$, we obtain the desired result. □

D Additional Experimental Details and Results

Example Dataset. In Fig. 6 we show one example dataset from our simulations. We fit a kernel ridge regression model of X to Z. As can be observed, the model we fit matches $\mathbb{E}[X|Z]$ closely.

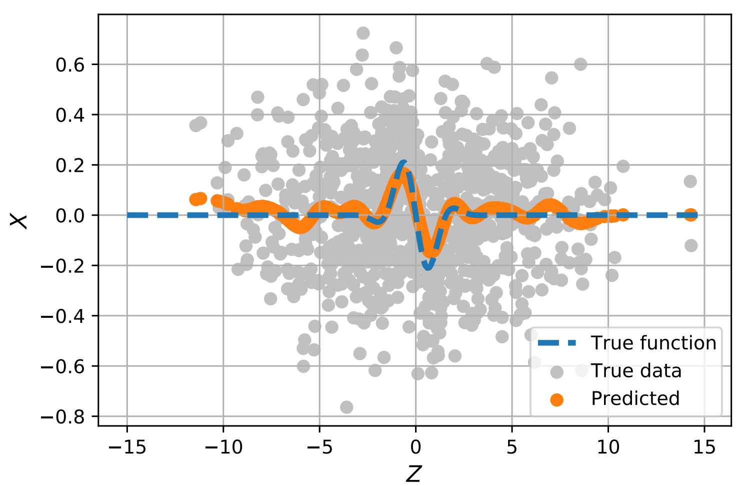

Figure 6: Values of X and Z (after rescaling) of one sampled dataset from our simulations, with $n = 1000$, $\beta = 0$, $s = 2$, $d = 1$. A kernel ridge regression model is fitted to the data. The model we fit closely matches $\mathbb{E}[X|Z]$.

Implementation of Private Kendall and PrivToT. The implementation of PrivToT requires setting a parameter k for the number of subsets into which the original dataset is divided. We use $k = 10$ for the experiments in Fig. 1. We additionally experimented with $k \in [20, 50, 100]$ and found that $k = 10$ performs the best in terms of type-I error. The implementation of PrivToT was adapted from the implementation of Kazan et al. [2023]. The private Kendall test works for categorical Z. To adapt it to continuous Z we apply k-means clustering to Z to obtain 100 clusters. The implementation of private Kendall was adapted from Wang et al. [2018].

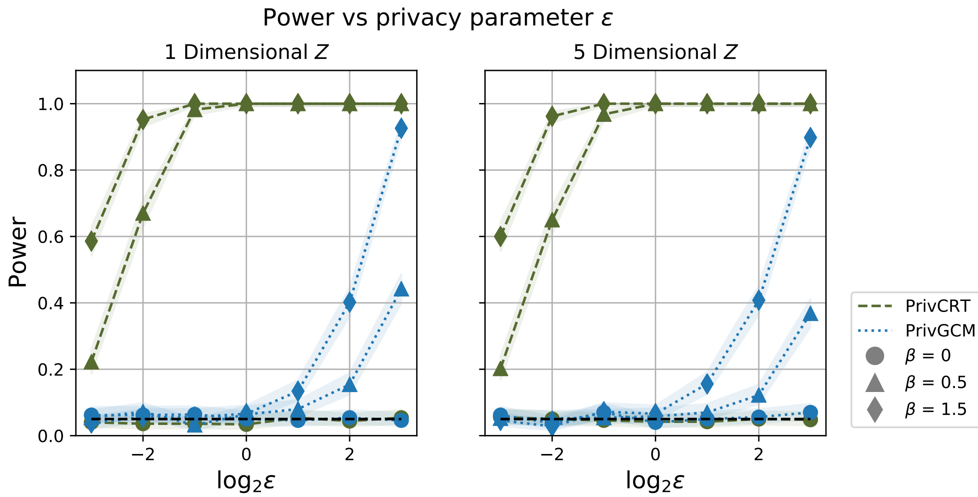

Figure 7: Power of PrivCRT and PrivGCM versus privacy ε.

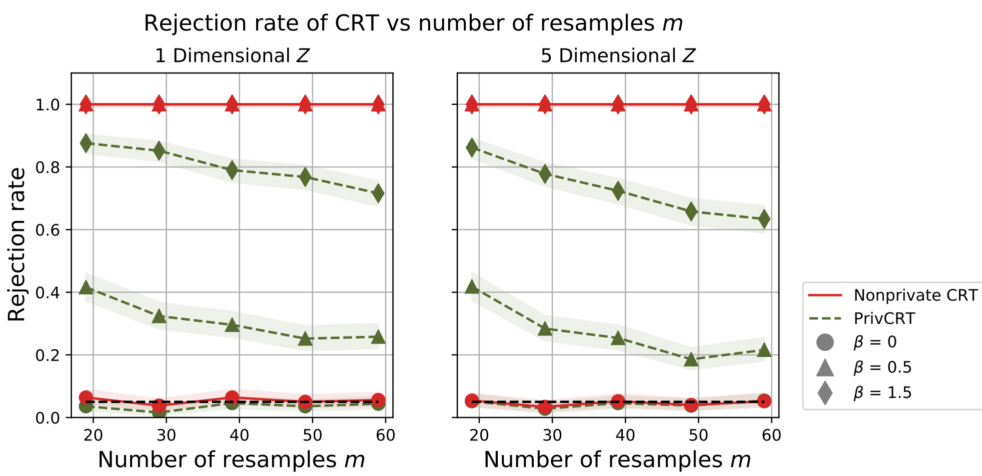

Figure 8: Effect on the power of PrivCRT with increasing m.

PrivCRT vs. PrivGCM. In Fig. 7 we compare the performance of PrivCRT with PrivGCM for different privacy parameters $\varepsilon \in [2^{-3}, 2^3]$. We set $n = 10^4$ and, for PrivCRT, $m = 19$. Both tests control type-I error, but PrivCRT achieves better power than PrivGCM for all privacy parameters ε. Therefore, PrivCRT appears preferable to PrivGCM when dataholders have access to the distribution $X \mid Z$. This result is consistent with the non-private scenario where the CRT has higher power because it does not have to learn $\mathbb{E}[X \mid Z]$.

The Effect of Varying m on the Power of PrivCRT. In Fig. 8, we vary m, the number of resamples used in the CRT algorithm and run our experiments for $\beta \in \{0, 0.5, 1.5\}$. We set $n = 10^3$ and $\varepsilon = 2$. Increasing m does not affect the type-I error control of PrivCRT. However, we observe that the power of PrivCRT decreases as the number of resamples m increases. This is due to the increase of the variable G_γ with m (see Definition 3.6). More specifically, for a fixed γ, as m increases, T_0 stays fixed, while the number of other statistics T_i within distance γ of T_0 increases. Thus, the private test is more likely to select a rank that is further from the true rank. It is an interesting open question whether the dependence on m in the accuracy of a private CRT test is avoidable. For now, we recommend using $m = O(1/\alpha)$ when employing PrivCRT.

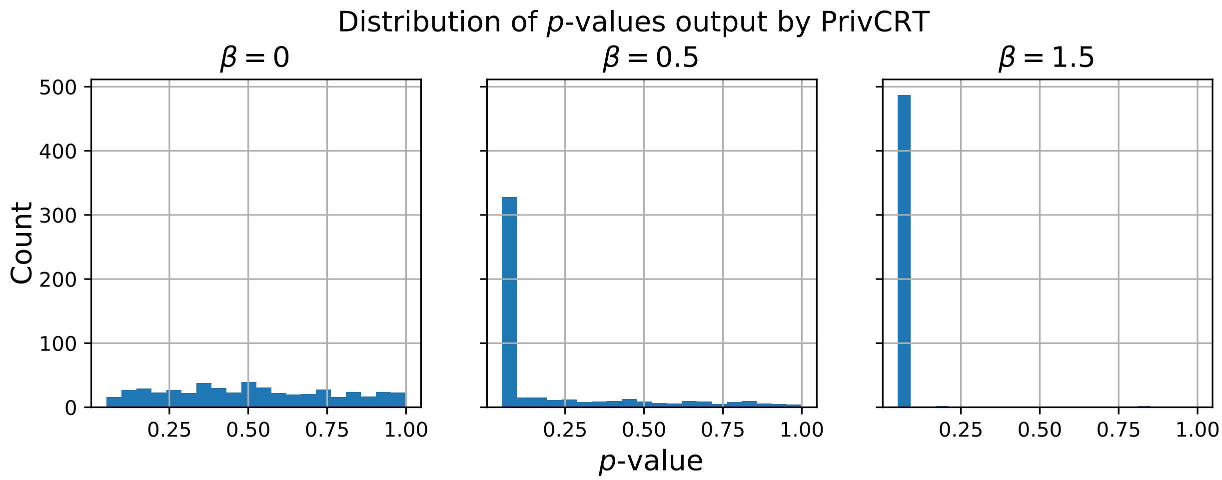

Figure 9: Distribution of p-values output by PrivCRT for different dependence strengths β under the setup in Section 4. Under the null, i.e., $\beta = 0$, the p-values are uniformly distributed as desired.

Distribution of p-values Output by PrivCRT. In Fig. 9 we show the distribution of the p-values output by PrivCRT for different dependence strengths β. We set $n = 10^3$, $m = 19$, and $\varepsilon = 2$. Under the null, i.e., when $\beta = 0$, the p-values output by PrivCRT are uniformly distributed in the interval $[\frac{1}{m+1}, 1]$. Thus, PrivCRT controls type-I error. When $\beta > 0$, most of the p-values are close to $\alpha = 0.05$, which is the desired outcome for PrivCRT to achieve power.