Differentially Private Conformal Prediction via Quantile Binary Search

Anonymous authors
Paper under double-blind review

Abstract

Differentially Private (DP) approaches have been widely explored and implemented for a broad variety of tasks delivering corresponding privacy guarantees in these settings. While most of these DP approaches focus on limiting privacy leakage from training data, there are fewer approaches that consider leakage when procedures involve *calibration data* which is common in uncertainty quantification through Conformal Prediction (CP). Since there is a limited amount of approaches in this direction, in this work we deliver a general DP approach for CP that we call Private Conformity via Quantile Search (P-COQS). The proposed approach adapts an existing randomized binary search algorithm for computing DP quantiles in the calibration phase of CP thereby guaranteeing privacy of the consequent prediction sets. This however comes at a price of marginally under-covering with respect to the desired $(1-\alpha)$-level when using finite-sample calibration sets (although broad empirical results show that the P-COQS generally targets the required level in the considered cases). Confirming properties of the adapted algorithm and quantifying the approximate coverage guarantees of the consequent CP, we conduct extensive experiments to examine the effects of privacy noise, sample size and significance level on the performance of P-COQS compared to existing alternatives. In addition, we empirically evaluate our approach on several benchmark datasets, including CIFAR-10, ImageNet and CoronaHack. Our results suggest that the proposed method is robust to privacy noise and performs favorably with respect to the current DP alternative in terms of *empirical coverage*, *efficiency*, and *informativeness*. Specifically, the results indicate that P-COQS produces smaller conformal prediction sets while simultaneously targeting the desired coverage and privacy guarantees in all these experimental settings.

1 Introduction

In high-stakes domains such as health care, criminal justice and financial risk assessment (among others) machine learning models are increasingly being used to guide decision-making processes. These approaches are commonly built to produce single-point predictions without quantifying uncertainty, which could lead to overconfident and unreliable outcomes with negative consequences for the following decisions. Many uncertainty quantification techniques have been proposed to address the need for reliable uncertainty quantification, including (but not limited to) Bayesian neural networks, ensemble methods, and dropout-based approximations (see e.g. Blundell et al., 2015; Lakshminarayanan et al., 2017; Osband et al., 2016; Gal & Ghahramani, 2016; Kendall & Gal, 2017). While these methods can offer meaningful uncertainty estimates, they often rely on strong modeling assumptions, are computationally intensive, or lack rigorous coverage guarantees (especially under model misspecification or when applied out-of-distribution). Conformal Prediction (CP) addresses various of these limitations by generating *prediction sets*, that is, subsets of the response space $\mathcal{Y}$ that, under the assumption of exchangeability, are guaranteed to contain the true response with a user-specified probability $1-\alpha$, where $\alpha \in (0,1)$. These sets provide a reliable and model-agnostic framework for uncertainty quantification, making them increasingly attractive in safety-critical applications (see e.g. Uddin & Lofstrom, 2023; Astigarraga et al., 2025; Tuwani & Beam, 2023; Olsson et al., 2022). While conformal methods require independent and identically distributed (iid) data for exact guarantees, recent

extensions have begun to explore how to adapt them to distribution shift settings with approximate validity (see e.g. Tibshirani et al., 2019; Gibbs & Candès, 2021; Jonkers et al., 2024).

However, while CP provides statistical reliability, its reliance on calibration data introduces privacy risks since any publicly released statistic based on these data could be exploited by an adversary. Moreover, when training models on data that collect individual-level information, these models tend to preserve individual-specific information, and some of them, such as deep neural networks, are known to *memorize* training examples (Fredrikson et al., 2015; Carlini et al., 2021), enabling adversaries to extract sensitive information via model inversion (Fredrikson et al., 2015) or membership inference attacks (Shokri et al., 2017). This poses a significant challenge also in regulated domains (e.g., under GDPR, HIPAA, or CCPA), where models must not leak information about individuals in the training or calibration sets. To address these issues, Differential Privacy (DP) (Dwork, 2006) has emerged as one of the main frameworks for privacy-preserving machine-learning, ensuring (with high probability) that model outputs do not reveal whether any individual's data was included in the training set. However, existing DP frameworks focus primarily on protecting the *training* phase, leaving the calibration phase (and thus the CP step) vulnerable to privacy breaches. Given this issue, there are nevertheless very few existing approaches that ensure that CP procedures can provide DP guarantees while maintaining reasonable performance in terms of uncertainty quantification metrics and computational efficiency (see Angelopoulos et al., 2022). Hence, this work aims to further contribute to the goal of uncertainty quantification under privacy constraints by adapting an existing DP quantile selection approach based on binary search (Huang et al., 2021) and using it as a subroutine to deliver CP sets that guarantee privacy. We confirm the theoretical properties of the resulting CP procedure and highlight its favorable experimental performance compared to the few existing alternatives, both in terms of uncertainty quantification and computational efficiency.

2 Related Work

The idea behind CP was first described in Vovk et al. (2005) followed by different papers that developed its theory and applications (see Vovk (2015), Vovk (2002), Vovk et al. (2017), Vovk & Petej (2012), and the references therein). Based on these, considerable attention has been paid in recent years to adapt CP to different settings and deliver additional applied and theoretical results (see Angelopoulos & Bates (2021) for a recent detailed review). Despite these different research outputs, little attention has been devoted to guaranteeing privacy for the calibration data through protection of the derived *non-conformity scores* used to deliver the prediction sets for uncertainty quantification. To the best of the authors' knowledge, the only existing work related to the central DP approach we present in this paper is that of Angelopoulos et al. (2022) where they privatize the CP procedure by discretizing the non-conformity scores into bins and applying the *exponential mechanism* (McSherry & Talwar, 2007) to select a DP quantile which is then used to form the prediction sets. More specifically, to maintain coverage guarantees under ϵ-DP, the target quantile is adjusted (inflated) to account for added noise. This ensures both privacy (via DP) and valid coverage, albeit with potentially larger prediction sets due to the privacy-utility trade-off. A possible practical limitation of this proposed approach lies in the choice of the optimal number of bins, as well as a hyperparameter that needs to be tuned to minimize the inflated quantile to achieve the smallest possible prediction set. Although procedures have been determined to compute these in an optimal manner, they can potentially increase the time complexity of this method. In recent years there have been few other CP approaches proposed in the setting of federated learning (Humbert et al., 2023) and *local DP* (Penso et al., 2025), however, these do not fit in the central DP framework of this paper.

3 Preliminaries

3.1 Conformal Prediction

To define the framework of the proposed method, let us consider n exchangeable data points $\mathcal{D} = \{(X_1, Y_1), \ldots, (X_n, Y_n)\}$ with $X_i \in \mathcal{X}^d$ being a d-dimensional input vector and $Y_i \in \mathcal{Y}$ being the target variable. Using the basic *split* CP (Papadopoulos et al., 2002; Lei et al., 2015), we can partition these points into a training set with n_{train} observations (to fit a model of choice f) and a calibration set with

$n_{\text{cal}} = n - n_{\text{train}}$ observations to quantify prediction uncertainty (assuming test data is taken from another sample). If we let $\mathcal{I} = \{1, \ldots, n\}$ represent the index set of the observations, then we can define $\mathcal{I}_{\text{cal}} \subset \mathcal{I}$ as the index set of observations in the calibration set. Assuming that we have trained a model $\hat{f}$ on the training set, the goal of CP is to compute *non-conformity scores* $s_i = s(X_i, Y_i, \hat{f})$ for each calibration point (X_i, Y_i), $\forall\, i \in \mathcal{I}_{\text{cal}}$. These scores measure the discrepancy between the model's prediction and the true target value such that lower scores suggest better agreement, that is, better predictions from the trained model $\hat{f}$. Therefore we now have a set of non-conformity scores $\mathcal{S} = \{s_1, \ldots, s_{\text{cal}}\}$ on which we can obtain α-quantiles with $\alpha \in (0, 1)$ being the significance level which represents the amount of errors (in percentage) that the model is allowed to make. We denote this quantile as q and let its dependence on the significance level α be implicit. Once the scores are computed, we can therefore sort them in increasing order (that is, $\{s_{[1]} \leq \ldots \leq s_{[n_{\text{cal}}]}\}$) and estimate this quantile by selecting the score in the rth position where we define $r = \lceil (1-\alpha)(n_{\text{cal}}+1) \rceil$, with $\lceil v \rceil$ representing the smallest integer greater than x, leading to $\hat{q} = s_{[r]}$. Suppose that we now have a new test data point X_{test}, the resulting prediction set for the target Y_{test} is defined as:

$$\mathcal{C}(X_{\text{test}}) = \left\{ Y \in \mathcal{Y} : s(X_{\text{test}}, Y, \hat{f}) \leq \hat{q} \right\}.$$

Under the assumption of exchangeability of the data points, this set guarantees the coverage probability $\mathbb{P}(Y_{\text{test}} \in \mathcal{C}(X_{\text{test}})) \geq 1 - \alpha$, where the probability is taken over the $n + 1$ data points $(X_1, Y_1), \ldots, (X_n, Y_n), (X_{\text{test}}, Y_{\text{test}})$. For further details and extensions we refer the reader to Angelopoulos & Bates (2021).

3.2 Differential Privacy

Differential Privacy (DP) currently represents one of the main frameworks for privacy protection with mathematically provable guarantees. More in detail, a randomized mechanism $\mathcal{M}$ is said to be (ϵ, δ)-DP if, for all neighboring datasets $\mathcal{D}$ and $\mathcal{D}'$ (that is, datasets with Hamming distance $\Delta(\mathcal{D}, \mathcal{D}') = 1$) and for all measurable subsets $\mathcal{Q}$ of the output space, we have that

$$\mathbb{P}[\mathcal{M}(\mathcal{D}) \in \mathcal{Q}] \leq e^{\epsilon} \mathbb{P}[\mathcal{M}(\mathcal{D}') \in \mathcal{Q}] + \delta.$$

There are many variations of this framework, including Gaussian Differential Privacy which benefits from a series of nice additional properties compared to the above (ϵ, δ)-DP (Dwork, 2006; Dong et al., 2022). For the purpose of this work, we rely on a specific version of DP defined below.

Definition 1 (Zero-Concentrated Differential Privacy, Bun & Steinke (2016))**.** *For $\rho > 0$, a randomized mechanism $\mathcal{M}$ satisfies $(\rho, 0)$-Zero-Concentrated Differential Privacy (zCDP) if for all neighboring datasets $\mathcal{D}$ and $\mathcal{D}'$ and for all $\eta > 1$, the Rényi divergence D of order η satisfies:*

$$D_{\eta}(\mathcal{M}(\mathcal{D}) \| \mathcal{M}(\mathcal{D}')) \leq \rho\eta.$$

Unlike (ϵ, δ)-DP, ρ-zCDP is *tight* under sequential composition without the need for the *advanced composition theorem*, which may consume extra privacy budget. Nevertheless, there is a direct relationship between the (ϵ, δ)-DP framework and the zCDP framework: indeed, if $\mathcal{M}$ satisfies ρ-zCDP, then for $\delta > 0$, $\mathcal{M}$ satisfies (ϵ, δ)-DP with $\epsilon = \rho + 2\sqrt{\rho \log(1/\delta)}$ (see Near & Abuah, 2021). Hence, the latter implies the former. In particular, a randomized mechanism $\mathcal{M}$ satisfies $(\epsilon, 0)$-DP if and only if it satisfies ϵ-zCDP (Bun & Steinke, 2016).

4 P-COQS: Private Conformity via Quantile Search

As highlighted in Angelopoulos et al. (2022), the release of the non-conformity score quantile $\hat{q}$ or of the prediction sets based on this quantile can compromise the privacy of individuals in the calibration set. Therefore, a solution to this problem is to directly release a DP quantile or its corresponding prediction sets, which would also preserve DP based on the privatized quantile. While the existing alternative in Angelopoulos et al. (2022) employs the exponential mechanism to sample a DP quantile, this work relies on a direct adaptation of the DP binary search algorithm presented in Huang et al. (2021). More specifically,

the latter algorithm releases a DP quantile by employing a noisy count function (denoted as `NoisyRC`) within a binary search procedure run on a sequence of ordered integers. In particular, the function `NoisyRC`$([a, b], \mathcal{G})$ returns a noisy count of $\mathcal{G} \cap [a, b]$, where $\mathcal{G}$ is a set containing ordered integers that are considered sensitive and hence must be accessed privately (see Huang et al., 2021). However, since in this work our sequences are not integers (given that the non-conformity scores are continuous), we adapt this DP quantile selection approach in a straightforward manner and, for completeness, we reproduce their adapted approach in Algorithm 1 with some modification to suit our application.

Algorithm 1 Adapted `PrivQuant` Algorithm of Huang et al. (2021)

Require: Non-conformity scores $\mathcal{S} = \{s_1, \ldots, s_{n_{\text{cal}}}\}$, significance level $\alpha \in (0, 1)$, lower and upper bounds for non-conformity scores $[a, b]$, $\delta > 0$ (small positive value, default $\delta = 10^{-10}$), privacy parameter ρ

Ensure: DP quantile q^{DP}

Fix $r = \lceil (1 - \alpha)(n_{\text{cal}} + 1) \rceil$ and $N = \lceil \log_2 ({}^{b-a}/_{\delta}) \rceil$
Initialize: left $\leftarrow a$, right $\leftarrow b$, $i \leftarrow 0$
while $i < N$ **do**
    mid $\leftarrow \frac{\text{left}+\text{right}}{2}$
    $c \leftarrow$ `NoisyRC`$([a, \text{mid}], \mathcal{S})$
    if $c < r$ **then**
        left $\leftarrow$ mid $+ \delta$
    else
        right $\leftarrow$ mid
    end if
    $i \leftarrow i + 1$
end while
return $q^{\text{DP}} = \frac{\text{left}+\text{right}}{2}$

Broadly speaking, Algorithm 1 performs a binary search over the interval $[a, b]$ (often corresponding to $[0, 1]$ in the case of classification tasks) by iteratively narrowing the search space to localize the quantile of interest while preserving privacy through a randomized counting mechanism. More specifically, at each iteration, the algorithm evaluates a midpoint and calls the function `NoisyRC`, which returns a DP count of the number of non-conformity scores (in $\mathcal{S}$) less than or equal to the midpoint. This count guides the search by indicating whether the true quantile lies to the left or right of the midpoint. The process continues until it reaches iteration N which is the maximum number of iterations allowed to ensure ρ-zCDP. Indeed, as stated further on, the DP noise used for the function `NoisyRC` needs to be scaled to the number of iterations in Algorithm 1. Since we would ideally want the algorithm to terminate when the interval length is smaller than a small value δ (i.e. right $-$ left $\leq \delta$), the fixed number of iterations N needed to reach this point is such that ${}^{b-a}/_{2^N} \leq \delta$ (since the interval is divided by two after each iteration) which, solving for N, gives us

$$N = \lceil \log_2 ({}^{b-a}/_{\delta}) \rceil.$$

With this representing the exact number of iterations to guarantee the required condition, Algorithm 1 returns the midpoint as the private quantile estimate q^{DP}. Once this quantile is obtained, following the definition in Section 3.1, the DP conformal prediction set is simply given by:

$$\mathcal{C}^{DP}(X_{\text{test}}) = \left\{ Y \in \mathcal{Y} : s(X_{\text{test}}, Y, \hat{f}) \leq q^{DP} \right\}. \tag{1}$$

We refer to the above procedure as Private Conformity via Quantile Search (P-COQS) which therefore is built on the adaptation described in Algorithm 1 and the consequent use of the resulting DP quantile q^{DP} in equation 1. The entire P-COQS procedure is summarized in Algorithm 2.

Let us now focus on the properties of P-COQS and, for completeness, we start by studying the error bound and DP properties of Algorithm 1 which directly follow from the properties of the `PrivQuant` algorithm in Huang et al. (2021). Indeed, while the latter algorithm is tailored to search over positive integers, as mentioned earlier, Algorithm 1 adapts the latter to any ordered data type and any set of bounds $[a, b]$ on

Algorithm 2 P-COQS

Require: Training data $\mathcal{D}_{\text{train}} = \{(X_1, Y_1), \ldots, (X_{n_{\text{train}}}, Y_{n_{\text{train}}})\}$, calibration data $\mathcal{D}_{\text{cal}} = \{(X_1, Y_1), \ldots, (X_{n_{\text{cal}}}, Y_{n_{\text{cal}}})\}$, test point X_{test}, significance level $\alpha \in (0, 1)$, bounds $[a, b]$, resolution $\delta > 0$, privacy parameter ρ

Ensure: DP prediction set $\mathcal{C}^{\text{DP}}$

1: Train model on $\mathcal{D}_{\text{train}}$ to obtain $\hat{f}$
2: Compute non-conformity scores $\mathcal{S} = \{s_1, \ldots, s_{n_{\text{cal}}}\}$ from $\mathcal{D}_{\text{cal}}$ using $\hat{f}$
3: Run Algorithm 1 to obtain q^{DP}
4: Define $\mathcal{C}^{DP}(X_{\text{test}}) = \{Y \in \mathcal{Y} : s(X_{\text{test}}, Y, \hat{f}) \leq q^{DP}\}$
5: **return** $\mathcal{C}^{DP}$

the real line. Let us therefore discuss (confirm) the DP properties of this adaptation and, to do so, let us first define the noisy count function as

$$\texttt{NoisyRC}([a, \text{mid}], \mathcal{S}) = \texttt{card}\big(\mathcal{S} \cap [a, \text{mid}]\big) + \mathcal{N}\left(0, \frac{\lceil \log_2(b-a/\delta) \rceil}{2\rho}\right), \tag{2}$$

where $\rho > 0$ is the privacy parameter under zCDP, with the sensitivity scaled to the maximum number of iterations N for Algorithm 1 (considering that count query l_1-sensitivity is 1), and `card` denotes the cardinality of set. Let us now denote $u = {}^{b-a}/\delta$ and let Φ represent the standard normal CDF. Then, adapting directly from Huang et al. (2021), the following proposition holds.

Proposition 1. *Algorithm 1 using the noisy count function in equation 2 is ρ-zCDP and, with probability at least $1 - \beta$, returns a quantile with rank error τ satisfying*

$$\tau \leq \sqrt{\frac{\lceil \log_2(u) \rceil}{\rho} \log\left(\frac{2\lceil \log_2(u) \rceil}{\beta}\right)}.$$

Proof. Since the sensitivity of the range query $\texttt{card}(\mathcal{S} \cap [a, \text{mid}])$ is 1, adding Gaussian noise $\mathcal{N}\left(0, \frac{N}{2\rho}\right)$ guarantees ρ/N-zCDP per call, where $N = \lceil \log_2(u) \rceil$. By composition (Bun & Steinke, 2016), after N calls the whole algorithm satisfies ρ-zCDP. Now, let $W \sim \mathcal{N}(0, \sigma^2)$ with $\sigma^2 = N/(2\rho)$. Then the error between the true count and its noisy version is distributed as W. For one call we have that

$$\Pr\big(|W| > \tau\big) \leq 2e^{-\tau^2/(2\sigma^2)}.$$

Applying a union bound over N calls we consequently have

$$\Pr\Big(\exists\, i : |W_i| > \tau\Big) \leq 2Ne^{-\tau^2/(2\sigma^2)}.$$

To ensure this probability is at most β, it suffices that

$$\tau \geq \sigma\sqrt{2\log\left(\tfrac{2N}{\beta}\right)}.$$

Substituting $\sigma^2 = N/(2\rho)$ and $N = \lceil \log_2(u) \rceil$ gives the stated bound. □

Remark 1. *An equivalent (but slightly sharper) formulation avoids the union bound and uses the Gaussian quantile. In that case,*

$$\tau = \sigma\, \Phi^{-1}\left(1 - \tfrac{\beta}{2N}\right) = \sqrt{\tfrac{\lceil \log_2(u) \rceil}{2\rho}}\; \Phi^{-1}\left(1 - \tfrac{\beta}{2\lceil \log_2(u) \rceil}\right).$$

Remark 2. *Noting that $\lceil \log_2 u \rceil \leq \log_2 u + 1$, we have that*

$$\tau \;\leq\; \sqrt{\frac{\log_2 u + 1}{\rho} \log\left(\frac{2(\log_2 u + 1)}{\beta}\right)} \;=\; \sqrt{\frac{\log u}{\rho \log 2}\Big(\log\log u + O(1)\Big)}.$$

Therefore, with ρ, β fixed, as $u \to \infty$ (i.e. as $\delta \to 0$) we have that

$$\tau \;=\; \Theta\left(\sqrt{\frac{\log u \,\log\log u}{\rho}}\right),$$

which matches the polylogarithmic order in Huang et al. (2021) (near-optimal up to constants).

These results allow us to quantify to what extent the rank associated with the private quantile q^{DP} from Algorithm 1 differs from the non-private rank in the calibration data. Firstly, obtaining a ρ-zCDP quantile ensures that Algorithm 2 preserves the desired privacy level. Moreover, Proposition 1 allows us to explicitly define this difference τ with high probability (at least $1-\beta$). We will see that this information can be used and is indeed helpful when determining the coverage guarantees of P-COQS in Algorithm 2 which are stated in Theorem 1. For this purpose, we also define $s_{\text{test}} \;=\; s(X_{\text{test}}, Y, \hat{f})$.

Theorem 1 (Coverage Guarantee)**.** *Let $(s_1, \ldots, s_{n_{cal}}, s_{test})$ be an exchangeable sequence of non-conformity scores. With probability at least $1-\beta$ (over the DP noise in Algorithm 1), the P-COQS prediction set $\mathcal{C}^{DP}(X_{test})$ satisfies:*

$$1-\alpha-\frac{\tau}{n_{cal}+1} \le \mathbb{P}\big[Y_{test} \in \mathcal{C}^{DP}(X_{test})\big] \le 1-\alpha+\frac{\tau+1}{n_{cal}+1}.$$

Proof. By Proposition 1 we have that Algorithm 1 outputs a private quantile q^{DP} with rank error τ, i.e. $s_{(r-\tau)} \;\le\; q^{DP} \;\le\; s_{(r+\tau)}$. By the exchangeability condition of the non-conformity scores, the rank of $s_{\text{test}} = s(X_{\text{test}}, Y, \hat{f})$ among $(s_1, \ldots, s_{n_{\text{cal}}}, s_{\text{test}})$ is uniformly distributed over $\{1, \ldots, n_{\text{cal}}+1\}$. Thus, recalling that $r = \lceil (1-\alpha)(n_{\text{cal}}+1) \rceil$ and that

$$Y \in \mathcal{C}^{DP}(X_{\text{test}}) \iff s_{\text{test}} \le q^{DP},$$

we consequently have:

$$\underbrace{\frac{r-\tau}{n_{\text{cal}}+1}}_{L} \le \mathbb{P}\left(s_{\text{test}} \le q^{DP}\right) \le \underbrace{\frac{r+\tau}{n_{\text{cal}}+1}}_{U},$$

where:

$$L = \frac{\lceil (1-\alpha)(n_{\text{cal}}+1) \rceil - \tau}{n_{\text{cal}}+1} \ge 1-\alpha-\frac{\tau}{n_{\text{cal}}+1} \quad \text{and}$$
$$U = \frac{\lceil (1-\alpha)(n_{\text{cal}}+1) \rceil + \tau}{n_{\text{cal}}+1} \le \frac{(1-\alpha)(n_{\text{cal}}+1)+1+\tau}{n_{\text{cal}}+1} = 1-\alpha+\frac{\tau+1}{n_{\text{cal}}+1}.$$

Therefore this allows us to conclude that

$$1-\alpha-\frac{\tau}{n_{\text{cal}}+1} \le \mathbb{P}\left[Y_{\text{test}} \in \mathcal{C}^{DP}(X_{\text{test}})\right] \le 1-\alpha+\frac{\tau+1}{n_{\text{cal}}+1}.$$

□

Remark 3. *If ties occur in the above setting, one can either employ randomized tie-breaking, or can replace the lower bound by $1-\alpha-\frac{\tau+1}{n_{cal}+1}$ for a deterministic rule.*

Although Theorem 1 does not ensure the coverage probability $(1-\alpha)$, as opposed to the method in Angelopoulos et al. (2022) that preserves this standard CP guarantee, it establishes an approximate coverage bound with an error term of order $\mathcal{O}(\tau/n_{\text{cal}})$. While this indeed implies an error margin for the actual coverage, it nevertheless also provides an upper bound to the coverage guarantee which allows to understand how conservative and how efficient the resulting prediction sets can be (see e.g. Lei et al., 2018; Li et al., 2025). More in detail, this error depends not only on the size of the calibration set but also on the width of the interval $[a, b]$ and the privacy level ρ under zCDP. Specifically, as shown in Proposition 1, the coverage error increases with the length of the interval and decreases with the privacy budget. Therefore, achieving accurate coverage requires a sufficiently large calibration set when the parameters of the error bound τ are fixed. Nevertheless, all the experimental results in Section 5 indicate that P-COQS is able to achieve coverage comparable to the non-private conformal prediction method, despite this weaker theoretical guarantee.

Remark 4. *As highlighted by Huang et al. (2021), the quantile method adapted in Algorithm 1 is nearly optimal, implying that our results are suboptimal (polylogarithmic) in terms of CP guarantees. Nevertheless, using the bounds in Proposition 1, it delivers a practical way to determine the true differentially private coverage guarantee with high probability (i.e.* $1-\beta$*) without having to inflate the coverage to mitigate the impact of privacy noise (which can negatively impact the informativeness of the CP sets). For example, suppose that we are dealing with a classification task where the non-conformity scores lie in the interval* $[0,1]$*, then by fixing the other parameters* δ *and* ρ *(e.g.,* $\delta = 10^{-10}$ *and* $\rho = 0.1$*) and choosing* $\beta = 0.01$*, following Proposition 1 the true probability of DP coverage of P-COQS is at least* $1-\alpha-0.0183$ *and at most* $1-\alpha+0.0186$ *guaranteed with probability at least* $1-\beta = 0.99$ *and calibration size* $n_{cal} = 3000$*.*

5 Experiments

In this section, we evaluate the proposed CP approach (P-COQS) under the same experimental setting as Angelopoulos et al. (2022). Additionally, we extend this evaluation with controlled simulation experiments. Specifically, we compare P-COQS with the method introduced by Angelopoulos et al. (2022) (henceforth referred to as ExponQ), examining scenarios where both approaches employ either non-private models ($\hat{f}$) or DP models ($\hat{f}^{\text{DP}}$). For differentially private models, we train Naïve Bayes and Random Forest models using IBM's `Diffprivlib` library in Python,[1] ensuring pure ϵ-DP guarantees. For deep neural networks, we adopt the same methodology as Angelopoulos et al. (2022), utilizing the `Opacus` library to obtain (ϵ, δ)-DP models. For DP conformal prediction methods, we leverage the exact equivalence between ϵ-DP and $(\epsilon, 0)$-zCDP established in Lemma 3.2 of Bun & Steinke (2016). This allows us to analyze both P-COQS and ExponQ under either privacy framework while maintaining identical privacy guarantees. We specifically examine how these methods behave under varying privacy parameters (ϵ) and different sample sizes. Consistent with the experimental design of Angelopoulos et al. (2022), we restrict our investigation to classification tasks. The non-conformity measure we used is given by the *hinge loss* function:

$$s(x, y, \hat{f}) = 1 - \hat{f}(x)_y,$$

where $\hat{f}(x)_y$ represents the predicted probability of the model for the true class y. We evaluate the performance of CP methods using the metrics of coverage, efficiency and informativeness. Therefore, if a CP approach performs well, we expect (i) the coverage to be close to $1-\alpha$, (ii) the efficiency to be close to 1 from above, and (iii) the informativeness to be close to 1 from below. When comparing to the benchmark datasets considered in Angelopoulos et al. (2022), we employ their same experimental and parameters settings.

5.1 Simulated Data

We first consider a simple low-dimensional binary classification problem with eight features. The feature matrix for class 1 is sampled from a Gaussian $\mathcal{N}(\boldsymbol{\mu}_1, \boldsymbol{\Sigma}_1)$, with $\boldsymbol{\mu}_1 = [0.8, \ldots, 0.8]^T \in \mathbb{R}^8$ and $\boldsymbol{\Sigma}_1 = \mathbb{I} \cdot 7 \in \mathbb{R}^{8\times 8}$, while class 2 follows $\mathcal{N}(\boldsymbol{\mu}_2, \boldsymbol{\Sigma}_2)$ with $\boldsymbol{\mu}_2 = [-1, \ldots, -1]$ and $\boldsymbol{\Sigma}_2 = \mathbb{I} \cdot 8$, where $\mathbb{I}$ denotes the identity matrix. This setting delivers a reasonable overlap between the two classes and implies a slightly non-linear decision boundary due to the small difference in the covariance matrices. The generated data is class-balanced, with 60% used for the training set, 24% for the calibration set, and 16% reserved for evaluating CP performance. As for the models, we consider the two classifiers mentioned earlier: Naïve Bayes (NB) and Random Forest (RF) (we will see applications with deep neural networks in Section 5.2). In particular, in this section we will focus on CP performance when employing the DP versions of these models (i.e. $\hat{f}^{DP}$), whereas the results using the non-DP models $\hat{f}$ can be found in the appendix. This being said, we evaluate coverage, efficiency, and informativeness with a fixed privacy budget $\epsilon_f = 2$ when privatizing the models and repeat experimental runs $H = 1,000$ times in each setting (unless otherwise specified). Moreover, when varying one of the parameters to study the sensitivity of the methods, the other parameters are fixed at: $\epsilon_{CP} = 1$ (privacy budget for CP); $n = 10,000$ (total sample size to be split); $\alpha = 0.1$ (significance level for coverage). For clarity of presentation, here we only discuss the results for the NB classifier, while we provide the same results for the RF classifier in Appendices A and B.

[1] DP implementations based on IBM's Diffprivlib: `https://diffprivlib.readthedocs.io/en/latest/modules/models.html#classification-models`

5.1.1 Effect of CP Privacy Budget (ϵ_{CP})

We examine the sensitivity of both P-COQS and ExponQ to variations in the CP privacy parameter ϵ_{CP}, using a private NB model while maintaining a fixed sample size of $n = 10,000$. For the DP model (that achieves 75% accuracy), the results in Table 1 indicate that P-COQS shows significantly lower sensitivity to ϵ_{CP} compared to ExponQ, while comparing favorably to it over the different evaluation metrics across the considered privacy budgets. For smaller values of ϵ_{CP} however, the P-COQS does appear to have larger variability compared to ExponQ. Similar behavior is observed for the private RF model (see Table 8 in Appendix B.1) and also when using the non-DP variants of the NB and RF models reported in Table 13 and Table 5 respectively, where as expected, efficiency and informativeness results are slightly better for both approaches.

ϵ_{CP}	**Coverage**		**Efficiency**		**Informativeness**	
	ExponQ	**P-COQS**	**ExponQ**	**P-COQS**	**ExponQ**	**P-COQS**
0.1	1.0000 (0.0002)	0.9000 (0.0107)	1.9995 (0.0030)	1.3991 (0.0350)	0.0005 (0.0030)	0.6009 (0.0350)
0.5	0.9402 (0.0141)	0.8999 (0.0100)	1.5692 (0.0694)	1.3985 (0.0326)	0.4308 (0.0694)	0.6015 (0.0326)
1	0.9217 (0.0116)	0.8999 (0.0098)	1.4841 (0.0457)	1.3985 (0.0322)	0.5159 (0.0457)	0.6015 (0.0322)
1.5	0.9148 (0.0104)	0.9000 (0.0098)	1.4553 (0.0385)	1.3986 (0.0319)	0.5447 (0.0385)	0.6014 (0.0319)
3	0.9076 (0.0098)	0.9000 (0.0097)	1.4272 (0.0337)	1.3987 (0.0318)	0.5728 (0.0337)	0.6013 (0.0318)
5	0.9046 (0.0097)	0.8999 (0.0097)	1.4160 (0.0325)	1.3986 (0.0320)	0.5840 (0.0325)	0.6014 (0.0320)
10	0.9024 (0.0096)	0.8999 (0.0097)	1.4073 (0.0321)	1.3986 (0.0320)	0.5927 (0.0321)	0.6014 (0.0320)

Table 1: Average effect of CP privacy budget ϵ_{CP} on conformal prediction with DP Naïve Bayes model. The numbers are metric averages over $1,000$ runs (per method and privacy budget) and in parentheses is the corresponding variance of the metrics.

5.1.2 Sample Size Effect

We investigate the impact of sample size on the performance of the CP methods considered here. For each sample size, the sample is split as mentioned at the start of this section (i.e. 60% training, 24% calibration and 16% test). We recall that we discuss the results with the DP version of NB (see Appendix C.2 for the result of the non-DP model $\hat{f}$) and also recall that, as in other experiments, the privacy budget for the models is fixed at $\epsilon_f = 2$. The results in Table 2 show that in general P-COQS targets the correct $1 - \alpha$ coverage except in smaller sample settings (that is, $n \leq 200$) and overall performs well compared to ExponQ. More in detail, as discussed in the previous section, it can be seen how the sample size has an important effect on the P-COQS precision (measured in terms of metric variability) where, aside from visibly under-covering with respect to the $1 - \alpha$ target-level, smaller sample sizes show lower precision of P-COQS compared to ExponQ (similar conclusions hold for RF in Appendices B.2 and A.2). This confirms the observations and conclusions made from Theorem 1. Nevertheless, it can be observed that the P-COQS under-covering appears to be solved already starting from $n = 200$ and does not appear to be an issue when using a non-DP model (see Table C.2 in the Appendix). In addition, the variability of the P-COQS metrics tend to converge towards that of ExponQ (as also seen in the other simulation settings of this section).

5.1.3 Effect of Significance Level (α)

We examine the performance across varying α values (fixing $n = 10,000$, $\epsilon_f = 2$, and $\epsilon_{CP} = 1$). As seen in Table 3, P-COQS appears to better target the required coverage level on average, but has a higher variability than ExponQ in this metric with a small $\alpha = 0.01$ level. This variability then becomes in line with (or smaller than) that of ExponQ with larger values of α. With respect to the other metrics, the results indicate that P-COQS generally performs better than ExponQ with the variability of the performance in line with the latter (similar conclusions holds for the DP RF model in Appendix B.3 as well as when using non-DP NB and RF models in Appendices C.3 and A.3 respectively).

n	Coverage		Efficiency		Informativeness		Model Accuracy
	ExponQ	**P-COQS**	**ExponQ**	**P-COQS**	**ExponQ**	**P-COQS**	
100	0.9791 (0.0447)	0.8529 (0.1472)	1.9266 (0.1180)	1.5958 (0.3184)	0.0734 (0.1180)	0.4042 (0.3184)	0.5867 (0.1248)
200	0.9954 (0.0148)	0.9295 (0.0731)	1.9896 (0.0287)	1.8077 (0.1663)	0.0104 (0.0287)	0.1923 (0.1663)	0.5543 (0.1039)
500	0.9969 (0.0074)	0.9043 (0.0474)	1.9830 (0.0274)	1.6153 (0.1206)	0.0170 (0.0274)	0.3847 (0.1206)	0.6289 (0.0612)
1000	0.9994 (0.0034)	0.9296 (0.0544)	1.9963 (0.0147)	1.7446 (0.1858)	0.0037 (0.0147)	0.2554 (0.1858)	0.6266 (0.0478)
2000	0.9761 (0.0130)	0.9014 (0.0220)	1.8469 (0.0577)	1.5316 (0.0644)	0.1531 (0.0577)	0.4684 (0.0644)	0.6972 (0.0268)
6000	0.9340 (0.0178)	0.9185 (0.0414)	1.6877 (0.0859)	1.6216 (0.1890)	0.3123 (0.0859)	0.3784 (0.1890)	0.6949 (0.0227)
10000	0.9217 (0.0116)	0.8999 (0.0098)	1.4841 (0.0457)	1.3985 (0.0322)	0.5159 (0.0457)	0.6015 (0.0322)	0.7479 (0.0125)

Table 2: Average effect of sample size on private conformal prediction with DP Naïve Bayes model. The numbers are metric averages over $1,000$ runs (per method and sample size) and in parentheses is the corresponding variance of the metrics.

α	Coverage		Efficiency		Informativeness	
	ExponQ	**P-COQS**	**ExponQ**	**P-COQS**	**ExponQ**	**P-COQS**
0.01	1.0000 (0.0002)	0.9988 (0.0045)	1.9995 (0.0030)	1.9857 (0.0511)	0.0005 (0.0030)	0.0143 (0.0511)
0.05	0.9732 (0.0088)	0.9500 (0.0076)	1.7579 (0.0604)	1.6152 (0.0373)	0.2421 (0.0604)	0.3848 (0.0373)
0.10	0.9217 (0.0116)	0.8999 (0.0098)	1.4841 (0.0457)	1.3985 (0.0322)	0.5159 (0.0457)	0.6015 (0.0322)

Table 3: Average effect of α on private conformal prediction using DP Naïve Bayes model. The numbers are metric averages over $1,000$ runs (per method and significance level) and in parentheses is the corresponding variance of the metrics.

5.1.4 Computational Efficiency

We compare the runtime of the considered methods under two settings which considered the non-DP and DP versions of each model (i.e. $\hat{f}$ and $\hat{f}^{DP}$ respectively). Confirming the model privacy budget to be $\epsilon_f = 2$, conformal privacy budget $\epsilon_{CP} = 1$, total sample size $n = 10,000$ and significance level $\alpha = 0.1$, we record the average runtime over 1,000 runs. Table 4 highlights the considerable computational gain that P-COQS delivers with respect to ExponQ while remaining comparable (or often better) across all performance metrics considered above (similar conclusions hold for the RF model in Appendix B.4). It must be underlined that, as mentioned in Section 2, the increased computational time for ExponQ is mainly due to the optimization subroutine needed to choose the optimal number of bins and the quantile-inflation hyperparameter to achieve the smallest possible prediction set.

	Coverage	Efficiency	Informativeness	Model Accuracy	Ave. time (secs)
$\hat{f}$ and ExponQ	0.9227 (0.0116)	1.2509 (0.0360)	0.7491 (0.0360)	0.8253 (0.0092)	0.7562 (0.0111)
$\hat{f}$ and P-COQS	0.9006 (0.0010)	1.1788 (0.0201)	0.8212 (0.0201)	0.8253 (0.0092)	0.0072 (0.0002)
$\hat{f}^{DP}$ and ExponQ	0.9217 (0.0116)	1.4841 (0.0457)	0.5159 (0.0457)	0.7479 (0.0125)	0.7534 (0.0152)
$\hat{f}^{DP}$ and P-COQS	0.8999 (0.0098)	1.3985 (0.0322)	0.6015 (0.0322)	0.7479 (0.0125)	0.0072 (0.0003)

Table 4: Average computational time of P-COQS and ExponQ combined with non-DP and DP versions of the NB classifier.

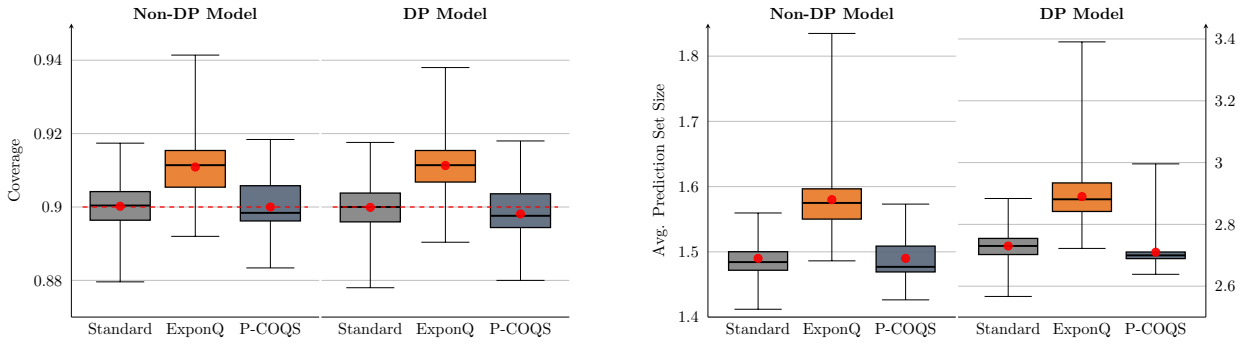
5.2 Datasets

In this section, we take the same settings as in Angelopoulos et al. (2022) and study the performance of P-COQS when applied to three benchmark datasets: CIFAR-10 (Krizhevsky et al., 2009), ImageNet (Deng et al., 2009) and CoronaHack (Pérez et al., 2020). As in the simulation experiment, we compare the performance of P-COQS with that of ExponQ proposed by Angelopoulos et al. (2022) and follow the same experimental setup as in the latter. Unless otherwise stated, the significance level is fixed at $\alpha = 0.1$, CP

privacy budget at $\epsilon_{CP} = 1$ and, when used, the DP models are trained to achieve (ϵ, δ)-DP using the `Opacus` library with ($\epsilon = 8$ and $\delta = 10^{-5}$).

5.2.1 CIFAR-10 Benchmark Analysis

We first evaluate P-COQS on the CIFAR-10 dataset, comparing its performance to ExponQ under different privacy settings. Following Angelopoulos et al. (2022), we consider two scenarios for model training: (i) one where a non-DP model is used ($\hat{f}$) and (ii) one where a DP model is used ($\hat{f}^{DP}$). Both DP and non-DP models share the same convolutional neural network architecture. The DP model achieved an accuracy of 60% compared to 77% for the non-DP model. The evaluation is based on $1,000$ random splits of the CIFAR-10 validation set, each of size $n = 5,000$. Figure 1 displays the empirical coverage and prediction set sizes across these settings. Our findings suggest that P-COQS generally produces smaller prediction sets (Figure 1b), while achieving empirical coverage levels that are comparable to those of the standard (non-private) CP baseline (Figure 1a), except for the case where a DP model is used where P-COQS appears to slightly undercover with respect to the standard CP baseline. On the other hand, compared to P-COQS, by inflating the quantile ExponQ guarantees the coverage level but tends to have larger prediction sets for this reason. In the latter case, for all methods it can be seen that prediction sets are larger when using a DP model (as expected).



(a) Coverage

(b) Avg. Prediction Set Size

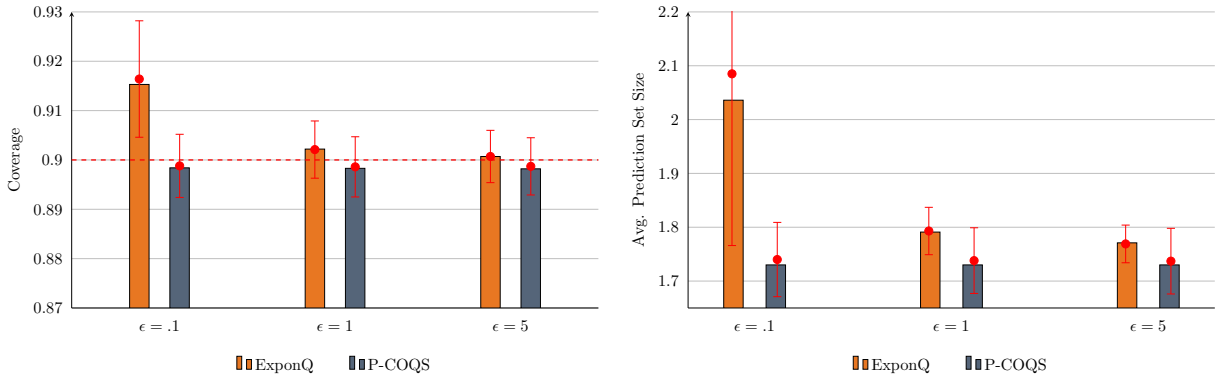
Figure 1: Results of Standard, ExponQ and P-COQS methods applied to the CIFAR-10 dataset. (a) Boxplots with coverage distributions of the three methods under the non-DP model (left) and DP model (right) scenarios; (b) Boxplots with distributions of average set sizes of the three methods under the non-DP model (left) and DP model (right) scenarios. Red dots represent respective average metric.

5.2.2 Large-Scale Evaluation on ImageNet

We apply both considered private CP methods to the ImageNet dataset using a pre-trained (non-DP) ResNet-152 model. We evaluated the performance of P-COQS and ExponQ under varying values of the conformal privacy budget ϵ_{CP}. The evaluation uses $n = 30,000$ samples for calibration and $20,000$ samples for validation. For each budget value ϵ_{CP}, performance metrics are computed over 100 random splits of the ImageNet validation set, following the procedure in Angelopoulos et al. (2022). As shown in Figure 2, P-COQS appears to slightly under-cover but this does not appear to be significant based on the 95% confidence intervals (red vertical whiskers in the plots) and remains stable in performance across the different values of ϵ_{CP}, whereas ExponQ appears to significantly over-cover for the small budgets (see Figure 2a). With this in mind, P-COQS also appears to be stable with respect to prediction set sizes while ExponQ approaches these sizes only as ϵ_{CP} increases (as highlighted also in the simulation results in Section 5.1).

5.2.3 Medical Imaging Analysis with CoronaHack Dataset

Finally, we evaluate both methods on the CoronaHack dataset, a publicly available chest X-ray dataset comprising $5,908$ images categorized into three classes: normal, viral pneumonia (primarily COVID-19), and bacterial pneumonia. We fine-tuned the final layer of a ResNet-18 model over 14 epochs using $4,408$

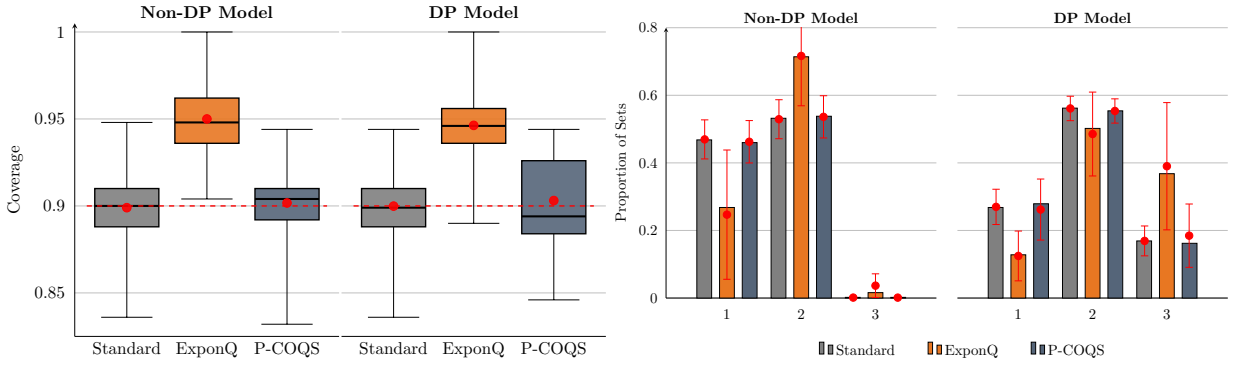


(a) Coverage

(b) Avg. Prediction Set Size

Figure 2: Results of ExponQ and P-COQS methods applied to the ImageNet dataset. (a) Median coverage (bar height), mean coverage (red dots) and 95% confidence intervals for coverage (red vertical whiskers) for each method under different privacy budgets ϵ (red-dashed horizontal line is the target coverage); (b) Average prediction set sizes (average set sizes in 100 splits): median (bar height), mean (red dots) and 95% confidence intervals (red vertical whiskers) for each method under different privacy budgets ϵ.

training samples, under both DP and non-DP settings. The DP model achieved 64% accuracy compared to 70% for the non-DP model. CP was calibrated on $1,000$ samples and validated on 500 samples, across $1,000$ random splits of the data. Figure 3 presents the results for different configurations of the DP and non-DP models. While ExponQ tends to produce overly conservative prediction sets, P-COQS appears to better target the nominal coverage level of 0.9 (see Figure 3a). Moreover, looking at the prediction set sizes, the distribution of the P-COQS appears to deliver roughly similar set sizes to the non-private CP approach since the proportions of sets of specific sizes (1, 2 or 3 on the x-axis) are very close to each other (see Figure 3b). Also in this case ExponQ produces larger sets (i.e. higher proportions for sets of size 2 or 3), where again the sizes tend to increase overall when using the DP model.



(a) Coverage

(b) Distribution of Prediction Set Sizes

Figure 3: Results of Standard, ExponQ and P-COQS methods applied to the CoronaHack dataset. (a) Boxplots with coverage distributions of the three methods under the non-DP model (left) and DP model (right) scenarios; (b) Distribution of prediction set sizes where the y-axis represents the empirical proportion of sets of size 1, 2 or 3 (represented on the x-axis) for each method: median proportion (bar height), mean proportion (red dots) and 95% confidence intervals (red vertical whiskers) for each method under the non-DP model (left) and DP model (right) scenarios.

6 Discussion

The proposed P-COQS provides a computationally efficient DP alternative to existing privacy-preserving CP approaches. It does so by adapting an existing DP quantile method and trading off some theoretical guarantees on the lower bound for the coverage probability, while however guaranteeing quantifiable lower and upper error bounds for this probability. In this way, it is possible to determine (tight) error bounds which can then be used to assess the true minimum coverage level with high probability. Despite this theoretical trade-off, which however remains small (if not negligible) in common settings, the P-COQS shows an empirical performance over different metrics that is in line with standard non-private CP, indicating that it targets the correct coverage level in all settings while delivering more precise CP sets compared to the existing DP alternative (that we denoted as ExponQ). The theoretical trade-off of the P-COQS can be observed mainly in settings with small sample sizes and/or privacy budgets in which the variability of P-COQS metrics is indeed larger compared to ExponQ. However, the latter approach also makes a trade-off by generally over-covering with respect to the required coverage level in smaller samples and for small privacy budgets. As a consequence, the latter tends to deliver less efficient and informative prediction sets in these settings and appears to only approach those of P-COQS for larger privacy budgets and/or sample sizes. In general, considering these different trade-offs and without claiming the existence of a better approach, the proposed P-COQS appears to provide a valid privacy-preserving (and computationally efficient) CP approach also based on its generally good performance compared to ExponQ in the different experimental settings considered. While both ExponQ and P-COQS can be applied within different forms of CP (e.g. full CP), future work will aim to refine the theoretical coverage bounds of P-COQS in order to achieve the minimal $(1-\alpha)$-coverage guarantees, without overly compromising the efficiency and informativeness of the prediction sets nor the computational efficiency of the method, particularly when the calibration sample size and/or privacy budget are small.

References

Anastasios N Angelopoulos and Stephen Bates. A gentle introduction to conformal prediction and distribution-free uncertainty quantification. *arXiv preprint arXiv:2107.07511*, 2021.

Anastasios Nikolas Angelopoulos, Stephen Bates, Tijana Zrnic, and Michael I Jordan. Private prediction sets. *Harvard Data Science Review*, 4(2), 2022.

Mario Astigarraga, Andrés Sánchez-Ruiz, and Gonzalo Colmenarejo. Conformal prediction-based machine learning in cheminformatics: Current applications and new challenges. *Artificial Intelligence in the Life Sciences*, pp. 100127, 2025.

Charles Blundell, Julien Cornebise, Koray Kavukcuoglu, and Daan Wierstra. Weight uncertainty in neural networks. In *International Conference on Machine Learning*, pp. 1613–1622. PMLR, 2015.

Mark Bun and Thomas Steinke. Concentrated differential privacy: Simplifications, extensions, and lower bounds. In *Theory of cryptography conference*, pp. 635–658. Springer, 2016.

Nicholas Carlini, Florian Tramer, Eric Wallace, Matthew Jagielski, Ariel Herbert-Voss, Katherine Lee, Adam Roberts, Tom Brown, Dawn Song, Ulfar Erlingsson, et al. Extracting training data from large language models. In *30th USENIX security symposium (USENIX Security 21)*, pp. 2633–2650, 2021.

Jia Deng, Wei Dong, Richard Socher, Li-Jia Li, Kai Li, and Li Fei-Fei. Imagenet: A large-scale hierarchical image database. In *2009 IEEE conference on computer vision and pattern recognition*, pp. 248–255. Ieee, 2009.

Jinshuo Dong, Aaron Roth, and Weijie J Su. Gaussian differential privacy. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 84(1):3–37, 2022.

Cynthia Dwork. Differential privacy. In *International colloquium on automata, languages, and programming*, pp. 1–12. Springer, 2006.

Matt Fredrikson, Somesh Jha, and Thomas Ristenpart. Model inversion attacks that exploit confidence information and basic countermeasures. In *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*, pp. 1322–1333, 2015.

Yarin Gal and Zoubin Ghahramani. Dropout as a bayesian approximation: Representing model uncertainty in deep learning. In *International Conference on Machine Learning*, pp. 1050–1059. PMLR, 2016.

Isaac Gibbs and Emmanuel Candès. Adaptive conformal inference under distribution shift. *arXiv preprint arXiv:2106.00170*, 2021.

Ziyue Huang, Yuting Liang, and Ke Yi. Instance-optimal mean estimation under differential privacy. *Advances in Neural Information Processing Systems*, 34:25993–26004, 2021.

Pierre Humbert, Batiste Le Bars, Aurélien Bellet, and Sylvain Arlot. One-shot federated conformal prediction. In *International Conference on Machine Learning*, pp. 14153–14177. PMLR, 2023.

Jef Jonkers, Glenn Van Wallendael, Luc Duchateau, and Sofie Van Hoecke. Conformal predictive systems under covariate shift. In *Proceedings of the Thirteenth Symposium on Conformal and Probabilistic Prediction with Applications*, pp. 406–423. PMLR, 2024.

Alex Kendall and Yarin Gal. What uncertainties do we need in bayesian deep learning for computer vision? In *Advances in Neural Information Processing Systems*, pp. 5574–5584, 2017.

Alex Krizhevsky, Geoffrey Hinton, et al. Learning multiple layers of features from tiny images. 2009.

Balaji Lakshminarayanan, Alexander Pritzel, and Charles Blundell. Simple and scalable predictive uncertainty estimation using deep ensembles. In *Advances in Neural Information Processing Systems*, pp. 6402–6413, 2017.

Jing Lei, Alessandro Rinaldo, and Larry Wasserman. A conformal prediction approach to explore functional data. *Annals of Mathematics and Artificial Intelligence*, 74:29–43, 2015.

Jing Lei, Max G'Sell, Alessandro Rinaldo, Ryan J Tibshirani, and Larry Wasserman. Distribution-free predictive inference for regression. *Journal of the American Statistical Association*, 113(523):1094–1111, 2018.

Miao Li, Michael Klamkin, Mathieu Tanneau, Reza Zandehshahvar, and Pascal Van Hentenryck. Conformal prediction with upper and lower bound models. *arXiv preprint arXiv:2503.04071*, 2025.

Frank McSherry and Kunal Talwar. Mechanism design via differential privacy. In *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*, pp. 94–103. IEEE, 2007.

Joseph P Near and Chiké Abuah. Programming differential privacy. *URL: https://uvm*, 2021.

Henrik Olsson, Kimmo Kartasalo, Nita Mulliqi, Marco Capuccini, Pekka Ruusuvuori, Hemamali Samaratunga, Brett Delahunt, Cecilia Lindskog, Emiel AM Janssen, Anders Blilie, et al. Estimating diagnostic uncertainty in artificial intelligence assisted pathology using conformal prediction. *Nature communications*, 13(1):7761, 2022.

Ian Osband, Charles Blundell, Alexander Pritzel, and Benjamin Van Roy. Deep exploration via bootstrapped dqn. In *Advances in Neural Information Processing Systems*, pp. 4026–4034, 2016.

Harris Papadopoulos, Kostas Proedrou, Volodya Vovk, and Alex Gammerman. Inductive confidence machines for regression. In *Machine learning: ECML 2002: 13th European conference on machine learning Helsinki, Finland, August 19–23, 2002 proceedings 13*, pp. 345–356. Springer, 2002.

Coby Penso, Bar Mahpud, Jacob Goldberger, and Or Sheffet. Privacy-preserving conformal prediction under local differential privacy. *arXiv preprint arXiv:2505.15721*, 2025.

Juan Caballero Pérez, José Manuel Caballero Contreras, Carlos de Blas Pérez, and Felipe Leza Alvarez. Databiology lab coronahack: Collection of public covid-19 data. *bioRxiv*, pp. 2020–10, 2020.

Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. Membership inference attacks against machine learning models. In *2017 IEEE symposium on security and privacy (SP)*, pp. 3–18. IEEE, 2017.

Ryan J Tibshirani, Rina Foygel Barber, Emmanuel J Candès, and Aaditya Ramdas. Conformal prediction under covariate shift. *arXiv preprint arXiv:1904.06019*, 2019.

Rudraksh Tuwani and Andrew Beam. Safe and reliable transport of prediction models to new healthcare settings without the need to collect new labeled data. *medRxiv*, 2023.

Nasir Uddin and Tuwe Lofstrom. Applications of conformal regression on real-world industrial use cases using crepes and mapie. In *Conformal and Probabilistic Prediction with Applications*, pp. 147–165. PMLR, 2023.

Vladimir Vovk. On-line confidence machines are well-calibrated. In *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.*, pp. 187–196. IEEE, 2002.

Vladimir Vovk. Cross-conformal predictors. *Annals of Mathematics and Artificial Intelligence*, 74:9–28, 2015.

Vladimir Vovk and Ivan Petej. Venn-abers predictors. *arXiv preprint arXiv:1211.0025*, 2012.

Vladimir Vovk, Alexander Gammerman, and Glenn Shafer. *Algorithmic learning in a random world*, volume 29. Springer, 2005.

Vladimir Vovk, Jieli Shen, Valery Manokhin, and Min-ge Xie. Nonparametric predictive distributions based on conformal prediction. In *Conformal and probabilistic prediction and applications*, pp. 82–102. PMLR, 2017.

A Simulation Results With Non-DP Random Forest Model

A.1 Effect of ϵ_{CP} with non-DP model

The parameter settings are as in the non-DP NB model and the model's accuracy is 81%.

$\epsilon_{\text{conformal}}$	Coverage		Efficiency		Informativeness	
	ExponQ	**P-COQS**	**ExponQ**	**P-COQS**	**ExponQ**	**P-COQS**
0.1	0.9998 (0.0004)	0.9024 (0.0104)	1.9885 (0.0123)	1.2222 (0.0243)	0.0115 (0.0123)	0.7778 (0.0243)
0.5	0.9464 (0.0188)	0.9025 (0.0098)	1.4094 (0.1213)	1.2223 (0.0220)	0.5906 (0.1213)	0.7777 (0.0220)
1	0.9228 (0.0123)	0.9026 (0.0098)	1.2936 (0.0408)	1.2224 (0.0218)	0.7064 (0.0408)	0.7776 (0.0218)
1.5	0.9154 (0.0107)	0.9026 (0.0098)	1.2660 (0.0294)	1.2225 (0.0217)	0.7340 (0.0294)	0.7775 (0.0217)
3	0.9084 (0.0099)	0.9026 (0.0098)	1.2415 (0.0235)	1.2225 (0.0220)	0.7585 (0.0235)	0.7775 (0.0220)
5	0.9058 (0.0099)	0.9026 (0.0099)	1.2327 (0.0224)	1.2225 (0.0220)	0.7673 (0.0224)	0.7775 (0.0220)
10	0.9041 (0.0100)	0.9026 (0.0099)	1.2273 (0.0224)	1.2226 (0.0219)	0.7727 (0.0224)	0.7774 (0.0219)

Table 5: Average effect of CP privacy budget ϵ_{CP} on conformal prediction with non-DP Random Forest model. The numbers are metric averages over 1000 runs (per method and privacy budget) and in parentheses is the corresponding variance of the metrics.

A.2 Sample size effect with non-DP model

Samples	Coverage		Efficiency		Informativeness	
	ExponQ	**P-COQS**	**ExponQ**	**P-COQS**	**ExponQ**	**P-COQS**
100	0.9892 (0.0326)	0.9280 (0.0973)	1.8658 (0.1716)	1.5599 (0.3114)	0.1342 (0.1716)	0.4401 (0.3114)
200	0.9931 (0.0183)	0.9298 (0.0678)	1.8925 (0.1308)	1.4749 (0.2301)	0.1075 (0.1308)	0.5251 (0.2301)
500	0.9973 (0.0076)	0.9083 (0.0455)	1.9274 (0.0872)	1.3108 (0.1210)	0.0726 (0.0872)	0.6892 (0.1210)
1000	0.9987 (0.0036)	0.9056 (0.0304)	1.9520 (0.0577)	1.2706 (0.0786)	0.0480 (0.0577)	0.7294 (0.0786)
2000	0.9865 (0.0126)	0.9054 (0.0227)	1.7402 (0.1492)	1.2501 (0.0561)	0.2598 (0.1492)	0.7499 (0.0561)
6000	0.9393 (0.0181)	0.9026 (0.0123)	1.3745 (0.0986)	1.2268 (0.0293)	0.6255 (0.0986)	0.7732 (0.0293)
10000	0.9229 (0.0120)	0.9025 (0.0098)	1.2939 (0.0406)	1.2224 (0.0222)	0.7061 (0.0406)	0.7776 (0.0222)

Table 6: Average effect of sample size on DP CP ($\epsilon_{CP} = 1$) with non-DP Random Forest model. The numbers are metric averages over 1000 runs (per method and sample size) and in parentheses is the corresponding variance of the metrics. Average effect of sample size on private CP with Non-DP Random Forest model.

A.3 Effect of α with non-DP model

α	Coverage		Efficiency		Informativeness	
	ExponQ	**P-COQS**	**ExponQ**	**P-COQS**	**ExponQ**	**P-COQS**
0.01	0.9998 (0.0004)	0.9909 (0.0033)	1.9885 (0.0123)	1.7554 (0.0370)	0.0115 (0.0123)	0.2446 (0.0370)
0.05	0.9800 (0.0120)	0.9516 (0.0072)	1.6512 (0.1426)	1.4204 (0.0275)	0.3488 (0.1426)	0.5796 (0.0275)
0.10	0.9229 (0.0120)	0.9025 (0.0098)	1.2939 (0.0406)	1.2224 (0.0222)	0.7061 (0.0406)	0.7776 (0.0222)

Table 7: Average effect of α on DP CP ($\epsilon_{CP} = 1$) with non-DP Random Forest model. The numbers are metric averages over 1000 runs (per method and α value) and in parentheses is the corresponding variance of the metrics.

B Simulation Results With DP Random Forest Model

The parameter settings are as in the DP NB model and the model's accuracy is 79%.

B.1 Effect of ϵ_{CP} with DP model

$\epsilon_{\text{conformal}}$	Coverage		Efficiency		Informativeness	
	ExponQ	**P-COQS**	**ExponQ**	**P-COQS**	**ExponQ**	**P-COQS**
0.1	1.0000 (0.0002)	0.8982 (0.0112)	1.9970 (0.0087)	1.2552 (0.0438)	0.0030 (0.0087)	0.7448 (0.0438)
0.5	0.9575 (0.0272)	0.8977 (0.0107)	1.5621 (0.2378)	1.2535 (0.0438)	0.4379 (0.2378)	0.7465 (0.0438)
1	0.9242 (0.0123)	0.8977 (0.0106)	1.3459 (0.0555)	1.2533 (0.0438)	0.6541 (0.0555)	0.7467 (0.0438)
1.5	0.9171 (0.0105)	0.8976 (0.0106)	1.3183 (0.0465)	1.2532 (0.0439)	0.6817 (0.0465)	0.7468 (0.0439)
3	0.9096 (0.0112)	0.8977 (0.0106)	1.2921 (0.0471)	1.2534 (0.0442)	0.7079 (0.0471)	0.7466 (0.0442)
5	0.9058 (0.0121)	0.8976 (0.0105)	1.2801 (0.0505)	1.2531 (0.0440)	0.7199 (0.0505)	0.7469 (0.0440)
10	0.9034 (0.0129)	0.8975 (0.0104)	1.2726 (0.0526)	1.2530 (0.0438)	0.7274 (0.0526)	0.7470 (0.0438)

Table 8: Average effect of CP privacy budget ϵ_{CP} on conformal prediction with DP Random Forest model and $\epsilon_f = 2$. The numbers are metric averages over 1000 runs (per method and privacy budget) and in parentheses is the corresponding variance of the metrics.

B.2 Sample size effect with DP model

Sample Size	Coverage		Efficiency		Informativeness		Model Accuracy
	ExponQ	**P-COQS**	**ExponQ**	**P-COQS**	**ExponQ**	**P-COQS**	
100	0.9979 (0.0142)	0.9669 (0.0800)	1.9977 (0.0146)	1.9534 (0.1166)	0.0022 (0.0146)	0.0466 (0.1166)	0.4201 (0.1141)
200	0.9993 (0.0060)	0.9597 (0.0653)	1.9990 (0.0078)	1.9306 (0.1092)	0.0010 (0.0078)	0.0694 (0.1092)	0.4503 (0.0975)
500	0.9998 (0.0019)	0.9098 (0.0484)	1.9983 (0.0094)	1.6637 (0.1346)	0.0017 (0.0094)	0.3364 (0.1346)	0.6183 (0.0776)
1000	0.9999 (0.0011)	0.9060 (0.0321)	1.9977 (0.0110)	1.5422 (0.1067)	0.0023 (0.0110)	0.4578 (0.1067)	0.6808 (0.0604)
2000	0.9978 (0.0065)	0.9066 (0.0226)	1.9678 (0.0756)	1.4203 (0.0800)	0.0322 (0.0756)	0.5797 (0.0800)	0.7371 (0.0455)
6000	0.9467 (0.0258)	0.9009 (0.0133)	1.5064 (0.1986)	1.2913 (0.0519)	0.4936 (0.1986)	0.7087 (0.0519)	0.7836 (0.0239)
10000	0.9242 (0.0123)	0.8977 (0.0106)	1.3459 (0.0555)	1.2533 (0.0438)	0.6541 (0.0555)	0.7467 (0.0438)	0.7941 (0.0173)

Table 9: Average effect of sample size on DP CP ($\epsilon_{CP} = 1$) with DP Random Forest model ($\epsilon_f = 2$). The numbers are metric averages over 1000 runs (per method and sample size) and in parentheses is the corresponding variance of the metrics.

B.3 Effect of α with DP model

α	Coverage		Efficiency		Informativeness	
	ExponQ	**P-COQS**	**ExponQ**	**P-COQS**	**ExponQ**	**P-COQS**
0.01	1.0000 (0.0002)	0.9904 (0.0036)	1.9970 (0.0087)	1.7604 (0.0422)	0.0030 (0.0087)	0.2396 (0.0422)
0.05	0.9914 (0.0121)	0.9484 (0.0077)	1.8486 (0.1751)	1.4475 (0.0435)	0.1514 (0.1751)	0.5525 (0.0435)
0.10	0.9242 (0.0123)	0.8977 (0.0106)	1.3459 (0.0555)	1.2533 (0.0438)	0.6541 (0.0555)	0.7467 (0.0438)

Table 10: Average effect of α on DP CP ($\epsilon_{CP} = 1$) with DP Random Forest model ($\epsilon_f = 2$). The numbers are metric averages over 1000 runs (per method and α value) and in parentheses is the corresponding variance of the metrics.

B.4 Average CP computational time with DP and non-DP models

Description	Empirical coverage	Efficiency	Informativeness	Model Accuracy	Ave. time (secs)
$\hat{f}$ and ExponQ	0.9229 (0.0120)	1.2939 (0.0406)	0.7061 (0.0406)	0.8125 (0.0093)	0.7353 (0.0098)
$\hat{f}$ and P-COQS	0.9025 (0.0098)	1.2224 (0.0222)	0.7776 (0.0222)	0.8125 (0.0093)	0.0074 (0.0002)
$\hat{f}^{DP}$ and ExponQ	0.9242 (0.0123)	1.3459 (0.0555)	0.6541 (0.0555)	0.7941 (0.0173)	0.7390 (0.0088)
$\hat{f}^{DP}$ and P-COQS	0.8977 (0.0106)	1.2533 (0.0443)	0.7467 (0.0443)	0.7941 (0.0173)	0.0074 (0.0002)

Table 11: Average computational time of P-COQS and ExponQ combined with non-DP and DP versions of the Random Forest classifier. The numbers are metric averages over 1000 runs (per setting) and in parentheses is the corresponding variance of the metrics.

B.5 Effect of Model Privacy Budget (ϵ_f)

ϵ_f	**Coverage**		**Efficiency**		**Informativeness**		**Model Accuracy**
	ExponQ	**P-COQS**	**ExponQ**	**P-COQS**	**ExponQ**	**P-COQS**	
0.1	0.9256 (0.0142)	0.9021 (0.0167)	1.5647 (0.0841)	1.4891 (0.0723)	0.4353 (0.0841)	0.5109 (0.0723)	0.6870 (0.0591)
0.5	0.9248 (0.0126)	0.8999 (0.0112)	1.3839 (0.0674)	1.2956 (0.0530)	0.6161 (0.0674)	0.7044 (0.0530)	0.7803 (0.0242)
1	0.9241 (0.0127)	0.8982 (0.0104)	1.3575 (0.0611)	1.2664 (0.0454)	0.6425 (0.0611)	0.7336 (0.0454)	0.7898 (0.0187)
2	0.9242 (0.0123)	0.8977 (0.0106)	1.3459 (0.0555)	1.2533 (0.0438)	0.6541 (0.0555)	0.7467 (0.0438)	0.7941 (0.0173)
5	0.9241 (0.0123)	0.8973 (0.0104)	1.3405 (0.0546)	1.2481 (0.0407)	0.6595 (0.0546)	0.7519 (0.0407)	0.7957 (0.0167)
10	0.9241 (0.0122)	0.8972 (0.0104)	1.3405 (0.0542)	1.2479 (0.0409)	0.6595 (0.0542)	0.7521 (0.0409)	0.7958 (0.0168)

Table 12: Average effect of model privacy budget ϵ_f on DP CP ($\epsilon_{CP} = 1$) with DP Random Forest model. The numbers are metric averages over 1000 runs (per method and privacy budget) and in parentheses is the corresponding variance of the metrics.

C Simulation Results With Non-DP Naïve Bayes Model

The parameter settings are as described in Section 5.1 and the accuracy of the model is 83%.

C.1 Effect of Privacy Budget (ϵ_{CP})

ϵ_{CP}	**Coverage**		**Efficiency**		**Informativeness**	
	ExponQ	**P-COQS**	**ExponQ**	**P-COQS**	**ExponQ**	**P-COQS**
0.1	0.9999 (0.0004)	0.9005 (0.0104)	1.9678 (0.0289)	1.1787 (0.0223)	0.0322 (0.0289)	0.8213 (0.0223)
0.5	0.9444 (0.0174)	0.9005 (0.0101)	1.3465 (0.0972)	1.1788 (0.0206)	0.6535 (0.0972)	0.8212 (0.0206)
1	0.9227 (0.0116)	0.9006 (0.0099)	1.2509 (0.0360)	1.1788 (0.0201)	0.7491 (0.0360)	0.8212 (0.0201)
1.5	0.9154 (0.0103)	0.9006 (0.0099)	1.2254 (0.0267)	1.1788 (0.0201)	0.7746 (0.0267)	0.8212 (0.0201)
3	0.9081 (0.0097)	0.9006 (0.0099)	1.2019 (0.0213)	1.1788 (0.0200)	0.7981 (0.0213)	0.8212 (0.0200)
5	0.9051 (0.0097)	0.9006 (0.0099)	1.1925 (0.0203)	1.1789 (0.0200)	0.8075 (0.0203)	0.8211 (0.0200)
10	0.9029 (0.0097)	0.9006 (0.0099)	1.1857 (0.0198)	1.1789 (0.0201)	0.8143 (0.0198)	0.8211 (0.0201)

Table 13: Average effect of CP privacy budget ϵ_{CP} on conformal prediction with non-DP Naïve Bayes model. The numbers are metric averages over 1000 runs (per method and privacy budget) and in parentheses is the corresponding variance of the metrics.

C.2 Sample size effect

Samples	Coverage		Efficiency		Informativeness	
	ExponQ	**P-COQS**	**ExponQ**	**P-COQS**	**ExponQ**	**P-COQS**
100	0.9794 (0.0434)	0.9040 (0.1004)	1.7300 (0.2179)	1.3677 (0.2713)	0.2700 (0.2179)	0.6323 (0.2713)
200	0.9905 (0.0207)	0.9206 (0.0695)	1.7901 (0.1638)	1.3394 (0.2004)	0.2099 (0.1638)	0.6606 (0.2004)
500	0.9967 (0.0078)	0.9053 (0.0440)	1.8566 (0.1158)	1.2222 (0.1071)	0.1434 (0.1158)	0.7778 (0.1071)
1000	0.9984 (0.0042)	0.9018 (0.0315)	1.8951 (0.0876)	1.1954 (0.0669)	0.1049 (0.0876)	0.8046 (0.0669)
2000	0.9836 (0.0129)	0.9030 (0.0212)	1.6272 (0.1483)	1.1891 (0.0466)	0.3728 (0.1483)	0.8109 (0.0466)
6000	0.9382 (0.0169)	0.9008 (0.0123)	1.3149 (0.0795)	1.1798 (0.0268)	0.6851 (0.0795)	0.8202 (0.0268)
10000	0.9227 (0.0116)	0.9006 (0.0099)	1.2509 (0.0360)	1.1788 (0.0200)	0.7491 (0.0360)	0.8212 (0.0200)

Table 14: Average effect of sample size on DP CP ($\epsilon_{CP} = 1$) with non-DP Naïve Bayes model. The numbers are metric averages over 1000 runs (per method and sample size) and in parentheses is the corresponding variance of the metrics. Average effect of sample size on private CP with Non-DP Random Forest model.

C.3 Effect of α

α	Coverage		Efficiency		Informativeness	
	ExponQ	**P-COQS**	**ExponQ**	**P-COQS**	**ExponQ**	**P-COQS**
0.01	0.9999 (0.0004)	0.9901 (0.0033)	1.9677 (0.0289)	1.6703 (0.0349)	0.0323 (0.0289)	0.3297 (0.0349)
0.05	0.9785 (0.0115)	0.9500 (0.0073)	1.5670 (0.1306)	1.3610 (0.0244)	0.4330 (0.1306)	0.6390 (0.0244)
0.10	0.9227 (0.0116)	0.9006 (0.0099)	1.2509 (0.0360)	1.1788 (0.0200)	0.7491 (0.0360)	0.8212 (0.0200)

Table 15: Average effect of α on DP CP ($\epsilon_{CP} = 1$) with non-DP Naïve Bayes model ($\epsilon_f = 2$). The numbers are metric averages over 1000 runs (per method and α value) and in parentheses is the corresponding variance of the metrics.

C.4 Effect of Model Privacy Budget (ϵ_f)

ϵ_f	Coverage		Efficiency		Informativeness		Model Accuracy
	ExponQ	**P-COQS**	**ExponQ**	**P-COQS**	**ExponQ**	**P-COQS**	
0.1	0.9218 (0.0115)	0.8994 (0.0101)	1.6580 (0.0335)	1.5905 (0.0233)	0.3420 (0.0335)	0.4095 (0.0233)	0.6319 (0.0139)
0.5	0.9222 (0.0110)	0.9000 (0.0094)	1.5361 (0.0389)	1.4532 (0.0263)	0.4639 (0.0389)	0.5468 (0.0263)	0.7233 (0.0110)
1	0.9405 (0.0366)	0.9812 (0.0409)	1.7647 (0.1443)	1.9207 (0.1718)	0.2353 (0.1443)	0.0793 (0.1718)	0.6559 (0.0303)
2	0.9217 (0.0116)	0.8999 (0.0098)	1.4841 (0.0457)	1.3985 (0.0322)	0.5159 (0.0457)	0.6015 (0.0322)	0.7479 (0.0125)
5	0.9224 (0.0117)	0.9000 (0.0098)	1.2784 (0.0372)	1.2036 (0.0216)	0.7216 (0.0372)	0.7964 (0.0216)	0.8156 (0.0095)
10	0.9225 (0.0116)	0.9002 (0.0098)	1.2570 (0.0361)	1.1840 (0.0204)	0.7430 (0.0361)	0.8160 (0.0204)	0.8230 (0.0093)

Table 16: Average effect of model privacy budget ϵ_f on conformal prediction with DP Naïve Bayes model. The numbers are metric averages over 1000 runs (per method and privacy budget) and in parentheses is the corresponding variance of the metrics.