Towards Personalized Privacy-Preserving Incentive for Truth Discovery in Crowdsourced Binary-Choice Question Answering

Peng Sun[†], Zhibo Wang[≀], Yunhe Feng[‡], Liantao Wu[†], Yanjun Li[§], Hairong Qi[‡], and Zhi Wang[†,*]
[†]State Key Laboratory of Industrial Control Technology, Zhejiang University, P. R. China
[≀]School of Cyber Science and Engineering, Wuhan University, P. R. China
[‡]Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, USA
[§]School of Computer Science and Technology, Zhejiang University of Technology, P. R. China
Email: {sunpengzju, wuliantao, zjuwangzhi}@zju.edu.cn, zbwang@whu.edu.cn, {yunhefeng, hqi}@utk.edu, yjli@gmail.com

***Abstract*—Truth discovery is an effective tool to unearth truthful answers in crowdsourced question answering systems. Incentive mechanisms are necessary in such systems to stimulate worker participation. However, most of existing incentive mechanisms only consider compensating workers' resource cost, while the cost incurred by potential privacy leakage has been rarely incorporated. More importantly, to the best of our knowledge, how to provide personalized payments for workers with different privacy demands remains uninvestigated thus far. In this paper, we propose a contract-based personalized privacy-preserving incentive mechanism for truth discovery in crowdsourced question answering systems, named PINTION, which provides personalized payments for workers with different privacy demands as a compensation for privacy cost, while ensuring accurate truth discovery. The basic idea is that each worker chooses to sign a contract with the platform, which specifies a privacy-preserving level (PPL) and a payment, and then submits perturbed answers with that PPL in return for that payment. Specifically, we respectively design a set of optimal contracts under both complete and incomplete information models, which could maximize the truth discovery accuracy, while satisfying the budget feasibility, individual rationality and incentive compatibility properties. Experiments on both synthetic and real-world datasets validate the feasibility and effectiveness of PINTION.**

***Index Terms*—crowdsourced question answering, truth discovery, personalized privacy-preserving, incentive, contracts**

I. Introduction

Crowdsourcing is becoming an increasingly popular human-empowered problem-solving paradigm, which outsources a specific set of tasks to a crowd of workers to complete via an open call [1], [2]. Thus far, crowdsourcing has witnessed extensive applications in various fields, such as environmental monitoring, smart transportation, healthcare, and online marketplace (e.g., Amazon Mechanical Turk) [3]–[6]. Recently, crowdsourcing, as a means of aggregating answers from participating workers, has gained immense popularity in question answering applications [7]–[9]. For example, workers engaged in geotagging campaigns can answer the question on whether there exist bumps or potholes on certain road segments [10]; patients who are taking new drugs can answer the question on whether there are any allergic reactions [11].

Due to the openness of crowdsourcing, answers from one particular worker may not be reliable. Thus, most of existing crowdsourcing studies resort to a redundancy-based strategy, which assigns each question to a group of workers and aggregates the answers provided by them to infer the correct answer (called truth) of each question. Moreover, due to the diversity of individual workers' expertise levels, experience levels, effort levels, or even the existence of malicious workers dispersing deceptive answers, the information quality of answers provided by different workers varies significantly. Therefore, it is more desirable to adopt a weighted answer aggregation mechanism which assigns higher weights to workers with higher information quality than naive methods (e.g., majority voting) regarding all the workers equally. To tackle the challenge that workers' information quality is usually unknown *a priori* in practice, a series of truth discovery mechanisms are proposed [12]–[16], which could jointly unearth the truthful information and estimate worker quality from noisy crowdsourced answers.

Participating in crowdsourced question answering activities introduces various costs for workers. First, it consumes workers' time and energy to generate answers to the questions assigned to them, and resources of their smart devices (e.g., power, memory) to store and upload the generated answers to the crowdsourcing platform. These costs can be collectively referred to as resource cost. Moreover, workers' answers may disclose their sensitive or private information. For example, soliciting patients' reactions to new drugs provides critical insights for medical scientists to discover the drugs' side effects, but may leak sensitive information that patients are unwilling to share. Although some privacy-preserving mechanisms (e.g., randomized response [17]) can be adopted, workers are still subject to a certain degree of potential privacy leakage, leading to privacy cost. Therefore, efficient incentive mechanisms should be provided to compensate for workers' various costs in order to stimulate adequate worker participation.

*Zhi Wang is the corresponding author.

Thus far, a wide spectrum of incentive mechanisms [3], [18]–[21] have been developed for crowdsourcing systems. However, most of them only consider compensating workers' resource cost, while the cost incurred by potential privacy leakage has been rarely incorporated. Recent works [22]–[26] have taken the first step towards privacy-preserving incentive mechanisms for crowdsourcing. Specifically, [22] employed a cryptography-based scheme to protect workers' privacy in their incentive mechanism design. The work in [23] and [24] respectively focused on preserving workers' bid privacy and location privacy based on differential privacy. However, in these works, the emphasis is put on the privacy preservation mechanism itself, while workers' privacy cost is not explicitly measured and compensated. In [25], [26], the authors first considered compensating workers' privacy cost in their incentive mechanisms. However, they assume that the platform is trusted, which may not hold in practice as the platform will probably be hacked and become untrusted. More importantly, different workers may raise different degrees of awareness even under the same degree of potential privacy leakage, that is, they bear different privacy preferences [27]. A worker with a higher privacy preference would usually expect a larger compensation than one with a lower privacy preference even when they are provided with the same privacy-preserving level (PPL). However, to the best of our knowledge, none of existing privacy-preserving incentive mechanisms in crowdsourcing has ever studied how to provide personalized payments for workers involved in question answering tasks with their different privacy preferences taken into consideration.

To address these issues, in this paper, we propose PINTION[1], a contract-based personalized privacy-preserving incentive mechanism for truth discovery in crowdsourced binary-choice question answering systems, which provides personalized payments for workers with different privacy preferences as a compensation for privacy cost, while achieving accurate truth discovery. The basic idea is that each worker chooses to sign a personalized contract with the platform, which specifies a PPL and a payment, and then submits perturbed answers with that PPL in return for that payment. The design objective of PINTION is to derive a set of optimal contracts, which maximizes the truth discovery accuracy, under both complete information model, where the platform knows each worker's precise privacy preference, and incomplete information model, where only the distribution of workers' privacy preferences is known by the platform. Meanwhile, the set of designed contracts can satisfy the budget feasibility (BF) property ensuring that the total cost of the platform does not exceed the budget available, the individual rationality (IR) property ensuring that each worker's privacy cost is properly compensated, and the incentive compatibility (IC) property ensuring that workers would truthfully reveal their privacy preferences.

In summary, this paper makes the following contributions:

- To the best of our knowledge, this is the first work to design a personalized privacy-preserving incentive mechanism for truth discovery in crowdsourced binary-choice question answering systems, which could provide personalized payments for workers with different privacy preferences, while achieving accurate truth discovery.
- We quantify each worker's PPL and privacy cost based on the idea of randomized response, and formally define the truth discovery accuracy in terms of γ-accuracy.
- We respectively design a set of optimal contracts under both complete and incomplete information models, which maximizes the truth discovery accuracy, while guaranteeing the BF, IR, and IC properties.
- We conduct extensive experiments of PINTION on both synthetic and real-world datasets, and the results demonstrate its feasibility and effectiveness.

[1]The name PINTION comes from Personalized prIvacy-preserving iNcentive for Truth dIscovery in crowdsourced questiOn aNswering.

II. Related Work

Empowered by human wisdom, crowdsourcing is gaining increasing popularity in question answering applications by soliciting answers from a crowd of participating workers [28], [29]. Considering the heterogeneity in the information quality of answers provided by different workers, a series of truth discovery algorithms [12], [14], [16], [30], [31] have been proposed to jointly find the true answers and infer worker quality from noisy crowdsourced answers. However, a key component missing in these works is an efficient incentive mechanism, which is of crucial importance for stimulating adequate worker participation.

Aware of the importance of incentivizing worker participation, researchers have developed a wide spectrum of incentive mechanisms for crowdsourcing [3], [18]–[20], [32], [33]. However, these incentive mechanisms only take workers' resource cost into consideration, while the cost incurred by potential privacy leakage (i.e., privacy cost) is not considered.

One line of previous work, which is highly related to this paper, incorporates workers' privacy concerns into their incentive mechanism designs [22]–[26], [34]. Specifically, cryptography techniques are employed in [22] to preserve workers' privacy. The work in [23] and [24] leverages differential privacy to protect workers' bid privacy and location privacy, respectively. However, these works put emphasis on the privacy preservation mechanism itself, while the privacy cost of workers is not explicitly measured and compensated. In [25], [26], workers' privacy cost is first integrated into the incentive mechanism design. However, the platform is assumed to be trusted in [25], [26], and data perturbation is performed on the aggregated results at the platform to resist privacy threats from adversaries outside the crowdsourcing system. In contrast, we do not make such an assumption in our incentive mechanism, and workers perturb their answers locally before uploading them to the platform. Moreover, workers' different privacy preferences are considered in our incentive mechanism. Although the researchers in [34] propose an incentive mechanism with workers' heterogeneous privacy demands taken into account, they focus on a simple averaging task of continuous values, where all workers are treated equally. In our work, however,

workers' diverse information quality is captured in finding the true answers to binary-choice questions.

III. Preliminaries

In this section, we first provide an overview of our crowdsourced binary-choice question answering system, and then briefly introduce truth discovery and randomized response.

A. System Overview

The crowdsourced binary-choice question answering system considered in this paper consists of two parties: a platform and a set of W participating workers, denoted by $\mathcal{W} = \{1, 2, \ldots, W\}$. The platform (i.e., the crowdsourcer) is interested in a set of questions $\mathcal{Q} = \{1, 2, \ldots, Q\}$. Each question $q \in \mathcal{Q}$ has two possible answers. Formally, we use $x_q^{truth} \in \{+1, -1\}$ to denote the true answer for question q. Due to the openness of crowdsourcing, answers from one particular worker may be unreliable. Therefore, in order to obtain the true answer to each question $q \in \mathcal{Q}$, the platform aggregates the answers from a group of workers. Specifically, if we denote the answer to question q from worker w by x_q^w, then we have $x_q^* = A\left(\left\{x_q^w\right\}_{w=1}^W\right)$, where x_q^* is the aggregated result for question q, and $A(\cdot)$ denotes the aggregation algorithm[2].

B. Truth Discovery

A fundamental issue in crowdsourced question answering is how to aggregate answers from multiple workers to find the correct answer for each question. A simple method is to conduct majority voting. Since there are only two possible answers (i.e., $+1$ or -1) for each question in our binary-choice question answering system, the majority voting method can be equivalently formulated as

$$x_q^* = \text{sign}\left(\sum\nolimits_{w \in \mathcal{W}} x_q^w\right), \tag{1}$$

where x_q^w is the answer for question q from worker w, and x_q^* is the corresponding aggregated result. The function $\text{sign}(z)$ equals to $+1$ if $z \geq 0$, and -1 otherwise. This simple aggregation strategy, which treats all the workers equally, may fail to provide reliable aggregated results, as the information quality of worker-provided answers usually varies significantly among different workers in crowdsourcing.

Recently, truth discovery has emerged as an effective tool in question answering problems, as it can infer workers' information quality from noisy crowdsourced answers in the form of weights, and incorporates such weights to conduct weighted aggregation to find the correct answers. We summarize the general procedure of truth discovery in Algorithm 1.

Answer Aggregation: This step conducts weighted answer aggregation for each question based on the currently estimated worker weights. Formally,

$$x_q^* = \text{sign}\left(\sum\nolimits_{w \in \mathcal{W}} \lambda_w x_q^w\right), \tag{2}$$

[2]Note that for ease of presentation, we assume herein that each worker $w \in \mathcal{W}$ provides an answer for each question $q \in \mathcal{Q}$.

Algorithm 1: Truth Discovery in Crowdsourced Binary-Choice Question Answering

Input: Answers from W workers for Q questions $\left\{x_q^w\right\}_{q,w=1}^{Q,W}$

Output: Aggregated answers for Q questions $\left\{x_q^*\right\}_{q=1}^{Q}$

```
Initialize workers' weights {λ_w}_{w=1}^W;
while convergence criterion is not satisfied do
    for q ∈ Q do
        Update the aggregated answer x_q^* using
         currently estimated weights based on Eq. (2);
    end
    for w ∈ W do
        Update the worker weight λ_w using currently
         aggregated answers based on Eq. (3);
    end
end
```

where λ_w is the weight of worker w. Obviously, this weighted aggregation process follows the principle that the aggregated result relies more on the answer provided by workers with higher information quality.

Weight Estimation: In this step, workers' weights are calculated based on the current aggregated answers. Specifically, the weight λ_w of each worker $w \in \mathcal{W}$ is calculated as

$$\lambda_w = g(p_w) = g\left(\frac{\sum_{q \in \mathcal{Q}} \mathbb{I}\left(x_q^*, x_q^w\right)}{Q}\right), \tag{3}$$

where $\mathbb{I}(\cdot)$ is the indicator function ($\mathbb{I}(x_1, x_2) = 1$ if $x_1 = x_2$, and 0 otherwise), and p_w is the probability that worker w provides correct answers. $g(\cdot)$ is a monotonically increasing function. Different truth discovery algorithms may adopt various forms of $g(\cdot)$, but the underlying principle that a worker who is more likely to provide correct answers will be assigned a higher weight remains the same.

C. Randomized Response

Workers usually have privacy concerns when they participate in question answering activities, as the submitted answers may disclose their sensitive information. As the platform in our crowdsourced question answering system is assumed to be untrusted, traditional definition of differential privacy, which provides workers with privacy protection against information leakage through published aggregated results, is no longer applicable [7]. Thus, we adopt the following local differential privacy definition in this paper.

Definition 1: (ε-Local Differential Privacy): A randomized algorithm $\mathcal{M}$ is said to satisfy ε-local differential privacy if for any two different values x_1 and x_2 in $\mathcal{D}$, and any $\mathcal{S} \subseteq \mathcal{D}$,

$$\Pr\{\mathcal{M}(x_1) \in \mathcal{S}\} \leq e^{\epsilon} \times \Pr\{\mathcal{M}(x_2) \in \mathcal{S}\}, \tag{4}$$

where ε is the privacy budget, indicating the level of privacy protection, and we refer to it as the PPL in this paper.

Recently, a set of local differential privacy (LDP) solutions has been proposed. Among them, randomized response [17],

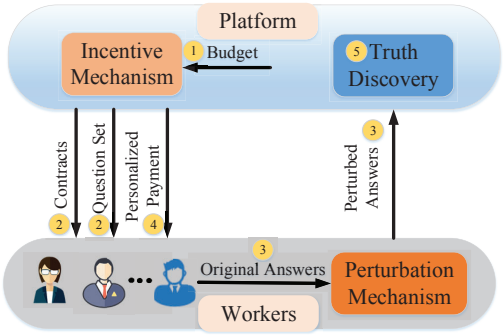

Fig. 1. Framework of PINTION (where circled numbers represent the sequence of the events).

[35], a surveying technique for collecting statistics on sensitive topics, has attracted significant attention. In randomized response, each worker will flip a coin before answering a question. If the coin comes up heads, she provides her original answer; otherwise, she provides the opposite of her original answer. Using this procedure, workers obtains plausible deniability for any answers they provide, thus they are provided with a certain level of privacy protection.

IV. System Framework

We present the framework of PINTION in Fig. 1, and describe the workflow as follows.

1) The platform designs a set of optimal contracts (each contract is a PPL-payment bundle), which maximizes the truth discovery accuracy, while satisfying the BF, IR, and IC properties (step ①).
2) The platform publishes the set of designed contracts along with the set of questions $\mathcal{Q}$ to the set of participating workers $\mathcal{W}$ (step ②).
3) Each worker $w \in \mathcal{W}$ makes her own decision to sign one contract with the platform to maximize her utility. Then, due to privacy concerns, worker w perturbs her original answers $\{x_q^w\}_{q=1}^{Q}$ for each question $q \in \mathcal{Q}$ with a probability determined by the PPL specified in the signed contract, yielding perturbed answers $\{\hat{x}_q^w\}_{q=1}^{Q}$ (step ③).
4) After collecting the perturbed answers $\{\hat{x}_q^w\}_{q,w=1}^{Q,W}$ from all workers, the platform pays each worker according to the payment specified in the signed contract (step ④).
5) The platform conducts truth discovery on the perturbed answers $\{\hat{x}_q^w\}_{q,w=1}^{Q,W}$ to obtain aggregated results $\{\hat{x}_q^*\}_{q=1}^{Q}$ for each question $q \in \mathcal{Q}$ (step ⑤).

V. Theoretical Analysis: Privacy Versus Accuracy

In this section, we first quantify workers' PPLs and privacy cost, and then formally define the truth discovery accuracy.

A. Workers' Privacy Analysis

As previously mentioned, workers will perturb their original answers before uploading them to the platform to preserve privacy. Inspired by the idea of randomized response, we adopt the following perturbation mechanism.

Definition 2: (Perturbation Mechanism): Given a binary answer x (i.e., $x \in \{+1, -1\}$) and a probability p^r, the answer perturbation mechanism $\mathcal{M}$ satisfies that $\mathcal{M}(x) = x$ with probability p^r, and $\mathcal{M}(x) = -x$ with probability $1 - p^r$.

If worker w chooses a probability p_w^r to perturb her original answers using this perturbation mechanism, that is, she provides her perturbed answer $\hat{x}_q^w$ for question q (i.e., $\hat{x}_q^w = x_q^w$ with probability p_w^r, $\hat{x}_q^w = -x_q^w$ with probability $1 - p_w^r$), she will be provided with a certain PPL. It is worth noting that when two probabilities $p_w^{r'}$, $p_w^{r''}$ satisfy $p_w^{r'} + p_w^{r''} = 1$, they can provide worker w with the same level of plausible deniability, which promises the same PPL. Thus, without loss of generality, we assume $p_w^r \geq 0.5$. Intuitively, moreover, when $p_w^r = 0.5$, worker w acquires the largest level of deniability, indicating the largest possible PPL. We present the explicit relationship between p_w^r and the acquired PPL in the following theorem.

Theorem 1: When worker w adopts the perturbation mechanism in Definition 2 to perturb her original answers with probability p_w^r, that is, she provides her original answers (resp. opposite of original answers) with probability p_w^r (resp. $1 - p_w^r$), she achieves ϵ_w-local differential privacy guarantee, and $\varepsilon_w = \ln\left(\frac{p_w^r}{1-p_w^r}\right)$ is referred to as her obtained PPL.

Proof 1: We omit the proof here because it is similar to the proof of Theorem 6.2 in [7].

According to Theorem 1, if worker w chooses to sign a contract with the platform which specifies a PPL ε_w, she would perturb her original answers using the perturbation mechanism in Definition 2 with the probability $p_w^r = \frac{e^{\varepsilon_w}}{e^{\varepsilon_w}+1}$. Obviously, if a contract specifying a higher PPL (i.e., a smaller ε_w) is signed between the platform and worker w, she would perturb her original answers with a probability p_w^r closer to 0.5, that is, she provides answers with larger deniability. Note that since all the workers $w \in \mathcal{W}$ adopt the same perturbation mechanism, Theorem 1 is applicable to all of them.

After quantifying a worker's PPL in Theorem 1, we now derive her privacy cost. Naturally, a worker's privacy cost is related to her obtained PPL, and a lower PPL (i.e., a higher degree of potential privacy leakage) leads to larger privacy cost. In other words, the privacy cost of worker w, denoted by $C_w(\varepsilon_w)$, is positively correlated with the privacy parameter ε_w. Moreover, $C_w(\varepsilon_w)$ is also related to her privacy preference, which indicates how sensitive about privacy leakage she is. Without loss of generality, in this paper, we adopt the linear privacy cost function in [36], i.e., $C_w(\varepsilon_w) = c_w\varepsilon_w$, where c_w is the cost of unit privacy leakage for worker w, which is referred to as her personalized privacy preference. Then, with a contract signed with the platform, a worker's utility is defined as follows.

Definition 3: (Worker Utility): The utility of worker w, denoted by u_w, is calculated as

$$u_w = r_w - c_w\varepsilon_w, \tag{5}$$

where the bundle (ε_w, r_w) is the contract signed between worker w and the platform, which specifies the payment r_w to her if she submits perturbed answers with the PPL ε_w.

B. Truth Discovery Accuracy Analysis

As described in Algorithm 1, before adding perturbation, the aggregated answers for each question $q \in \mathcal{Q}$ are obtained through weighted aggregation on original answers, i.e., $x_q^* = \text{sign}\left(\sum_{w\in\mathcal{W}} \lambda_w x_q^w\right)$, where λ_w is the estimated weight for worker w. According to Eq. (3), $\lambda_w = g(p_w)$, where p_w is the probability that worker w provides correct answers (i.e., $\Pr\left\{x_q^w = x_q^{truth}\right\}$), and $g(\cdot)$ is a monotonically increasing function. Without loss of generality, in this paper, we adopt a simple weight calculation function $\lambda_w = 2p_w - 1$.

Before presenting the truth discovery accuracy analysis after answer perturbation, let's consider a simple scenario of two workers. Worker a provides correct answers with probability p_a, where $p_a \in [0, 0.5]$, and worker b provides correct answers with probability p_b, where $p_b = 1 - p_a$. If worker b flips all her answers to the opposite ones, she would also have the probability p_a to provide correct answers. Therefore, we have $x_q^b = -x_q^a$. Using the above-mentioned weight calculation function, the weight of worker b is $\lambda_b = 2p_b - 1 = 2(1-p_a) - 1 = 1 - 2p_a = -\lambda_a$. When the platform conducts weighted aggregation for question q on the answers from worker a and worker b, the contribution from worker b is $\lambda_b x_q^b = (-\lambda_a)\left(-x_q^a\right) = \lambda_a x_q^a$, which is exactly the contribution from worker a. Note that this observation, which indicates that worker b is equivalent to worker a in the weighted answer aggregation, will be used in our subsequent analysis of the truth discovery accuracy from perturbed answers.

When worker w perturbs her answers using the perturbation mechanism in Definition 2 with the probability p_w^r, that is, she provides her original answers (resp. opposite of original answers) with probability p_w^r (resp. $1 - p_w^r$), then the probability that she provides correct answers is calculated as

$$\hat{p}_w = p_w p_w^r + (1 - p_w)(1 - p_w^r). \tag{6}$$

Now, the aggregated answers for each question $q \in \mathcal{Q}$ are obtained through weighted aggregation on perturbed answers, i.e., $\hat{x}_q^* = \text{sign}\left(\sum_{w\in\mathcal{W}} \hat{\lambda}_w \hat{x}_q^w\right)$, where $\hat{\lambda}_w$ is the estimated weight for worker w after perturbation, and $\hat{\lambda}_w = 2\hat{p}_w - 1$.

In order to measure the truth discovery accuracy based on perturbed answers, we introduce an accuracy metric, which is formally defined as follows.

Definition 4: (γ-Accuracy): For each aggregated answer $\hat{x}_q^*$ for question $q \in \mathcal{Q}$ based on workers' submitted perturbed answers, given $\gamma \in (0, 1)$, it satisfies γ-accuracy if and only if $\Pr\left\{\hat{x}_q^* \neq x_q^{truth}\right\} \leq \gamma$.

According to Definition 4, γ-accuracy ensures that the aggregated answer from workers' perturbed answers for question $q \in \mathcal{Q}$ equals to the correct answer with high probability. Obviously, a smaller γ implies a stronger accuracy guarantee.

In Theorem 2, we prove that the aggregated answer for question $q \in \mathcal{Q}$ based on workers' submitted perturbed answers using the truth discovery algorithm in Algorithm 1 satisfies γ-accuracy.

Theorem 2: For each question $q \in \mathcal{Q}$, using the truth discovery procedure in Algorithm 1, the error probability of the aggregated answer based on workers' submitted perturbed answers, i.e., $\Pr\left\{\hat{x}_q^* \neq x_q^{truth}\right\}$, satisfies that

$$\Pr\left\{\hat{x}_q^* \neq x_q^{truth}\right\} \leq \exp\left(-\frac{\sum_{w\in\mathcal{W}}(2\hat{p}_w - 1)^2}{2}\right). \tag{7}$$

Proof 2: Since worker w provides correct answers with probability $\hat{p}_w$ after perturbation, and $\hat{\lambda}_w = 2\hat{p}_w - 1$, if we denote the weighted answer from worker w for question q by $\tilde{x}_q^w$, then $\tilde{x}_q^w = \hat{\lambda}_w x_q^{truth}$ with probability $\hat{p}_w$, and $\tilde{x}_q^w = -\hat{\lambda}_w x_q^{truth}$ with probability $1 - \hat{p}_w$. Then, the weighted sum of all workers' answers is $\tilde{x}_q^* = \sum_{w\in\mathcal{W}} \tilde{x}_q^w$, and we have $\mathbb{E}\left[\tilde{x}_q^*\right] = \mathbb{E}\left[\sum_{w\in\mathcal{W}} \tilde{x}_q^w\right] = \sum_{w\in\mathcal{W}} \mathbb{E}\left[\tilde{x}_q^w\right] = \sum_{w\in\mathcal{W}} x_q^{truth} \hat{\lambda}_w (2\hat{p}_w - 1)$.

The error probability of the aggregated answer after perturbation can be calculated as $\Pr\left\{\hat{x}_q^* \neq x_q^{truth}\right\} = \Pr\left\{\tilde{x}_q^* < 0 \middle| x_q^{truth} = 1\right\} \Pr\left\{x_q^{truth} = 1\right\} + \Pr\left\{\tilde{x}_q^* \geq 0 \middle| x_q^{truth} = -1\right\} \Pr\left\{x_q^{truth} = -1\right\}$. According to the Chernoff-Hoeffding bound, we have

$$\begin{aligned}&\Pr\left\{\tilde{x}_q^* < 0 \middle| x_q^{truth} = 1\right\} = \Pr\left\{\mathbb{E}\left[\tilde{x}_q^*\right] - \tilde{x}_q^* > \mathbb{E}\left[\tilde{x}_q^*\right] \middle| x_q^{truth} = 1\right\} \\ &\leq \exp\left(-\frac{2\left(\mathbb{E}\left[\tilde{x}_q^* \middle| x_q^{truth}=1\right]\right)^2}{\sum_{w\in\mathcal{W}}\left(2\hat{\lambda}_w\right)^2}\right) = \exp\left(-\frac{\left(\sum_{w\in\mathcal{W}} \hat{\lambda}_w(2\hat{p}_w-1)\right)^2}{2\sum_{w\in\mathcal{W}} \hat{\lambda}_w^2}\right).\end{aligned} \tag{8}$$

With $\hat{\lambda}_w = 2\hat{p}_w - 1$ and based on the Cauchy-Schwarz inequality, we have

$$\left(\sum_{w\in\mathcal{W}} \hat{\lambda}_w (2\hat{p}_w - 1)\right)^2 = \left(\sum_{w\in\mathcal{W}} \hat{\lambda}_w^2\right)\left(\sum_{w\in\mathcal{W}} (2\hat{p}_w - 1)^2\right). \tag{9}$$

Thus, we have

$$\Pr\left\{\tilde{x}_q^* < 0 \middle| x_q^{truth} = 1\right\} \leq \exp\left(-\frac{\sum_{w\in\mathcal{W}}(2\hat{p}_w-1)^2}{2}\right). \tag{10}$$

In a similar way, we can also get

$$\Pr\left\{\tilde{x}_q^* \geq 0 \middle| x_q^{truth} = -1\right\} \leq \exp\left(-\frac{\sum_{w\in\mathcal{W}}(2\hat{p}_w-1)^2}{2}\right). \tag{11}$$

In summary, we have $\Pr\left\{\hat{x}_q^* \neq x_q^{truth}\right\} \leq \exp\left(-\frac{\sum_{w\in\mathcal{W}}(2\hat{p}_w-1)^2}{2}\right)$, which completes the proof.

According to Theorem 2, in order to provide a good guarantee for the truth discovery accuracy after perturbation, we need to minimize $\exp\left(-\frac{\sum_{w\in\mathcal{W}}(2\hat{p}_w-1)^2}{2}\right)$, which is equivalent to maximizing $\sum_{w\in\mathcal{W}}(2\hat{p}_w - 1)^2$.

VI. Contract-based Incentive Mechanism Design

In this section, we present our contract-based incentive mechanism design.

A. Design Objective

Without loss of generality, we assume that workers can be divided into K privacy groups according to their privacy preferences, and the privacy preference of workers in the i-th ($1 \leq i \leq K$) privacy group is c_i. The privacy preferences of K privacy groups can be sorted as $c_1 < c_2 < \cdots < c_K$.

The design objective of our incentive mechanism is to derive a set of optimal contracts $\{(\varepsilon_1, r_1), (\varepsilon_2, r_2), \ldots, (\varepsilon_K, r_K)\}$

for K privacy groups, which could maximize the truth discovery accuracy (i.e., maximizing $\sum_{w\in\mathcal{W}}\left(2\hat{p}_w-1\right)^2$). Substituting Eq. (6) into $\sum_{w\in\mathcal{W}}\left(2\hat{p}_w-1\right)^2$, the design objective becomes maximizing $\sum_{w\in\mathcal{W}}\left(4p_wp_w^r-2p_w-2p_w^r+1\right)^2$. As in most prior work on truth discovery [16], [37], we assume that most workers have fairly high information quality (i.e., p_w is close to 1), and a small portion of workers have relatively low quality (i.e., p_w is close to 0), and we have demonstrated that workers with $p_w=0$ are equivalent to workers with $p_w=1$, thus we could resort to maximizing $\sum_{w\in\mathcal{W}}\left(2p_w^r-1\right)^2$ as an approximation. Moreover, as $p_w^r=\frac{e^{\varepsilon_w}}{e^{\varepsilon_w}+1}$ according to Theorem 1, we finally turn to maximizing $\sum_{w\in\mathcal{W}}\left(\frac{e^{\varepsilon_w}-1}{e^{\varepsilon_w}+1}\right)^2$. Meanwhile, the set of designed contracts should satisfy the following three constraints.

The first constraint that needs to be satisfied is budget feasibility defined in Definition 5.

Definition 5: (Budget Feasibility (BF)): A set of contracts is budget feasible, if and only if the total payment for all participating workers does not exceed the budget B, i.e.,

$$\sum\nolimits_{w\in\mathcal{W}} r_w \le B. \tag{12}$$

In order to prevent workers from being disincentivized to participate, it is necessary to satisfy individual rationality, defined in Definition 6.

Definition 6: (Individual Rationality (IR)): A set of contracts satisfy IR if they provide workers in any privacy groups with non-negative utility, i.e.,

$$r_i-c_i\varepsilon_i\ge 0,\ (1\le i\le K)\,. \tag{13}$$

Moreover, the set of contracts should satisfy incentive compatibility, defined in Definition 7, which ensures that selfish and strategic workers cannot improve their utility by cheating their privacy groups.

Definition 7: (Incentive Compatibility (IC)): A set of contracts satisfy IC if they ensure that the workers in the i-th privacy group achieve the maximum utility when they sign the (ε_i, r_i) contract rather than other contracts (ε_j, r_j), i.e.,

$$r_i-c_i\varepsilon_i\ge r_j-c_i\varepsilon_j,\ (1\le i\,,j\le K, j\ne i)\,. \tag{14}$$

In the next two subsections, we present the optimal contract design under the following two information models.

1) **Complete Information Model**: Under this model, the platform knows each worker's privacy group (i.e., privacy preference) in advance. Thus, the platform can specially design and offer one contract for each group. This is an ideal case which usually cannot be achieved in practice, and we employ it as a benchmark.
2) **Incomplete Information Model**: Under this model, instead of each worker's privacy group, the platform only knows the distribution of workers in different privacy groups, say the number of workers in each group.

B. Contract Design under Complete Information Model

This section investigates the optimal contract design under complete information model. Under this model, workers in group i $(i=1,...,K)$ could only receive one contract (ε_i, r_i) from the platform. In this case, the IC property is satisfied naturally, and the platform only needs to consider the BF and IR properties in the contract design.

Assume there are m_i workers distributed in group i, thus the optimal contract design under complete information model can be formulated as

$$\max \quad \sum\nolimits_{i=1}^{K} m_i\left(\frac{e^{\varepsilon_i}-1}{e^{\varepsilon_i}+1}\right)^2 \tag{15a}$$

$$\text{s.t.} \quad \sum\nolimits_{i=1}^{K} m_ir_i\le B, \tag{15b}$$

$$r_i-c_i\varepsilon_i\ge 0,\ \text{for } 1\le i\le K, \tag{15c}$$

where B is a fixed budget available to the platform, and c_i is the privacy preference of workers in the i-th privacy group.

Since the objective function (15a) is an increasing function of ε_i, the inequality constraints (15b)(15c) can be equivalently simplified to equality constraints, i.e., $\sum_{i=1}^{K} m_ir_i=B$ and $r_i-c_i\varepsilon_i=0$ $(1\le i\le K)$. Due to the difficulty in finding the analytical solution to the optimization problem (15), we transform it into an unconstrained optimization problem using a penalty function, and solve it numerically based on gradient ascent. After obtaining the set of optimal PPLs ε_i^* $(i=1,...,K)$, the set of optimal payments r_i^* are calculated as $r_i^*=c_i\varepsilon_i^*$. We would like to stress that the problem of finding the global optimum is beyond the scope of this paper.

C. Contract Design under Incomplete Information Model

A more realistic and complicated scenario is the incomplete information model, where the platform only knows the distribution of workers in different privacy groups (i.e., the number of workers m_i in each group i). Note that this can be achieved by making a survey questionnaire [38].

Without the knowledge of the privacy preferences of workers, the platform needs to offer the set of contracts designed for different privacy groups to each worker. In this case, selfish and strategic workers may pretend to be in other privacy groups to sign contracts not designed for her group to obtain undeserved utility. Thus, in addition to the BF and IR properties, the set of designed contracts should also satisfy the IC property. Therefore, the optimal contract design under incomplete information model is formulated as

$$\max \quad \sum\nolimits_{i=1}^{K} m_i\left(\frac{e^{\varepsilon_i}-1}{e^{\varepsilon_i}+1}\right)^2 \tag{16a}$$

$$\text{s.t.} \quad \sum\nolimits_{i=1}^{K} m_ir_i\le B, \tag{16b}$$

$$r_i-c_i\varepsilon_i\ge 0,\ \text{for } 1\le i\le K, \tag{16c}$$

$$r_i-c_i\varepsilon_i\ge r_j-c_i\varepsilon_j,\ \text{for } 1\le i,\ j\le K,\ i\ne j. \tag{16d}$$

As shown in Eqs. (16c)(16d), there are K IR constraints and $K\times(K-1)$ IC constraints, making it intractable to solve this problem directly. Therefore, we simplify it.

We first simplify the BF and IR constraints as in Lemma 1.

Lemma 1: The BF constraint Eq. (16b) and IR constraints Eq. (16c) can be equivalently simplified to $\sum_{i=1}^{K} m_ir_i=B$ and $r_K-c_K\varepsilon_K=0$.

Proof 3: Recall that $c_1 < c_2 < \cdots < c_K$ and based on the IC constraints Eq. (16d), for $\forall i < K$, we have $r_i - c_i\varepsilon_i \geq r_K - c_i\varepsilon_K > r_K - c_K\varepsilon_K$. Thus, in order to satisfy the IR property for all workers, we only need to ensure that $r_K - c_K\varepsilon_K \geq 0$. Furthermore, it is obvious that the platform could always choose a larger ε_K to achieve higher truth discovery accuracy without violating the IR constraints until $r_K - c_K\varepsilon_K = 0$. Also, if $\sum_{i=1}^{K} m_i r_i < B$, the platform could choose a larger r_K, which corresponds to a larger ε_K until $\sum_{i=1}^{K} m_i r_i = B$.

Next, we simplify the IC constraints Eq. (16d). To this end, we first provide the following lemma.

Lemma 2 (PPL Monotonicity): Workers in groups with higher privacy preferences (or higher privacy groups in short) prefer a higher PPL. Specifically, for any two feasible contracts (ε_i, r_i) and (ε_j, r_j), $\varepsilon_j \leq \varepsilon_i$ if $c_i \leq c_j$.

Proof 4: Based on Eq. (16d), for $i \neq j$, we have $r_i - c_i\varepsilon_i \geq r_j - c_i\varepsilon_j$ and $r_j - c_j\varepsilon_j \geq r_i - c_j\varepsilon_i$. Adding the two inequalities, we have $(\varepsilon_j - \varepsilon_i)(c_i - c_j) \geq 0$, indicating $\varepsilon_j \leq \varepsilon_i$ if $c_i \leq c_j$.

Then, the IC constraints Eq. (16d) can be simplified as in Lemma 3 below.

Lemma 3: The IC constraints Eq. (16d) can be simplified to $r_i - c_i\varepsilon_i = r_{i+1} - c_i\varepsilon_{i+1},\ 1 \leq i \leq K-1$.

Proof 5: We prove Lemma 3 in three steps. First, we prove that if $r_i - c_i\varepsilon_i \geq r_{i+1} - c_i\varepsilon_{i+1}$, then $r_i - c_i\varepsilon_i \geq r_{i+1} - c_i\varepsilon_{i+1} \geq ... \geq r_K - c_i\varepsilon_K$ holds.

Assume $c_i \leq c_{i+1} \leq c_{i+2}$, based on the IC property and Lemma 2, we have $r_{i+1} - c_{i+1}\varepsilon_{i+1} \geq r_{i+2} - c_{i+1}\varepsilon_{i+2} \Rightarrow r_{i+1} - r_{i+2} \geq c_{i+1}(\varepsilon_{i+1} - \varepsilon_{i+2}) \Rightarrow r_{i+1} - r_{i+2} \geq c_i(\varepsilon_{i+1} - \varepsilon_{i+2}) \Rightarrow r_{i+1} - c_i\varepsilon_{i+1} \geq r_{i+2} - c_i\varepsilon_{i+2}$. We also have $r_i - c_i\varepsilon_i \geq r_{i+1} - c_i\varepsilon_{i+1}$. Thus, $r_i - c_i\varepsilon_i \geq r_{i+2} - c_i\varepsilon_{i+2}$. In this way, we can derive that $r_i - c_i\varepsilon_i \geq r_{i+1} - c_i\varepsilon_{i+1} \geq ... \geq r_K - c_i\varepsilon_K$.

Following a similar methodology, we can prove that if $r_i - c_i\varepsilon_i \geq r_{i-1} - c_i\varepsilon_{i-1}$, then $r_i - c_i\varepsilon_i \geq r_{i-1} - c_i\varepsilon_{i-1} \geq ... \geq r_1 - c_i\varepsilon_1$ holds.

Second, we prove that $r_i - c_i\varepsilon_i \geq r_{i+1} - c_i\varepsilon_{i+1}$ is active in the optimal contract, i.e., $r_i - c_i\varepsilon_i = r_{i+1} - c_i\varepsilon_{i+1}$. This is because the platform could always choose a larger ε_i in the optimal contract design to achieve higher truth discovery accuracy until the equality holds.

Third, we prove that if $r_i - c_i\varepsilon_i = r_{i+1} - c_i\varepsilon_{i+1}$, then $r_i - c_i\varepsilon_i \geq r_{i-1} - c_i\varepsilon_{i-1}$ holds naturally.

Based on Lemma 2, we have $r_i - c_i\varepsilon_i = r_{i+1} - c_i\varepsilon_{i+1} \Rightarrow r_i - r_{i+1} = c_i(\varepsilon_i - \varepsilon_{i+1}) \Rightarrow r_i - r_{i+1} \leq c_{i+1}(\varepsilon_i - \varepsilon_{i+1}) \Rightarrow r_{i+1} - c_{i+1}\varepsilon_{i+1} \geq r_i - c_{i+1}\varepsilon_i$.

In summary, $r_i - c_i\varepsilon_i = r_{i+1} - c_i\varepsilon_{i+1}$ implies that $r_i - c_i\varepsilon_i \geq r_j - c_i\varepsilon_j, \forall i \neq j$, which completes the proof.

With Lemma 1, Lemma 3, the optimization problem Eq. (16) can be equivalently simplified to

$$\max \quad \sum_{i=1}^{K} m_i \left(\frac{e^{\varepsilon_i} - 1}{e^{\varepsilon_i} + 1}\right)^2 \tag{17a}$$

$$\text{s.t.} \quad \sum_{i=1}^{K} m_i r_i = B, \tag{17b}$$

$$r_K - c_K\varepsilon_K = 0, \tag{17c}$$

$$r_i - c_i\varepsilon_i = r_{i+1} - c_i\varepsilon_{i+1},\ 1 \leq i \leq K-1. \tag{17d}$$

The optimization problem (17) can be further simplified as in the following theorem.

Theorem 3: The optimization problem (17) is equivalent to

$$\max \quad \sum_{i=1}^{K} m_i \left(\frac{e^{\varepsilon_i} - 1}{e^{\varepsilon_i} + 1}\right)^2 \tag{18a}$$

$$\text{s.t.} \quad \sum_{i=1}^{K} Q_i\varepsilon_i = B, \tag{18b}$$

where

$$Q_i = \begin{cases} m_1 c_1, i = 1 \\ m_i c_i + \Delta c_i \sum_{j=1}^{i-1} m_j, i \geq 2 \end{cases} \tag{19}$$

$$\Delta c_i = c_i - c_{i-1}. \tag{20}$$

Proof 6: According to Eq. (17d), we have

$$r_{K-1} - c_{K-1}\varepsilon_{K-1} = r_K - c_{K-1}\varepsilon_K. \tag{21}$$

Substituting $r_K = c_K\varepsilon_K$ (i.e., Eq. (17c)) into it, we have

$$\begin{aligned} r_{K-1} &= c_{K-1}\varepsilon_{K-1} + (c_K - c_{K-1})\varepsilon_K \\ &= c_{K-1}\varepsilon_{K-1} + \Delta c_K\varepsilon_K, \end{aligned} \tag{22}$$

where $\Delta c_K = c_K - c_{K-1}$.

Following the same methodology, we can represent r_i $(1 \leq i \leq K)$ as follows

$$r_i = \begin{cases} c_i\varepsilon_i + \sum_{j=i+1}^{K} \Delta c_j\varepsilon_j, i \leq K-1 \\ c_K\varepsilon_K, i = K \end{cases} \tag{23}$$

Substituting Eq. (23) into Eq. (17b), we have

$$\sum_{i=1}^{K} m_i r_i = \sum_{i=1}^{K-1} \left(m_i c_i\varepsilon_i + m_i \sum_{j=i+1}^{K} \Delta c_j\varepsilon_j\right) + m_K c_K\varepsilon_K, \tag{24}$$

which can be summarized as

$$\sum_{i=1}^{K} m_i r_i = \sum_{i=1}^{K} Q_i\varepsilon_i = B, \tag{25}$$

where Q_i is defined as in Eq. (19).

Therefore, the set of optimal PPLs ε_i^* $(i = 1, ..., K)$ can be obtained by solving the optimization problem (18), and the set of optimal payments r_i^* are calculated according to Eq. (23).

VII. Performance Evaluation

In this section, we evaluate the performance of PINTION.

A. Baselines

In PINTION, we customize contracts for workers with different privacy preferences in order to provide them with personalized PPLs and payments. As elaborated in Section II, none of existing work has considered the same scenario as this paper, thus they are not comparable with PINTION. Instead, we choose a simple single-contract strategy as the baseline, where the platform designs and offers one and the same contract to all the participating workers regardless of their different privacy preferences. In particular, we consider the following two options in the single-contract design.

1) **Single Contract with Individual Rationality (SC-IR)**: This single contract ensures that workers in the highest privacy group (i.e., with highest privacy preference) achieve zero utility, and thus workers in lower groups achieve

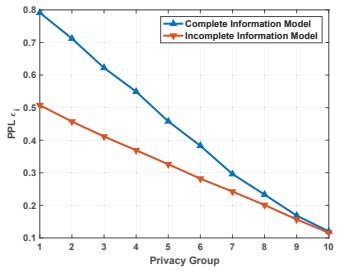

Fig. 2. PPL monotonicity.

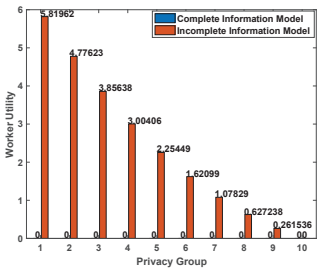

Fig. 3. IR property.

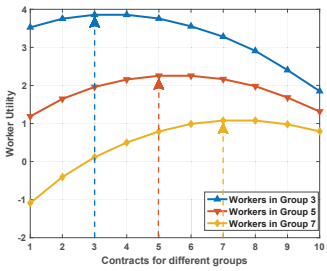

Fig. 4. IC property.

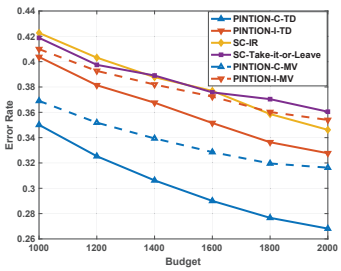

Fig. 5. Error rate versus the platform's budget.

positive utility. That is, the IR property is satisfied for all the workers.

2) **Single Contract with Take-it-or-Leave (SC-Take-it-or-Leave)**: This single contract guarantees that workers in the median privacy group achieve zero utility. Thus, only workers in lower groups will sign the contract and provide answers, while those in higher groups will leave as their received utility will be negative.

Furthermore, under PINTION, we compare the truth discovery mechanism with the simple majority voting scheme.

B. Experiments on Synthetic Dataset

In this part, we provide experimental results on synthetic dataset. We assume that the platform needs to find the correct answers to $Q = 1000$ binary-choice questions, by aggregating the answers from $W = 100$ workers. The correct answer x_q^{truth} for each question q is randomly selected from $\{+1, -1\}$. Each worker randomly selects a subset of questions $\mathcal{Q}^{'}$ from $\mathcal{Q}$ to answer, and we denote $s = \left|\mathcal{Q}^{'}\right| / |\mathcal{Q}|$ as the worker participation level. To generate workers' original answers x_q^w, we assume that W_1 workers have a relatively high information quality, while the rest $W - W_1$ workers have a relatively low information quality. The probability of providing correct answers p_w for workers of high quality is assumed to be sampled from a uniform distribution $\mathbb{U}(a, 1)$, while that for workers with low quality is simply sampled from the uniform distribution $\mathbb{U}(0, 0.3)$. After a worker signs a contract with the platform, she perturbs her original answers following the perturbation mechanism in Definition 2 with a probability p_w^r determined by the PPL specified in the signed contract, and gets the corresponding payment. Then, truth discovery is conducted on the perturbed answers $\hat{x}_q^w$ from all participating workers. We assume that W workers are uniformly at random distributed in $K = 10$ privacy groups. The privacy preference of each privacy group is sampled from a uniform distribution of $\mathbb{U}(15, 40)$, and we sort them in ascending order. Note that s, W_1, a, and the budget B are respectively set to 0.02, 80, 0.7, and 1000 unless otherwise specified.

1) Contract Feasibility: We first evaluate the feasibility of the contracts designed in PINTION.

PPL Monotonicity: We first present the PPL ε_i in the set of contracts designed for K privacy groups. As shown in Fig. 2, under both complete and incomplete information models, contracts designed for higher privacy groups offer higher PPLs (i.e., smaller ε_i), indicating that workers with higher privacy preferences pursue higher PPLs. This is consistent with Lemma 2. In addition, workers in the same group are provided with higher PPLs under incomplete information model. The underlying reason is that the platform does not know workers' privacy preferences, and thus it would waste some budget to provide workers with positive utility to encourage them to truthfully reveal their privacy groups.

IR Property: The utility of workers in different privacy groups is shown in Fig. 3. Obviously, workers in arbitrary groups achieve non-negative utility under both information models, which validates the IR property. Specifically, all workers achieve zero utility with complete information, as the platform knows each worker's privacy group and designs personalized contracts with zero utility for workers. In contrast, under incomplete information model, only workers in the highest group achieve zero utility, while contracts for other groups offer workers positive utility, as they are designed with extra utility to incentivize workers to behave truthfully.

IC Property: With incomplete information, we demonstrate the utility of workers in group 3, 5, 7 when signing K different contracts in Fig. 4. As indicated by the arrows, workers achieve the maximum utility when they sign the contract customized for them. Moreover, workers in lower groups achieve higher utility than those in higher groups when signing the same contract. This can be explained by the definition of worker utility in Eq. (5) and the fact that the privacy preference of lower groups is smaller.

2) System Performance: Next, we investigate the impact of different system parameters on the truth discovery accuracy. We employ error rate on all the Q questions (i.e., $\frac{\sum_{q\in\mathcal{Q}} \Gamma\left(\hat{x}_q^*, x_q^{truth}\right)}{Q}$, where $\Gamma(x_1, x_2) = 1$ if $x_1 \neq x_2$, and 0 otherwise) as the accuracy metric.

Impact of Budget: The impact of the platform's budget B on error rate is shown in Fig. 5, where B ranges from 1000 to 2000. Note that hereafter we use "C" and "I" to respectively represent complete and incomplete information model, and we use "TD" and "MV" to respectively represent the truth discovery and majority voting scheme. As depicted in Fig. 5, whichever the mechanism, lower error rate is achieved as B rises. This result is self-explanatory. When the platform has more budget to afford, it can provide more payment to incentivize workers to choose a lower PPL, leading to lower error rate. Besides, truth discovery achieves lower error rate than majority voting under both complete and incomplete information models, which demonstrates the importance of incorporating workers' diverse quality into answer aggregation.

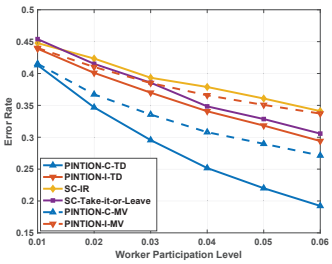

Fig. 6. Error rate versus worker participation level.

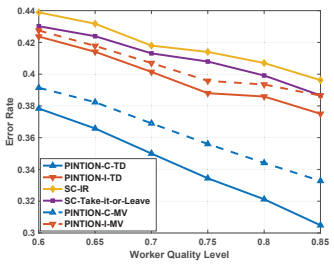

Fig. 7. Error rate versus worker quality level.

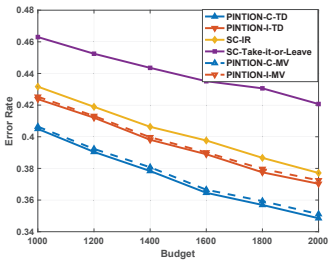

Fig. 8. Error rate versus the platform's budget on tweets dataset.

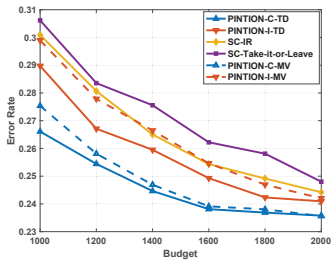

Fig. 9. Error rate versus the platform's budget on duck dataset.

Finally, we can see that our personalized contract design in PINTION is superior to the single-contract strategies.

Impact of Worker Participation Level: We investigate the impact of worker participation level s (s varies from 0.01 to 0.06) on the truth discovery accuracy in Fig. 6. Unsurprisingly, when each worker provides answers for more questions (i.e., higher worker participation level), the platform achieves lower error rate. This is because with higher worker participation level, we can aggregate answers from more workers for each question, and thus gain stronger robustness to unreliable answers from some low-quality workers. Moreover, as illustrated in Fig. 6, truth discovery outperforms majority voting in answer aggregation, and the personalized contract design in PINTION achieves higher aggregation accuracy than the single-contract baselines.

Impact of Worker Quality Level: Intuitively, truth discovery accuracy is inherently correlated with workers' answer quality before perturbation, which is reflected by the probability of providing correct answers p_w. We simulate different p_w via changing the value of the parameter a of the uniform distribution $\mathbb{U}(a, 1)$, from which p_w of high-quality workers are sampled. Clearly, larger value of a indicates higher overall worker quality. The performance comparison when a ranges from 0.6 to 0.85 is shown in Fig. 7, from which we can see that a higher worker quality before perturbation, leads to better accuracy in final answer aggregation. As for the comparison between truth discovery and majority voting, and the comparison between PINTION and the single-contract mechanism, consistent results are observed from Fig. 7.

C. Experiments on Real-world Dataset

To further validate the effectiveness of PINTION, we conduct experiments on the following two real-world datasets.

1) **Sentiment Analysis For Tweets** [39]: This dataset contains 5000 labels (answers) from 83 Amazon Mechanical Turk workers for 1000 tweets (questions) with hand-labeled sentiment (i.e., true answers). In order to estimate worker quality more accurately, we only include workers who provide answers to more than 5 questions in the experiment.
2) **Duck Dataset** [40]: This dataset contains binary judgments about whether a duck appears in a picture. We utilize a subset of it, which includes judgments (answers) from 39 MTurk annotators (workers) for 108 images (questions).

The above-mentioned datasets are workers' original answers. Similar to synthetic experiments, workers will perturb their original answers according to the contracts they signed with the platform, and truth discovery is conducted on the perturbed answers. Since the number of workers here is not that large, we assume that they are uniformly distributed in $K = 8$ privacy groups, and the privacy preference of each group is also sampled from $\mathbb{U}(15, 40)$.

We now investigate the impact of budget on the truth discovery accuracy using these two datasets. Consistent results are observed from Fig. 8 with Fig. 9. Specifically, truth discovery outperforms majority voting under both complete and incomplete information models. Moreover, the platform achieves higher aggregation accuracy under complete information model, as the contracts are designed to exactly provide all workers with zero utility, and thus the budget is fully utilized to incentivize workers to choose lower PPLs, promising lower error rate. Finally, the results can demonstrate the superiority of our personalized contract design in PINTION compared to the single-contract baselines.

VIII. Conclusions

This paper presented PINTION, a personalized privacy-preserving incentive mechanism for truth discovery in crowdsourced question answering systems based on contract theory, which provides personalized payments for workers with different privacy preferences as a compensation for privacy cost, while ensuring accurate truth discovery. The basic idea of PINTION is that each worker will sign a contract with the platform, which specifies a personalized PPL and the corresponding payment, and then submits perturbed answers according to that PPL in return for that payment. Specifically, a set of optimal contracts are respectively designed under both complete and incomplete information models, which maximizes the truth discovery accuracy, while satisfying some desirable properties, including budget feasibility, individual rationality, and incentive compatibility. We conduct extensive experiments on both synthetic and real-world datasets to validate the feasibility and effectiveness of PINTION.

Acknowledgment

This work was supported in part by the National Key R & D Program of China under Grant 2017YFE0101300, the National Natural Science Foundation of China under Grant 61773344 and Grant 61872274, and the Natural Science Foundation of Zhejiang Province, China, under Grant LZ19F010003, and financially supported by fund from Hubei Province Key Laboratory of Intelligent Information Processing and Real-time Industrial System (Wuhan University of Science and Technology).

REFERENCES

[1] A. I. Chittilappilly, L. Chen, and S. Amer-Yahia, "A survey of general-purpose crowdsourcing techniques," *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, no. 9, pp. 2246–2266, 2016.

[2] F. Daniel, P. Kucherbaev, C. Cappiello, B. Benatallah, and M. Allahbakhsh, "Quality control in crowdsourcing: A survey of quality attributes, assessment techniques, and assurance actions," *ACM Computing Surveys (CSUR)*, vol. 51, no. 1, p. 7, 2018.

[3] X. Zhang, G. Xue, R. Yu, D. Yang, and J. Tang, "Truthful incentive mechanisms for crowdsourcing," in *2015 IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2015, pp. 2830–2838.

[4] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Exploiting mobile crowdsourcing for pervasive cloud services: challenges and solutions," *IEEE Communications Magazine*, vol. 53, no. 3, pp. 98–105, 2015.

[5] Y. Tong, L. Chen, and C. Shahabi, "Spatial crowdsourcing: challenges, techniques, and applications," *Proceedings of the VLDB Endowment*, vol. 10, no. 12, pp. 1988–1991, 2017.

[6] Z. Wang, J. Hu, Q. Wang, R. Lv, J. Wei, H. Chen, and X. Niu, "Task-bundling-based incentive for location-dependent mobile crowdsourcing," *IEEE Communications Magazine*, vol. 57, no. 2, pp. 54–59, 2019.

[7] Y. Li, C. Miao, L. Su, J. Gao, Q. Li, B. Ding, Z. Qin, and K. Ren, "An efficient two-layer mechanism for privacy-preserving truth discovery," in *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*. ACM, 2018, pp. 1705–1714.

[8] B. I. Aydin, Y. S. Yilmaz, Y. Li, Q. Li, J. Gao, and M. Demirbas, "Crowdsourcing for multiple-choice question answering," in *Twenty-Sixth IAAI Conference*, 2014.

[9] P. Rajpurkar, J. Zhang, K. Lopyrev, and P. Liang, "Squad: 100,000+ questions for machine comprehension of text," *arXiv preprint arXiv:1606.05250*, 2016.

[10] J. Eriksson, L. Girod, B. Hull, R. Newton, S. Madden, and H. Balakrishnan, "The pothole patrol: using a mobile sensor network for road surface monitoring," in *Proceedings of the 6th international conference on Mobile systems, applications, and services*. ACM, 2008, pp. 29–39.

[11] L. O'Neill, F. Dexter, and N. Zhang, "The risks to patient privacy from publishing data from clinical anesthesia studies," *Anesthesia & Analgesia*, vol. 122, no. 6, pp. 2017–2027, 2016.

[12] Y. Zheng, G. Li, Y. Li, C. Shan, and R. Cheng, "Truth inference in crowdsourcing: Is the problem solved?" *Proceedings of the VLDB Endowment*, vol. 10, no. 5, pp. 541–552, 2017.

[13] J. Zhang, V. S. Sheng, J. Wu, and X. Wu, "Multi-class ground truth inference in crowdsourcing with clustering," *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, no. 4, pp. 1080–1085, 2015.

[14] F. Ma, Y. Li, Q. Li, M. Qiu, J. Gao, S. Zhi, L. Su, B. Zhao, H. Ji, and J. Han, "Faitcrowd: Fine grained truth discovery for crowdsourced data aggregation," in *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM, 2015, pp. 745–754.

[15] X. Zhang, Y. Wu, L. Huang, H. Ji, and G. Cao, "Expertise-aware truth analysis and task allocation in mobile crowdsourcing," in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2017, pp. 922–932.

[16] Q. Li, Y. Li, J. Gao, B. Zhao, W. Fan, and J. Han, "Resolving conflicts in heterogeneous data by truth discovery and source reliability estimation," in *Proceedings of the 2014 ACM SIGMOD international conference on Management of data*. ACM, 2014, pp. 1187–1198.

[17] Ú. Erlingsson, V. Pihur, and A. Korolova, "Rappor: Randomized aggregatable privacy-preserving ordinal response," in *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*. ACM, 2014, pp. 1054–1067.

[18] Y. Zhang, C. Jiang, L. Song, M. Pan, Z. Dawy, and Z. Han, "Incentive mechanism for mobile crowdsourcing using an optimized tournament model," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 4, pp. 880–892, 2017.

[20] D. Yang, G. Xue, X. Fang, and J. Tang, "Crowdsourcing to smartphones: Incentive mechanism design for mobile phone sensing," in *Proceedings of the 18th annual international conference on Mobile computing and networking*. ACM, 2012, pp. 173–184.

[19] H. Wang, S. Guo, J. Cao, and M. Guo, "Melody: A long-term dynamic quality-aware incentive mechanism for crowdsourcing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 29, no. 4, pp. 901–914, 2017.

[21] H. Jin, L. Su, and K. Nahrstedt, "Theseus: Incentivizing truth discovery in mobile crowd sensing systems," in *Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. ACM, 2017, p. 1.

[22] Y. Wang, Z. Cai, G. Yin, Y. Gao, X. Tong, and G. Wu, "An incentive mechanism with privacy protection in mobile crowdsourcing systems," *Computer Networks*, vol. 102, pp. 157–171, 2016.

[23] H. Jin, L. Su, B. Ding, K. Nahrstedt, and N. Borisov, "Enabling privacy-preserving incentives for mobile crowd sensing systems," in *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2016, pp. 344–353.

[24] Y. Wang, Z. Cai, X. Tong, Y. Gao, and G. Yin, "Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems," *Computer Networks*, vol. 135, pp. 32–43, 2018.

[25] H. Jin, L. Su, H. Xiao, and K. Nahrstedt, "Inception: Incentivizing privacy-preserving data aggregation for mobile crowd sensing systems," in *Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. ACM, 2016, pp. 341–350.

[26] ——, "Incentive mechanism for privacy-aware data aggregation in mobile crowd sensing systems," *IEEE/ACM Transactions on Networking (TON)*, vol. 26, no. 5, pp. 2019–2032, 2018.

[27] Y. Wang, G. Norice, and L. F. Cranor, "Who is concerned about what? a study of american, chinese and indian users' privacy concerns on social network sites," in *International conference on trust and trustworthy computing*. Springer, 2011, pp. 146–153.

[28] M. J. Franklin, D. Kossmann, T. Kraska, S. Ramesh, and R. Xin, "CrowdDB: answering queries with crowdsourcing," in *Proceedings of the 2011 ACM SIGMOD International Conference on Management of data*. ACM, 2011, pp. 61–72.

[29] J. Song, H. Wang, Y. Gao, and B. An, "Active learning with confidence-based answers for crowdsourcing labeling tasks," *Knowledge-Based Systems*, vol. 159, pp. 244–258, 2018.

[30] Y. Li, J. Gao, C. Meng, Q. Li, L. Su, B. Zhao, W. Fan, and J. Han, "A survey on truth discovery," *ACM Sigkdd Explorations Newsletter*, vol. 17, no. 2, pp. 1–16, 2016.

[31] J. Gao, Q. Li, B. Zhao, W. Fan, and J. Han, "Truth discovery and crowdsourcing aggregation: A unified perspective," *Proceedings of the VLDB Endowment*, vol. 8, no. 12, pp. 2048–2049, 2015.

[32] N. B. Shah and D. Zhou, "Double or nothing: Multiplicative incentive mechanisms for crowdsourcing," in *Advances in neural information processing systems*, 2015, pp. 1–9.

[33] T. Luo, S. K. Das, H. P. Tan, and L. Xia, "Incentive mechanism design for crowdsourcing: An all-pay auction approach," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 7, no. 3, p. 35, 2016.

[34] Z. Zhang, S. He, J. Chen, and J. Zhang, "REAP: An efficient incentive mechanism for reconciling aggregation accuracy and individual privacy in crowdsensing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 12, pp. 2995–3007, 2018.

[35] A. Chaudhuri, "Randomized response; theory and techniques," Tech. Rep., 1988.

[36] A. Ghosh and A. Roth, "Selling privacy at auction," *Games and Economic Behavior*, vol. 91, pp. 334–346, 2015.

[37] X. Yin, J. Han, and S. Y. Philip, "Truth discovery with multiple conflicting information providers on the web," *IEEE Transactions on Knowledge and Data Engineering*, vol. 20, no. 6, pp. 796–808, 2008.

[38] L. Tian, J. Li, W. Li, B. Ramesh, and Z. Cai, "Optimal contract-based mechanisms for online data trading markets," *IEEE Internet of Things Journal*, 2019.

[39] B. Mozafari, P. Sarkar, M. J. Franklin, M. I. Jordan, and S. Madden, "Active learning for crowd-sourced databases," *CoRR*, vol. abs/1209.3686, 2012.

[40] P. Welinder, S. Branson, P. Perona, and S. J. Belongie, "The multidimensional wisdom of crowds," in *Advances in neural information processing systems*, 2010, pp. 2424–2432.