LoPub: High-Dimensional Crowdsourced Data Publication with Local Differential Privacy

Xuebin Ren, Chia-Mu Yu, Weiren Yu, Shusen Yang, Xinyu Yang, Julie A. McCann, and Philip S. Yu

I. INTRODUCTION

Nowadays, with the development of various integrated sensors and crowd sensing systems, the crowdsourced information from all aspects can be collected and analyzed among various data attributes to better produce rich knowledge about the group [19], [47], thus benefiting everyone in the crowdsourced system [24]. Particularly, with high-dimensional crowdsourced data (data with multiple attributes), a lot of potential information and rules behind the data can be mined or extracted to provide accurate dynamics and reliable prediction for both group and individuals [27]. For example, both individual electricity usage and community-wide electricity usage should be captured to achieve the real-time community-aware pricing in the smart grid, which integrates the distributed energy generation as well as consumption [29], [56]. People’s historical medical records and genetic information [4], [32] can be collected and mined to help hospital staff better diagnose and monitor patients’ health status. Various environment monitoring data collected from smart phone users can make urban planning more efficient and people’s daily life more convenient [23].

However, the privacy of participants can be easily inferred or identified due to the publication of crowdsourced data [17], [33], [43], especially high-dimensional data, even though some existing privacy-preserving schemes are used. The reasons for the privacy leak are two-fold:

- **Non-local Privacy.** Most existing work for privacy protection focus on centralized datasets under the assumption that the server is trustworthy. However, in crowdsourced scenarios, direct data aggregation from distributed users can give adversaries (such as curious server and misbehaved insiders) the opportunity to identify individual privacy, even if end-to-end encryption is used. Despite the privacy protection against difference and inference attacks from aggregate queries, individual’s data may still suffer from privacy leakage before aggregation because of no guaranteed privacy on the user side (i.e., local privacy [6], [9], [20], [21]).

- **Curse of High-dimensionality.** In crowdsourced systems, high-dimensional data is ubiquitous. With the increase of data dimension, some existing privacy-preserving techniques like differential privacy [10] (a de-facto standard privacy paradigm), if straightforwardly applied to multiple attributes with high correlations, will become vulnerable, thereby increasing the success ratio of many reference attacks like cross-checking. According to the combination theorem [31], differential privacy degrades exponentially when multiple correlated queries are processed. From the aspect of utility, baseline differential privacy algorithms can hardly achieve reasonable scalability and desirable data accuracy due to the dimensional correlations [48].

In addition to the privacy vulnerability, a large scale of various data records collected from distributed users can imply the inefficiency of data processing. Especially in IoT applications, the ubiquitous but resource-constrained sensors and infrastructures require extremely high efficiency and low overhead. For example, privacy-preserving real-time pricing mechanism requires not only effective privacy guarantee for individuals’ electricity usages but also fast response to the dynamic changes of the demands and supplies in the smart grid [29]. Thus, it is important to provide an efficient privacy-preserving method to publish the crowdsourced high-dimensional data.

In addressing the above issues, various existing schemes demonstrated their effectiveness in terms of different perspectives. One is to provide local privacy for distributed users [14], while some recent work [40] [16] have been proposed to provide a local privacy guarantee for individuals in data aggregations. However, these schemes are either inefficient or not applicable for high-dimensional data [46] because of the high computation complexity and great utility loss. The other is to privately release high dimensional data [8] [46] [7]. For example, Chen et al. [7] proposed to achieve differential privacy on compacted attribute clusters after dimension reduction according to the attribute correlations. However, these schemes mainly deal with the centralized dataset without local privacy guarantee for distributed data contributors. To overcome the compatibility problem between those schemes, we propose a novel scheme to publish high-dimensional crowdsourced data while guaranteeing local privacy.

A. Contribution

Our major contributions are summarized as follows.

- In this paper, we propose a locally privacy-preserving scheme for crowdsensing systems to collect and build high dimensional data from the distributed users. Particularly, we propose an efficient algorithm for multivariate joint distribution estimation and a combined algorithm to improve the existing estimation algorithms in order to achieve both high efficiency and accuracy.
• Based on the distribution and correlation information, the dimensionality and sparsity in the original dataset can be reduced by splitting the dataset into many compacted clusters.
• After learning the marginal distribution in these compacted clusters, the server can draw a new dataset from these compacted clusters, thus achieving an approximation of the whole original crowd data while guaranteeing local privacy for individuals.
• We implement and evaluate our schemes on different real-world datasets, experimental results show that our scheme is both efficient and effective in marginal estimation as well as high-dimensional data releasing.

B. Organization

The paper is organized as follows: In Section III, we introduce the system model in our paper. In Section IV, we present preliminaries of our approach. Then, Section V presents our proposed schemes in detail. In Section VI, we present the experiment results to validate the efficiency and effectiveness of our schemes. Last, we concludes this paper in Section VII.

II. RELATED WORK

A. High-dimensional data

To solve the privacy issue in data releasing, differential privacy [10] was proposed to lay a mathematical privacy foundation by adding proper randomness. Examples of the use of differential privacy include the privacy-preserving data aggregation operations, where differential privacy of individuals can be guaranteed by injecting carefully-calibrated Laplacian noise [7], [15], [22], [26], [37], [55], [46]. The techniques for non-interactive differential privacy [11], [12] suffer from "curse of dimensionality" [7], [46]. Particularly, the combination theorems [31] have pointed out that differential privacy degrades when multiple related queries are processed [35]. To deal with the correlations in high-dimensional data, different schemes have been proposed [7], [8], [22], [30], [42], [46], [48].

For example, Liu et al. [30] proposed the notion of dependent differential privacy (DDP) and dependent perturbation mechanism (DPM) to both measure and preserve the privacy with consideration of the dependence and correlations. Another solution to mitigate correlation problem is to group the correlated records into clusters and then achieve privacy on each low-dimensional cluster. Based on the data structure of dimensions, these solutions can be categorized into two classes: homogeneous and heterogeneous.

1) Homogeneous data means the data structure of all dimensions is the same. For example, in the massive text document, each dimension represents the frequency histogram of a text on the distinct words. Since the data structure is the same, basic distance metrics can be simply used to cluster the similar dimensions. For example, Kellaris et al. [22] proposed to group the data attributes with similar sensitivities together to reduce the overall sensitivity. Based on the similar idea, Wang et al. [42] proposed to group the data streams with the similar trend to achieve efficient privacy on data streams. However, both value and trend similarities cannot truly reflect the correlations in heterogeneous data.

2) Heterogeneous data refers to the high-dimensional data with different dimensions, i.e., different attribute domains. For example, personal profiles may include various attributes like gender, age, education status. Intuitive distance metrics cannot measure the correlations among heterogeneous. Therefore, Zhang et al. [46] proposed to calculate the mutual information of attribute-parent pairs and then model the correlations via a Bayesian network. Li et al. [25] proposed to use copula functions to model joint distribution for high-dimensional data. However, Copula functions cannot handle attributes with small domains, which limits its application. Chen et al. [4] proposed to directly calculate the mutual information between pairwise dimensions and build a dependency graph and junction tree to model the correlations.

However, in existing schemes [7], [46] as depicted by Figure 1 the original dataset are plainly accessed twice to learn the correlations among attributes and generate the distributions for clusters. Although calibrated noises are added separately (the 4th and 7th step) on the aggregation results, individual’s privacy can only be protected against the third parties from the aggregation but still be threatened by the server, who collects and aggregates the data. In addition, the two accesses are computed separately without a consistent privacy guarantee. That is, two differential privacy budgets were allocated separately but it is not clear about how to allocate the privacy budget to achieve both sufficient privacy guarantee and utility maximization. Besides, although the entire high dimensional data can be reduced into several low-dimensional clusters. The sparsity caused by combinations in each cluster still exists and may lead to lower utility. In contrast to the totally centralized setting in [2], Su et al. [39] proposed a distributed multi-party setting to publish new dataset from multiple data curators. However, their multi-party computation can only protect the privacy between data servers. Instead, individual’s local privacy in a data server cannot be guaranteed.

Also, for high-dimensional data, to show the crowd statistics and draw the correlations between attributes (variables), both privacy-preserving histogram (univariate distribution) [3] and contingency table1 (multivariate joint distribution) [44] are widely investigated. However, these work can not provide local privacy guarantee, thus being unable to apply to crowdsourced systems.

B. Local privacy

However, the schemes mentioned above mainly deal with the centralized dataset. There could be scenarios, where distributed users contribute to the aggregate statistics. Despite the privacy protection against difference and inference attacks from aggregate queries, individual’s data may also suffer from privacy leakage before aggregation. Hence, the notion of local privacy has been proposed to provide local privacy guarantee for distributed users. In addition, local privacy from the end

1A contingency table is a visualised table widely used in statistic areas that displays multivariate joint distribution of attributes.
user can ensure the consistency of the privacy guarantee when there are multiple access to users’ data. Instead, non-local privacy schemes like [40] and [7] have to split and assign proper privacy budgets to different steps while accessing to the original data.

Local privacy schemes mainly focus on achieving differentially private noise via combining the data from distributed source. Many different distributed differential privacy techniques were proposed [14]. However, the local noise may be too small to cover the original data. Recently, local privacy aims to learn particular aggregation features from distributed users with some public knowledge [14], [16], [17], [40]. Sun et al. [40] proposed a percentile aggregation scheme for monitoring distributed stream. In this scheme, the possible range information is public known. For example, Groat et al. [17] proposed the technique negative surveys, which is based on frequencies of different strings in a candidate set. Their scheme EMD [16]. Also, our method has relatively lower communication cost, time, and storage complexity.

### TABLE I: Comparison of LoPub with existing methods

| Comparison | LoPub [Ours method] | RAPPOR [14] | EM [16] | JTree [7] |
|------------|---------------------|-------------|---------|----------|
| Local Privacy | Y | Y | Y | Y |
| High-Dimensional | Y | Y | Y | Y |
| Communication | O(Nd) | O(1) | O(1) | O(1) |
| Time Complex | Low | Low | Low | Low |
| Space Complex | Low | Low | Low | Low |

### III. System Model

The system model is depicted in Figure 2 where a lot of users and a central server are interconnected, constituting a crowdsourcing system. The users first collect high-dimensional data records from multiple attributes at the same time, and then send these data to the central server. The server gathers all the data and estimates high-dimensional crowdsourced data distribution with local privacy, aiming to release a privacy-preserving dataset to third-parties for conducting data analysis. In this paper, we mainly focus on data privacy, thus the detailed network model is not emphasised.

**Problem Statement.** Given a collection of data records with $d$ attributes from different users, our goal is to help the central server publish a synthetic dataset that has the approximate joint distribution of $d$ attributes with local privacy. Formally, let $N$ be the total number of users (i.e., data record) and sufficiently large. Let $X = \{X^1, X^2, \ldots, X^N\}$ be the crowdsourced dataset, where $X^i$ denotes the data record from the $i$th user. We assume that there are $d$ attributes $A = \{A_1, A_2, \ldots, A_d\} \subseteq x$. Then each data record $X^i$ can be represented as $X^i = \{x^i_1, x^i_2, \ldots, x^i_d\}$, where $x^i_j$ denotes the $j$th element of the $i$th user record. For each attribute $A_j (j = 1, 2, \ldots, d)$, we denote $\Omega_j = \{\omega^j_1, \omega^j_2, \ldots, \omega^j_{|\Omega_j|}\}$ as the domain of $A_j$, where $\omega^j_i$ is the $i$th attribute value of $\Omega_j$ and $|\Omega_j|$ is the cardinality of $\Omega_j$.

With the above notations, our problem can be formulated as follows: Given a dataset $X$, we aim to release a locally privacy-preserving dataset $X^*$ with the same attributes $A$ and number $N$ of users in $X$ such that

$$P_X(A_1 \ldots A_d) \approx P_X(A_1 \ldots A_d) \quad (1)$$

and

$$P_X(A_1 \ldots A_d) \triangleq P_X(x_1^i = \omega_1, \ldots, x_d^i = \omega_d) \quad (2)$$

for $i = 1, \ldots, N$, and $\omega_1, \ldots, \omega_d \in \Omega_d$ where $P_X(x_1^i = \omega_1, \ldots, x_d^i = \omega_d)$ is defined as the $d$-dimensional (multivariate) joint distribution on $X$.

To focus our research on data privacy, we assume that the central server and users are all honest-but-curious in the sense that they will honestly follow the protocols in the system without maliciously manipulating their received data. However, they may be curious about others’ data privacy and even collude to infer others’ data. In addition, the central server and users share the same public information, such as the privacy-preserving protocols (including the hash functions used) and the domain $\Omega_j$ for each attribute $A_j (j = 1, 2, \ldots, d)$.

### IV. Preliminaries

#### A. Differential Privacy

Differential privacy is the de-facto standard for privacy guarantee on data. It limits the adversaries’ ability of inferring the participation or absence of any user in a data set via adding carefully calibrated noise to the query results on the data set. The definition of $\epsilon$-differential privacy can be found in [10]. $\epsilon$ is the privacy budget (or privacy parameter) to specify the level of privacy protection and smaller $\epsilon$ means better privacy. According to the combination theorem [35], extra privacy budget will be required when multiple differential privacy mechanisms are applied on related queries. Once $\epsilon$ is run out, no more differential privacy can be guaranteed.

If a mechanism $M$ is $\epsilon$-differential privacy on dataset $D$ and a new dataset $D'$ sampled from $D$ with uniformly sampling rate $\beta$. Then, querying $M$ on $D'$ can guarantee a $\ln(1+\beta(\epsilon^\epsilon - 1))$—differential privacy for dataset $D$. [28]

#### B. Local Differential Privacy

Generally, differential privacy focuses on centralized database and implicitly assumes data aggregation is trustworthy. Aiming to eliminate this assumption, local privacy was proposed for crowdsourced systems to provide a stringent privacy guarantee that data contributors trust no one [9], [21]. A formal definition of local differential privacy is given below.
Definition 1: For any user $i$, a mechanism $\mathcal{M}$ satisfies $\epsilon$-local differential privacy (or simply local privacy) if for any two data records $X^i, Y^i \in \Omega_1 \times \cdots \times \Omega_d$, and for any possible privacy-preserving outputs $\hat{X}^i \in \text{Range}(\mathcal{M})$,

$$P \left( \mathcal{M}(X^i) = \hat{X}^i \right) \leq e^\epsilon \cdot P \left( \mathcal{M}(Y^i) = \hat{X}^i \right),$$

where the probability is taken over $\mathcal{M}$’s randomness and $\epsilon$ has similar impact on privacy as in the ordinary differential privacy.

Local privacy has many applications. A typical example is the randomized response technique [44], which is widely used in the survey of people’s “yes or no” opinions about a private issue. Participants of the survey are required to give their true answers with a certain probability or random answers with the remaining probability. Due to the randomness, the surveyor cannot determine the true answers of participants individually (i.e., local privacy is guaranteed) while can predict the true proportions of alternative answers.

C. RAPPOR based Local Privacy

Recently, RAPPOR (Randomized Aggregatable Privacy-Preserving Ordinal Response) has been proposed for statistics aggregation [14]. RAPPOR is only applicable to one or two dimensional crowdsourced data for estimating data distribution with local privacy. The basic idea of RAPPOR is the extension of the randomized response technique. In the randomized response technique, the candidate set of the domain $\Omega$ is only a binary input $\{0, 1\}$ denoting “yes or no”, whereas RAPPOR generalizes the candidate set of $\Omega$ to multiple inputs such that a sufficiently long $\{0, 1\}$ bit string can be applied to the domain $\Omega$.

On users, RAPPOR consists of two phases:

1) Feature Assignment. In this phase, the dataset $X$ has only one attribute with the domain $\Omega$. For each candidate value $\omega \in \Omega$, several hash functions are used to transform $\omega$ into a $m$-bit $\{0, 1\}$ string $S$ (a.k.a. a Bloom filter). Once $m$ and the number of hash functions are well chosen, this transformation can maximize the uniqueness of a bit string $S$ to represent any attribute value $\omega \in \Omega$. As suggested by [38], $m$ is proportional to the domain size $|\Omega|$, i.e., $m \propto |\Omega|$.

2) Feature Cloaking. After the Bloom filter $S$ is obtained, each bit in $S$ will be randomized to 0 or 1 with a certain probability, or remains unchanged with the remaining probability. This randomness is important as it endows the privacy on the original data. The more randomness, the better privacy.

On the central server, RAPPOR first gathers randomized Bloom filters from different users, and then estimates the univariate distribution as follows:

1) Aggregation. Once gathered by the central server, all the bit strings will be summed up bitwise. Then the true count of each bit can be estimated based on the randomness of the bit strings.

2) Feature Rebuilding. The hash functions used on the user side are replayed on the server side to reconstruct the Bloom filters for each $\omega \in \Omega$.

3) Distribution Estimation. Taking the Bloom filters as the feature variables, the server can estimate the univariate distribution of the single attribute via linear regression.

It is important to note that RAPPOR is only efficient in low dimensional data because when the dimension $k$ is high, the length $m_{\text{RAPPOR}}$ of Bloom filters over the multi-attribute domain $\Omega_1 \times \Omega_2 \times \cdots \times \Omega_k$ will become

$$m_{\text{RAPPOR}} \propto |\Omega_1 \times \Omega_2 \times \cdots \times \Omega_k| = \prod_{j=1}^{k} |\Omega_j|,$$

Fig. 1: Main procedures of high-dimensional data publishing without local privacy

Fig. 2: An architecture of distributed high-dimensional private data collecting and publishing
which requires exponential storage space in terms of $k$.

To address this problem, Fanti et al. [10] proposed an EM (Expectation Maximization) based association learning scheme, which extends the 1-dimensional RAPPOR to estimate the 2-dimensional joint distribution. First, a bivariate joint distribution is initialized uniformly. Then, for each record, the conditional probability distribution of the true data record, the conditional probability distribution of the true 2-dimensional distribution on each attribute independently. Then, for each record, the conditional probability distribution of the true 2-dimensional Bloom filters given the observed noisy record is calculated according to the Bayes’ theorem. Finally, the bivariate joint distribution is updated as the expectation of the conditional probability distributions over all records. By iterating the above steps several rounds, an estimation of the bivariate joint distribution can be obtained. However, repeating scanning all the collected RAPPOR strings in each round of EM algorithm incurs considerable computational complexity.

Some notations used in this paper are listed in Table I.

### V. LoPub: High-dimensional Data Publication with Local Privacy

We propose LoPub, a novel solution to achieve high-dimensional crowdsourced data publication with local privacy. In this section, we first introduce the basic idea behind LoPub and then elaborate the algorithmic procedures in more details.

#### A. Basic idea

Privacy-preserving high-dimensional crowdsourced data publication aims at releasing an approximate dataset with similar statistical information (i.e., statistical distribution defined in Equation (1)) while guaranteeing the local privacy. This problem can be considered in four aspects:

First, to achieve local privacy, some local transformation should be designed on the user side to cloak individuals’ original data record. Then, the central server needs to obtain the statistical information, a.k.a. the distribution of original data. There are two plausible solutions. One is to obtain the 1-dimensional distribution on each attribute independently. Unfortunately, the lack of consideration of correlations between dimensions will lose the utility of original dataset. Another is to consider all attributes as one and compute the $d$-dimensional joint distribution. However, due to combinations, the possible domain will increase exponentially with the number of dimensions, thus leading to both low scalability and the signal-noise-ratio problems [46]. Particularly, with fixed local privacy guarantee, the statistical accuracy of distribution estimation will degrade significantly with the increase of the possible domain and dimensionality. Therefore, next crucial problem is to find a solution for reducing the dimensionality while keeping the necessary correlations. Finally, with the statistical distribution information on low-dimensional data, how to synthesize a new dataset is the remaining problem.

To this end, we present LoPub, a locally privacy-preserving data publication scheme for high-dimensional crowdsourced data. Figure 3 shows the overview of LoPub, which mainly consists of four mechanisms: local privacy protection, multi-dimensional distribution estimation, dimensionality reduction, and data synthesizing.

1) **Local Privacy Protection.** We first propose the local transformation process that adopts randomized response technique to cloak the original multi-dimensional data records on distributed users to provide local privacy for all individuals in the crowdsourced systems. Particularly, we locally transform each attribute value to a random bit string. Then, the locally privacy-preserved data is sent to and aggregated at the central server.

2) **Multi-dimensional Distribution Estimation.** We then propose multi-dimensional joint distribution estimation schemes to obtain both the joint and marginal probability distribution on multi-dimensional data. Inspired by [16], we present an EM-based approach for high-dimensional estimation. Moreover, we present Lasso-based approach for fast estimation at the cost of slight accuracy degradation. Finally, we propose a hybrid approach striking the balance between the accuracy and efficiency.

3) **Dimensionality Reduction.** Based on the multi-dimensional distribution information, we then propose to reduce the dimensionality by identifying mutually-correlated attributes among all dimensions and split the high-dimensional attributes into several compact low-dimensional attribute clusters. In this paper, considering the heterogeneous attributes, we adopt mutual information and undirected dependency graph to measure and model the correlations of attributes, respectively. In addition, we also propose a heuristic pruning scheme to further boost the process of correlation identification.

4) **Synthesizing New Dataset.** Finally, we propose to sample each low-dimensional dataset according to the estimated joint or conditional distribution on each attribute cluster, thus synthesizing a new privacy-preserving dataset.

#### B. Local Transformation

1) **Design Rationale:** A common framework of locally private distribution estimation is that each individual user applies a local transformation on the data for privacy protection and then sends the transformed data to the server. The server estimates the joint distribution according to the transformed data. Local transformation in our design includes two key steps: one is mapping into Bloom filters and the other is adding randomness. Particularly, Bloom filter over $\Omega$ with multiple hash functions can hash all the variables in the domain into a pre-defined space. Thus, the unique bit strings are the representative features of the original report. Then, after

| TABLE II: Notation |
|---------------------|
| $N$ | number of users (data records) in the system |
| $X$ | entire crowdsourced dataset on the server side |
| $X^i$ | data record from the $i$th user |
| $\mathbb{X}_i$ | set of all attribute clusters |
| $A_j$ | $j$th attribute of $X$ |
| $\Omega_j$ | domain of $A_j$ |
| $H_j(x)$ | hash functions for $A_j$ that map $x$ into a Bloom filter |
| $\tilde{S}_j^i$ | Bloom filter of $s_j^i$ ($\tilde{S}_j^i = H_j(x_j^i)$) |
| $s_j^i[b]$ | $b$th bit of $\tilde{S}_j^i$ |
| $s_j^i$ | randomized Bloom filter of $s_j^i$ |
| $\hat{s}_j^i[b]$ | $b$th bit of $s_j^i$ |
| $m_j$ | length of $s_j^i$ |
| $f$ | probability of randomly flipping a bit of a Bloom filter |
privacy protection by randomized responses, a large number of samples with various levels of noise are generated by individual users. After aggregation, the central server obtain a large sample space with random noises. As a result, one may estimate the distribution from the noised sample space by taking advantage of machine learning techniques such as EM algorithm and regression analysis.

Under the above framework, a key observation can be made: if features are mutual-independent, one can easily conclude that the combinations of features from different candidate sets are also mutual-independent. Therefore, when Bloom filters of each attribute are mutual-independent (i.e., no collisions for all bits), then the Cartesian product of Bloom filters of different attributes are mutual-independent. In this sense, with mutual-independent features of Bloom filters, existing machine learning techniques like EM and Lasso regression are effective for the multivariate distribution estimation. Some notations used in this paper are listed in Table II.

2) Algorithmic Procedures of Local Transformation: Before describing the distribution estimation, we present that details about the local transformation. In essence, local transformation consists of three steps:

1) On each ith user, suppose we have an original data record $X^i = \{x^i_1, x^i_2, \ldots, x^i_d\}$ with $d$ attributes. For each attribute $A_j (j = 1, \ldots, d)$, we employ hash functions $\mathcal{H}_j(\cdot)$ to map $x^i_j$ to a length-$m_j$ bit string $s^i_j$ (called a Bloom filter). That is,

$$s^i_j = \mathcal{H}_j(x^i_j) \quad (\forall j = 1, \ldots, d)$$

2) Each bit $s^i_j[b]$ ($b = 1, 2, \ldots, m_j$) in $s^i_j$ is randomly flipped into 0 or 1 according to the following rule:

$$\tilde{s}^i_j[b] = \begin{cases} s^i_j[b], & \text{with probability of } 1 - f \\ 1, & \text{with probability of } f/2 \\ 0, & \text{with probability of } f/2 \end{cases} \quad (5)$$

where $f \in (0, 1)$ is a user-controlled flipping probability that quantifies the level of randomness for local privacy.

3) Having flipped each bit string $s^i_j$ bit by bit into randomized Bloom filter $\tilde{s}^i_j (j = 1, \ldots, d)$, we concatenate $\tilde{s}^i_1, \ldots, \tilde{s}^i_d$ to obtain a stochastic $(d \cdot m_j)$-bit vector:

$$[\tilde{s}^i_1[m_1], \ldots, \tilde{s}^i_1[m_1], \ldots, \tilde{s}^i_2[m_2], \ldots, \tilde{s}^i_d[m_d]]$$

and send it to the server with guaranteed local privacy.

---

### Table III: An example of census data $X$ of college alumni

| Age  | Gender | Education | Income Level |
|------|--------|-----------|--------------|
| 29   | M      | college   | working      |
| 35   | F      | master    | low-middle   |
| 45   | F      | college   | working      |
| \ldots | \ldots | \ldots | \ldots |
| 49   | M      | PhD       | up-middle    |

### Table IV: Attribute domain information of dataset $X$

| $A_j$ | $\Omega_j$ | $|\Omega_j|$ |
|-------|-------------|------------|
| Age   | [25, 60]    | 35         |
| Gender| {M, F}      | 2          |
| Educa-| {college, master, PhD} | 3          |
| Income| {working, low-middle, up-middle, affluent} | 4          |

### Table V: Bloom strings of attribute domain $\mathcal{H}_j(\Omega_j)$

| $A_j$ | $\mathcal{H}_j(\Omega_j)$ | $|\mathcal{H}_j(\Omega_j)|$ |
|-------|--------------------------|-----------------------------|
| Age   | \{100100111, \ldots, 01010110\} | 35                          |
| Gender| \{01, 10\}               | 2                           |
| Educa-| \{0101, 0110, 1100\}     | 3                           |
| Income| \{0110, 0011, 1001, 1100\} | 4                           |

### Table VI: Privacy-preserving bit strings of $X$

| $u_k$ | $\mathcal{H}_1(\Omega_j)$ | $\mathcal{H}_2(\Omega_j)$ | $\mathcal{H}_3(\Omega_j)$ | $\mathcal{H}_4(\Omega_j)$ | $\mathcal{H}_5(\Omega_j)$ |
|-------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| $u_1$ | 010101110010111          | 10                        | 0111                      | 0100                      | 0100                      |
| $u_2$ | 0110001110010010          | 00                        | 1100                      | 0100                      | 0100                      |
| $u_N$ | 1101010000110110110      | 00                        | 0110                      | 1111                      | 1111                      |

---

**Example 1:**

Table III shows a simplified example of original census dataset $X$ with 4 attributes \{"Age","Gender", "Education", "Income Level"\}, where each record is contributed by user $u_i$, $1 \leq i \leq N$. Consider data record $X^2 = \{35, F, Master, Low-middle\}$ on 2nd user. To guarantee local privacy, we first use hash functions $\mathcal{H}_j(\cdot)$ to map $j$th element of $X^2$ into a bit string. Next, having been randomly flipped bit by bit, these bit strings become

$$\mathcal{H}_1(35) = \{01011001\} \Rightarrow \{10021011\}$$

$$\mathcal{H}_2(F) = \{10\} \Rightarrow \{00\}$$

$$\mathcal{H}_3(master) = \{0110\} \Rightarrow \{1110\}$$

$$\mathcal{H}_4(low-middle) = \{0011\} \Rightarrow \{0011\}$$

where underlined bits have been changed according to Equation (5). Finally, the concatenation of these randomized bit strings for each attribute yields a privacy-preserving bit string for the entire record $X^2$

$$[100210111101001\underline{00}11100111]$$

which will be sent to the central server under local privacy.

Similarly, other users should transform their data in a same way. Table VI shows the example of transformed privacy-preserving report strings received by the server.

**Parameters Setup:** According to the characteristic of Bloom filter [38], given the false positive probability $p$ and the number $|\Omega_j|$ of elements to be inserted, the optimal length $m_j$ of Bloom filter can be calculated as

$$m_j = \frac{\ln(1/p)}{(\ln 2)^2 |\Omega_j|}. \quad (6)$$
Furthermore, the optimal number $h_j$ of hash functions is
\[
h_j = \frac{m_j}{|\Omega_j|} \ln 2 = \frac{\ln(1/p)}{(\ln 2)^2}. \tag{7}
\]
So, the optimal $h = \frac{\ln(1/p)}{(\ln 2)^2}$ for all dimensions.

**Privacy Analysis:** Because local transformation is performed by the individual user, no one can obtain the original record $X_i$, local privacy can be easily achieved and we only have to analyze the privacy guarantee on the user side. According to the conclusion in [14], differential privacy obtained for each attribute on the user side is $2h \ln ((2 - f)/f)$, where $h$ is the number of hash functions in the Bloom filter and $f$ is the probability that a bit vector was flipped.

Since both hash operations and randomized response on all attributes are independent, then as pointed by the composition theorem [31], the overall differential privacy achieved on the user side should be
\[
\epsilon = 2dh \ln ((2 - f)/f), \tag{8}
\]
where $d$ is the number of dimensions.

Overall, since the same transformation is done by all users independently, this $\epsilon$-local privacy guarantee is equivalent for all distributed users. In the rest of our paper, we will focus on how to achieve a better utility-privacy tradeoff from users’ privacy-preserving high-dimensional data with this privacy guarantee $\epsilon$.

**Communication Overhead:**

**Theorem 1:** The minimal communication cost $C$ after the local transformation is
\[
C = \sum_{j=1}^{d} m_j = \frac{\ln(1/p)}{(\ln 2)^2} \sum_{j=1}^{d} |\Omega_j|. \tag{9}
\]

**Proof** If we assume that the domain of each attribute is publicly known by both users and the server, then the communication cost of non-private collection is basically $\sum_{j=1}^{d} \ln |\Omega_j|$, which is related to the domain size. Nevertheless, in our method with local privacy, the communication cost is $\sum_{j=1}^{d} m_j$, which is related to the length of Bloom filters because only randomly flipped bit strings (not original data record) are sent.

For comparison, under the same condition, when RAPPOR [14] is directly applied to the $k$-dimensional data, all $\Omega_1 \times \cdots \times \Omega_k$ candidate value will be regarded as 1-dimensional data, then the cost is
\[
C_{\text{RAPPOR}} = \frac{\ln(1/p)}{(\ln 2)^2} \prod_{j=1}^{k} |\Omega_j|, \tag{10}
\]
where $\prod_{j=1}^{k} |\Omega_j|$ is due to the size of the candidate set $\Omega_1 \times \cdots \times \Omega_k$. Difference between Equation[9] and [??] is because our LoPub, compared with straightforward RAPPOR, considers the mutual independency between multiple attributes. It should be noted that the Bloom filter length $m_j$ as well as communication cost $C_{\text{LoPub}}$ (or $C_{\text{RAPPOR}}$) is independent from the privacy level achieved.

### C. Multivariate Distribution Estimation with Local Privacy

1) **EM-based Distribution Estimation:** After receiving randomized bit strings, the central server can aggregate them and estimate their joint distribution. However, the existing EM-based estimation [15] for joint distribution estimation is restricted to 2 dimensions, which is impractical to many real-world datasets with high dimensions. Here, we propose an alternative EM-based estimation that can apply to $k$-dimensional dataset ($2 \leq k \leq d$) with provable complexity analysis.

Before illustrating our algorithm, we first introduce the following notations. Without loss of generality, we consider $k$ specified attributes as $A_1$, $A_2$, . . . , $A_k$ and their index collection $C = \{1, 2, \ldots, k\}$. For simplicity, the event $A_j = \omega_j$ or $x_j = \omega_j$ is abbreviated as $\omega_j$. For example, the prior probability $P(x_1 = \omega_1, x_2 = \omega_2, \ldots, x_k = \omega_k)$ can be simplified into $P(\omega_1|\omega_2|\ldots|\omega_k)$ or $P(\omega_2|\omega_3|\ldots|\omega_k)$.

Algorithm[1] depicts our EM-based approach for estimating $k$-dimensional joint distribution. More specifically, it consists of the following five main steps.

#### Algorithm 1 EM-based $k$-Dimensional Joint Distribution

**Input:** $C$: attribute indexes cluster, i.e., $C = \{1, 2, \ldots, k\}$  
$A_j$: $k$-dimensional attributes $\{1 \leq j \leq k\}$  
$\Omega_j$: domain of $A_j$ ($1 \leq j \leq k$)  
$\hat{\delta}_j$: observed Bloom filters ($1 \leq i \leq N$) ($1 \leq j \leq k$)  
$f$: flipping probability  
$\delta$: convergence accuracy  

**Output:** $P(A_C)$: joint distribution of $k$ attributes specified by $C$.

1. initialize $P(\omega_C) = 1/|\Omega_C|$.  
2. for each $i = 1, \ldots, N$ do  
3. for each $j \in C$ do  
4. compute $P(\hat{\delta}_j|\omega_j) = \prod_{b=1}^{m_j}(\frac{1}{2}j^1|b)(1 - j^1-1|b)$,  
5. end for  
6. compute $P(\hat{\delta}_C|\omega_C) = \prod_{j \in C} P(\hat{\delta}_j|\omega_j)$.  
7. end for  
8. initialize $t = 0$, $\forall i$ number of iterations $\forall i$  
9. repeat  
10. for each $i = 1, \ldots, N$ do  
11. for each $(\omega_C) \in \Omega_1 \times \Omega_2 \times \cdots \times \Omega_k$ do  
12. compute $P_t(\omega_C|\hat{\delta}_C) = \frac{P_t(\omega_C)P(\hat{\delta}_C|\omega_C)}{\sum_{\omega_C} P_t(\omega_C)P(\hat{\delta}_C|\omega_C)}$  
13. end for  
14. end for  
15. set $P_{t+1}(\omega_C) = \frac{1}{N} \sum_{i=1}^{N} P_t(\omega(C)|\hat{\delta}_C)$  
16. update $t = t + 1$  
17. until $\max_{\omega_C} P_t(\omega(C)) - \max_{\omega_C} P_{t-1}(\omega(C)) \leq \delta$.  
18. return $P(A_C) = P_t(\omega(C))$.

1) Before executing EM procedures, we set an uniform distribution $P(\omega_1|\omega_2|\ldots|\omega_k) = 1/|\Omega_1|\times|\Omega_2|\times|\Omega_3|\ldots|\Omega_k|$ as the initial prior probability.

**Example 2:** For simplicity, we consider the joint distribution on attributes $A_2$,$A_3$ (a.k.a. “Gender” and “Education”). First, we initialize the probability on each combination as $P(A_2,A_3) = 1/(|\Omega_2|\times|\Omega_3|) = 1/6$.

2) According to Equation[5], each bit $\hat{\delta}_j[b]$ will be changed with probability $\frac{f}{2}$ and remains unchanged with probability $1 - \frac{f}{2}$. By comparing the bits $H_j(\omega_j)$ with the randomized bits, the conditional probability $P(\hat{\delta}_j|\omega_j)$ can be computed (see line 4 of Algorithm[1]).
Example 3: We calculate the conditional probability \( P(\hat{\omega}_i|\hat{\omega}_j) \) of each attribute \( A_j \) \((j = 2, 3)\). For example, on attribute \( A_3 \) (or Education), in the case of privacy parameter \( f = 1/2 \), we have

\[
P(\hat{\omega}_3|A_3 = \text{college}) = \frac{P(\hat{\omega}_3 = \text{college} | H_3 \in \Omega_3)}{P(\hat{\omega}_3 = \text{college} | H_3 \in \Omega_3)} = \frac{0.0011}{0.1011} = 0.0101
\]

Similarly, the conditional probabilities on other combinations can also be obtained.

3) Due to the independence between attributes (and their Bloom filters), the joint conditional probability can be easily calculated by combining each individual attribute, so \( P(\hat{\omega}_1, \hat{\omega}_2, \hat{\omega}_3) = \prod_{i=1}^{N} P(\hat{\omega}_i) \).

Example 4: The joint conditional probability \( P(\hat{\omega}_2 \hat{\omega}_3 | A_2 A_3) \) of attributes \( A_2 A_3 \) can be enumerated. For example, the probability that \( u_1 \) is “a female (Gender=F) alumni with phd degree and low-middle income” can be computed as

\[
P(\hat{\omega}_2 = F, A_3 = \text{phd}) = P(\hat{\omega}_2 | A_2 = F) \times P(\hat{\omega}_3 | A_3 = \text{phd})
\]

Similarly, the conditional probability \( P(\hat{\omega}_2 \hat{\omega}_3 | A_2 A_3) \) on other 5 candidate combinations of \( A_2 A_3 \) can be obtained.

4) Given all the conditional distributions of one particular combination of bit strings, their corresponding posterior probability can be computed by the Bayes’ Theorem,

\[
P(A_2 A_3 | \hat{\omega}_2 \hat{\omega}_3) = \frac{P(\hat{\omega}_2 \hat{\omega}_3 | A_2 A_3) \cdot P(A_2 A_3)}{\sum_{A_2 A_3} \sum_{\hat{\omega}_2 \hat{\omega}_3} P(\hat{\omega}_2 \hat{\omega}_3 | A_2 A_3) \cdot P(A_2 A_3)}
\]

Example 5: Given the privacy-preserving bit string \( \hat{\omega}_2 \hat{\omega}_3 \), the posterior probability \( P(A_2 A_3 | \hat{\omega}_2 \hat{\omega}_3) \) at the first iteration can be computed such as

\[
P(A_2 = F, A_3 = \text{phd} | \hat{\omega}_2 \hat{\omega}_3) = \frac{P(A_2 = F, A_3 = \text{phd}) \cdot P(\hat{\omega}_2 \hat{\omega}_3 | A_2 = F, A_3 = \text{phd})}{\sum_{\omega_2 \in \Omega_2} \sum_{\omega_3 \in \Omega_3} P(A_2 = F, A_3 = \text{phd}) \cdot P(\hat{\omega}_2 \hat{\omega}_3 | A_2 = F, A_3 = \text{phd})}
\]

Similarly, after observing the privacy-preserving bit string 10 0111 0100 (\(S^1\)), all posterior probabilities of different combinations of \( A_2 A_3 \) can be obtained.

5) After identifying posterior probability for each user, we calculate the mean of the posterior probability from a large number of users to update the prior probability. The prior probability is used in another iteration to compute the posterior probability in the next iteration. The above EM-like procedures are executed iteratively until convergence, i.e., the maximum difference between two estimations is smaller than the specified threshold \( \max P_i(\omega_1 \omega_2 \ldots \omega_k) = \max P_{i-1}(\omega_1 \omega_2 \ldots \omega_k) \geq \delta \).

Example 6: For each observed privacy-preserving bit string \( S^i \) \((i = 1, 2, \ldots, N)\), the posterior probability \( P(A_2 = F, A_3 = \text{phd}) \) for each combination can be obtained by the above procedures. Then, the prior probability \( P(A_2 = F, A_3 = \text{phd}) \) is updated by the mean value of \( N \) (here we take the 4 records \( u_1, u_2, u_3, \) and \( u_4 \) in the table) posterior probabilities as

\[
P(A_2 = F, A_3 = \text{phd}) = \frac{1}{N} \sum_{i=1}^{N} P(A_2 = F, A_3 = \text{phd}, |S^i|)
\]

So, instead of initial probability \( P_0(A_2 = F, A_3 = \text{phd}) = 1/6 = 0.1667 \), the updated prior probabilities \( P_1(A_2 = F, A_3 = \text{phd}) \) (should be about 0.1564 in our example) will be used in the next iteration. Similarly, the initial probabilities of other 5 combinations will be updated for the next iteration.

The above algorithm can converge to a good estimation when the initial value is well chosen. EM-based \( k \)-dimensional joint distribution estimation will also fail when converging to local optimum. Especially when \( k \) increases, there will be many local optimum to prevent good convergence because sample space of all combinations in \( \Omega_{j_1} \times \Omega_{j_2} \times \cdots \times \Omega_{j_k} \) explodes exponentially.

Complexity: Before the analysis of complexity, we should note that number of user records \( N \) needs to be sufficiently large according to the analysis in [4], i.e., \( N \gg v^k \), where \( v \) denotes the average size of \( \Omega_j \), otherwise it is difficult to estimate reliably from a small sample space with low signal-noise-ratio.

Theorem 2: Suppose that the average length of \( m_j \) is \( m \) and the average \( |\Omega_j| \) is \( v \). Then, the time complexity of Algorithm I is

\[
O(Nkmv^k + tNv^{2k}).
\]

Proof: EM-based estimation will scan all \( N \) users’ bit strings with the length of \( km \) one by one to compute the conditional probability for \( v^k \) different combinations, the time complexity basically can be estimated as \( O(N(km)(v^k)) \). Also, in the \( t \)th iteration, computing the posterior probability of each combination when observing each bit string will incur the time complexity of \( O(tNv^{2k})^2 \). As a consequence, the overall time complexity is \( O(tNv^{2k} + Nkmv^k) \).

Theorem 3: The space complexity of Algorithm I is

\[
O(Nkm + 2Nv^k).
\]

Proof: In Algorithm I the necessary storage includes \( N \) users’ bit strings with the length of \( km \), so it is \( O(Nkm) \). The prior probabilities on \( k \) dimensions is \( O(v^k) \). The conditional probabilities and posterior probabilities on \( v^k \) candidates for all bit strings is \( O(2Nv^k) \). So, the overall complexity is \( O(Nkm + 2Nv^k + v^k) = O(Nkm + 2Nv^k) \) since \( N \) is the dominant variable.
According to Theorem 2, the space overhead could be daunting when either \( N \) or \( k \) is large. This makes the performance of EM-based \( k \)-dimensional distribution estimation degrade dramatically and not applicable to high dimensional data.

### D. Lasso-based Multivariate Distribution Estimation

To improve the efficiency of the \( k \)-dimensional joint distribution estimation, we present a Lasso regression-based algorithm here. As mentioned in Section V-B1, the bit strings are the representative features of the original report. After randomized responses and flipping, a large number of samples with various levels of noise will be generated by individual users. So, one may consider that the central server receives a large number of samples from specific distribution, however, with random noise. In this sense, one may estimate the distribution from the noised sample space by taking advantage of linear regression \( \hat{\mathbf{y}} = \mathbf{M} \hat{\beta} \), where \( \mathbf{M} \) is predictor variables and \( \hat{\mathbf{y}} \) is response variable, and \( \hat{\beta} \) is the regression coefficient vector. The determinism of Bloom filter can guarantee that the features (predictor variables \( \mathbf{M} \)) re-extracted at the server side are the same as the user side. Moreover, response variable \( \hat{\mathbf{y}} \) can be estimated from the randomized bit strings according to the statistic characters of known \( f \). Therefore, the only problem is to find a good solution to the linear regression \( \hat{\mathbf{y}} = \mathbf{M} \hat{\beta} \). Obviously, \( k \)-dimensional data may incur an output domain \( \Omega_{1} \times \ldots \times \Omega_{k} \) with the size of \( |\Omega_{1}| \times \ldots \times |\Omega_{k}| \), which increases exponentially with \( k \). With fixed \( N \) entries in the dataset \( X \), the frequencies of many combination \( \omega_{1}, \omega_{2}, \ldots, \omega_{k} \in \Omega_{1} \times \ldots \times \Omega_{k} \) are rather small or even zero. So, \( \mathbf{M} \) is actually sparse and only part of the sparse but effective predictor variables need to be chosen. Otherwise, the general linear regression techniques will lead to overfitting problem. Fortunately, Lasso regression \( \| \| \) is effective to solve the sparse linear regression by choosing predictor variables.

**Algorithm 2** Lasso-based \( k \)-dimensional Joint Distribution

**Input:**
- \( C \): attribute indexes cluster i.e., \{1, 2, ..., \( k \)\},
- \( A_{j} \): \( k \)-dimensional attributes \( (1 \leq j \leq k) \),
- \( \Omega_{j} \): domain of \( A_{j} \) \( (1 \leq j \leq k) \),
- \( s_{j} \): observed Bloom filters \( (1 \leq i \leq N) \) \( (1 \leq j \leq k) \),
- \( f \): flipping probability.

**Output:**
- \( P(A_{C}) \): joint distribution of \( k \) attributes specified by \( C \).

1. for each \( j \in C \) do
2. for each \( b = 1, 2, \ldots, m_{j} \) do
3. compute \( \hat{y}_{j}[b] = \sum_{i=1}^{N} s_{j}[b] \)
4. compute \( y_{j}[b] = (\hat{y}_{j}[b] - fN/2)/(1 - f) \)
5. end for
6. set \( H_{j}(\Omega_{j}) = \{ H_{j}(\omega) \mid \forall \omega \in \Omega_{j} \} \)
7. end for
8. set \( \mathbf{y} = [y_{1}[1], \ldots, y_{1}[m_{1}], y_{2}[1], \ldots, y_{2}[m_{2}], \ldots, y_{k}[1], \ldots, y_{k}[m_{k}] \]
9. set \( \mathbf{M} = \{ H_{1}(\Omega_{1}) \times H_{2}(\Omega_{2}) \times \cdots \times H_{k}(\Omega_{k}) \} \)
10. compute \( \hat{\beta} = \text{Lasso regression}(\mathbf{M}, \mathbf{y}) \)
11. return \( P(A_{C}) = \hat{\beta}/N \)

Our Lasso-based estimation is described in Algorithm 2 and consists of the following four major steps.

1. After receiving all randomized Bloom filters from \( N \) nodes, for each bit \( b \) in each attribute \( j \), the central server counts the number of 1’s as \( \hat{y}_{j}[b] = \sum_{i=1}^{N} s_{j}[b] \).

**Example 7:** In Table [IV] each bit is counted to obtain the sum. With current 4 records, the count vector is \( (2, 0 | 1, 4, 3, 1) \).

2. The true count sum of each bit \( y_{j}[b] \) can be estimated as \( y_{j}[b] = (\hat{y}_{j}[b] - fN/2)/(1 - f) \) according to the randomized response applied to the true count. These count sums of all bits form a vector \( \mathbf{y} \) with the length of \( \sum_{j=1}^{k} m_{j} \).

**Example 8:** With the count vector \( (2, 0 | 1, 4, 3, 1) \), the true counts on each bit can be estimated as \( (2 - 0.5 \times 4/2)/(0.5) = 2, (0 - 0.5 \times 4/2)/0.5 = -2, (1 - 0.5 \times 4/2)/0.5 = 0, (4 - 0.5 \times 4/2)/0.5 = 6, \) and \( (3 - 0.5 \times 4/2)/0.5 = 4 \). Therefore, the true count vector is \( (2, -2 | 0, 6, 4, 0) \).

3. To construct the features of the overall candidate set of attribute \( \omega_{1} \ldots \omega_{k} \), the Bloom filters on each dimension \( \omega_{j} \) is re-implemented by the server with the same hash functions \( H_{j}(\cdot) \) on the user end. Suppose all distinct Bloom filters on \( \Omega_{j} \) are \( H_{j}(\omega_{j}) \mid \forall \omega_{j} \in \Omega_{j} \), where they are orthogonal with each other. The candidate set of Bloom filters is then \( \mathbf{M} = \{ H_{1}(\Omega_{1}) \times H_{2}(\Omega_{2}) \times \cdots \times H_{k}(\Omega_{k}) \} \) and the members in \( \mathbf{M} \) are still mutual orthogonal.

**Example 9:** By Cartesian product of multiple Bloom filters of different individual attributes, the Bloom filters of all candidate attribute combinations can be reconstructed. For example, the case that “a male alumni with master degree and high-middle income” can be represented by the concatenated Bloom filter \( H_{2}(\mathbf{M})H_{3}(\text{master}) = 010110 \). Similarly, all \( |\Omega_{j}| \times |\Omega_{3}| = 2 \times 3 = 6 \) candidate combinations can reconstruct their corresponding Bloom filters as \( 010101, 01110, 011100, 100101, 101110, 101100 \). Therefore, the candidate matrix \( \mathbf{M} \) can be represented as

\[
\mathbf{M} = \begin{bmatrix}
0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 & 0
\end{bmatrix}
\]

Similar demonstration is also shown in Figure 4.

4. Fit a Lasso regression model to the counter vector \( \mathbf{y} \) and the candidate matrix \( \mathbf{M} \), and then choose the non-zero coefficients as the corresponding frequencies of each candidate string. By reshaping the coefficient vector into a \( k \)-dimensional matrix by natural order and dividing with \( N \), we can get the \( k \)-dimensional joint distribution estimation \( P(A_{1}, A_{2}, \ldots, A_{k}) \). For example, in Figure 4 we fit a linear regression to \( \mathbf{y}_{12} \) and the candidate matrix \( \mathbf{M} \) to estimate the joint distribution \( P(A_{1}, A_{2}) \).

**Example 10:** Suppose \( \hat{\beta} = [\beta_{11}, \beta_{12}, \beta_{13}, \beta_{21}, \beta_{22}, \beta_{23}] \) represents the frequency of 6 combinations of \( A_{2} \) and \( A_{3} \). Then, without noises caused by random flipping, there should be the only \( \hat{\beta} \) satisfying the linear equations

\[
\hat{\beta} \cdot \mathbf{M} = \mathbf{y},
\]

However, since \( \mathbf{y} \) is an estimated vector with noises, \( \hat{\beta} \) cannot be directly solved. Therefore, linear regression
techniques can be used to capture the best \( \hat{\beta} \), which includes the frequency entries for possible combinations of \( A_2 \) and \( A_3 \). So \( \hat{\beta}/N \) is the ratio of frequencies and the estimated probability of \( P(A_2A_3) \).

Generally, the regression operation, the core of the estimation, will lose accuracy only when there are many collisions between Bloom filter strings. However, as mentioned in Section V-B1 if there is no collision in the bit strings of each single dimension, then there is no collision in conjuncted bit strings of different dimensions. In fact, the probability of collision in conjuncted bit strings will not increase with dimensions. For example, suppose the collision rate of Bloom filter in one dimension is \( p \), then the collision rate will decrease to \( p^k \) when we connect bit strings of \( k \) dimensions together. Therefore, we only need to choose proper \( m \) and \( h \) according to Equation (6) and (7) to lower the collision probability for each dimension and then we are guaranteed to have a proper estimation for multiple dimensions.

**Complexity:** Compared with Algorithm 1 our Lasso-based estimation can effectively reduce the time and space complexity.

**Theorem 4:** The time complexity of Algorithm 2 is

\[
O(v^3k + kmv^2k + Nkm). \tag{20}
\]

**Proof** Algorithm 2 involves two parts: to compute the bit counter vector, \( N \) bit strings with each length of \( km \) will be summed up and this operation at most incurs the complexity of \( O(Nkm) \); and Lasso regression with \( v^k \) candidates (total domain size) and \( km \) samples (the length of the bit counter vector is \( km \)) has the complexity of \( O((v^k)^3 + (v^k)^2(km)) \).

Based on the general assumption that \( N \) dominates Equation (20), then we can see the complexity in Equation (20) is much less than Equation (16) in Theorem 2.

**Theorem 5:** The space complexity of Algorithm 2 is

\[
O(Nkm + kmv^k). \tag{21}
\]

**Proof** In Algorithm 2, the storage overhead consists of three parts: users’ bit strings \( O(Nkm) \), a count vector with size \( O(km) \), and the candidate bit matrix \( M \) with size \( O(kmv^k) \). Therefore, the overall space complexity of our proposed Lasso based estimation algorithm is \( O(Nkm + km + k^2v^k) = O(Nkm + v^kkm) \), which is also smaller than Equation (17) as \( N \) is dominant.

The empirical results are shown in Section VII. The efficiency comes from the fact that the \( N \) bit strings of length \( m \) will be scanned to count sum only once and then one-time Lasso regression is fitted to estimate the distribution. In addition, Lasso regression could extract the important (i.e., frequent) features with high probability, which fits well with the sparsity of high-dimensional data.

1) Hybrid Algorithm: Recall that, with sufficient samples, EM-based estimation could have good convergence but also high complexity. Instead, Lasso-based estimation can be very efficient with some estimation deviation compared with EM-based algorithm. The high complexity of EM algorithm stems from two parts: Firstly, it iteratively scans user’s reports and builds a prior likely distribution table, which has the size of \( N \cdot \prod_j |\Omega_j| \). And for each record of table, the computation has to compare \( \sum m_j \) bits. However, when the dimension is high, the combination of \( \Omega_j \) will be very sparse and has lots of zero items. Secondly, Without prior knowledge, the initial value of the random assignment (i.e., uniform distribution) will lead to too many iterations for final convergence to occur.

To achieve a balance between the EM-based estimation and Lasso-based estimation, we also propose a hybrid algorithm Lasso+EM in Algorithm 3 that first eliminates the redundant candidates and estimates the initial value with Lasso based algorithm 2 and then refines the convergence using EM-based algorithm 1. The hybrid algorithm has two advantages:

1) The sparse candidates will be selected out by the Lasso based estimation algorithm, as shown in Steps 1, 2, 7, 8 of Algorithm 5. So the EM algorithm can just compute the conditional probability on these sparse candidates instead of all candidates, which can greatly reduce both time and space complexity.

2) Lasso-based algorithm can give a good initial estimation of the joint distribution. Compared with using initial values with random assignments, using the initial value estimated with the Lasso-based algorithm can further boost the convergence of the EM algorithm, which is sensitive to the initial value especially when the candidate space is sparse.

**Theorem 6:** The time complexity of Algorithm 3 is

\[
O((v^3k + kmv^2k + Nkm) + (t(v')^2 + Nkm(v'))), \tag{22}
\]

where \( v' \) is the average size of sparse items in \( \Omega_1 \times \cdots \times \Omega_k \), and \( v < v' \).

**Proof** See Theorem 2 and Theorem 4 the only difference is that after the Lasso based estimation, only sparse items in \( \Omega_1 \times \cdots \times \Omega_k \) are selected.

**Theorem 7:** The space complexity of Algorithm 3 is

\[
O(Nkm + v^km + 2Nv'). \tag{23}
\]

**Proof** See Theorem 3 and Theorem 5.

**Algorithm 3 Lasso+EM k-dimensional Joint Distribution (Lasso+EM_JD)**

Input: \( A_j \): \( k \)-dimensional attributes \( (1 \leq j \leq k) \), \( \Omega_j \): domain of \( A_j \) \( (1 \leq j \leq k) \), \( \hat{s}_{ij} \): observed Bloom filters \( (1 \leq i \leq N) \), \( 1 \leq j \leq k \), \( f_j \): flipping probability.

Output: \( P(A_1A_2\ldots A_k) \): \( k \)-dimensional joint distribution.

1: compute \( P_0(\omega_1\omega_2\ldots\omega_k) = \text{Lasso}_\text{JD}(A_j, \Omega_j, \{\hat{s}_{ij}\}_{i=1}^N, f_j) \)
2: set \( C' = \{x| x \in C; P_0(x) = 0 \} \)
3: for each \( i = 1, \ldots, N \) do
4: for each \( j = 1, \ldots, k \) do
5: compute \( P(\hat{s}_{ij}|\omega_j) = \prod_{b=1}^{m_j}(\hat{s}_{ij}^{b}[1-(1-f_j)^{1-\hat{s}_{ij}^{b}}]) \)
6: end for
7: if \( \omega_1\omega_2\ldots\omega_k \in C' \) then
8: \( P(\hat{s}_{1j}\hat{s}_{2j}\ldots\hat{s}_{kj}|\omega_1\omega_2\ldots\omega_k) = 0 \)
9: else
10: compute \( P(\hat{s}_{1j}\hat{s}_{2j}\ldots\hat{s}_{kj}|\omega_1\omega_2\ldots\omega_k) = \prod_{j=1}^{k} P(\hat{s}_{ij}|\omega_j) \)
11: end if
12: end for
13: initialize \( t = 0 \)/ *number of iterations*/
14: repeat
15: \( \ldots \)
16: \( t \) (similar to Algorithm 1)/ *
17: \( \ldots \)
18: until \( P_0(\omega_1\omega_2\ldots\omega_k) \) converges.
19: return \( P(A_1A_2\ldots A_k) = P_0(\omega_1\omega_2\ldots\omega_k) \)
E. Dimension Reduction with Local Privacy

1) Dimension Reduction via 2-dimensional Joint Distribution Estimation: The key to reducing dimensionality in high-dimensional dataset is to find the compact clusters, within which all attributes are tightly correlated to or dependent on each other. Inspired by [7], [46] but without extra privacy budget on dimension reduction, our dimension reduction based locally once-for-all privacy-preserved data records consists of the following three steps:

Algorithm 4: Dimension reduction with local privacy

Input: 
- \( A_j \): \( k \)-dimensional attributes \((1 \leq j \leq k)\),
- \( \Omega_j \): domain of \( A_j \) \((1 \leq j \leq k)\),
- \( s^i_j \): observed Bloom filters \((1 \leq i \leq N) (1 \leq j \leq k)\),
- \( f \): flipping probability,
- \( \phi \): dependency degree

Output: 
- \( C_1, C_2, ..., C_l \): attribute indexes clusters

1. initialize \( G_{d \times d} = 0 \).
2. for each \( j = 1, 2, \ldots, d \) do
3. estimate \( P(A_j) \) by Lasso based Algorithm 3
4. end for
5. for each attribute \( m = 1, 2, \ldots, d \) do
6. for each attribute \( n = m + 1, m + 2, \ldots, d \) do
7. estimate \( P(A_m, A_n) \) by Lasso based Algorithm 3
8. compute \( I_{m,n} = \sum_{i \in \Omega_m} \sum_{j \in \Omega_n} p_{ij} \ln \frac{p_{ij}}{p_i \cdot p_j} \)
9. compute \( \tau_{m,n} = \min(|\Omega_m| - 1, |\Omega_n| - 1) \cdot \varphi^2 / 2 \)
10. if \( I(m, n) \geq \tau_{m,n} \), then
11. set \( G_{m,n} = G_{n,m} = 1 \), \( G \in G_{d \times d} \)
12. end if
13. end for
14. end for
15. build dependency graph with \( G_{d \times d} \)
16. triangulate the dependency graph into a junction tree
17. split the junction tree into several cliques \( C_1, C_2, ..., C_l \) with elimination algorithm.
18. return \( C = \{C_1, C_2, ..., C_l\} \)

1) Pairwise Correlation Computation. We use mutual information to measure pairwise correlations between attributes. The mutual information is calculated as

\[
I_{m,n} = \sum_{i \in \Omega_m} \sum_{j \in \Omega_n} p_{ij} \ln \frac{p_{ij}}{p_i \cdot p_j}
\]  

(24)

where, \( \Omega_m \) and \( \Omega_n \) are the domains of attributes \( A_m \) and \( A_n \), respectively, \( p_{ij} \) represent the probability that \( A_m \) is the \( i \)th value in \( \Omega_m \) and the probability that \( A_n \) is the \( j \)th value in \( \Omega_n \), respectively. Then, \( p_{ij} \) is their joint probability. Particularly, both \( p_i \) and \( p_j \) can be learned from the direct RAPPOR scheme with Lasso regression [14]. Their joint distribution \( p_{ij} \) then can be efficiently obtained with our proposed multi-dimensional marginal estimation algorithm in Section V-D.

Example 11: A 4 \times 4 correlation matrix \( I \) can be built for the example dataset of Table III to record the mutual information measure.

\[
I = \begin{bmatrix}
1.00 & 0.05 & 0.03 & 0.16 \\
0.05 & 1.00 & 0.02 & 0.04 \\
0.03 & 0.02 & 1.00 & 0.15 \\
0.16 & 0.04 & 0.15 & 1.00
\end{bmatrix}
\]  

(25)

where \( I_{m,n} \) is the mutual information between \( A_m \) and \( A_n \), e.g., \( I_{2,3} = 0.02 \) means the mutual information between \( A_2 \) and \( A_3 \) is 0.02. It should be noted that the correlations need to be learnt between all attributes pairs in heterogeneous multi-attribute data. That is to say the basic complexity is \( O(d^2) \), where \( d \) is the number. And in each learning process, the complexity is decided by the distribution estimation algorithm. So, the overall complexity is quite
The core of the dimension reduction process is the

2) **Dependency Graph Construction.** Based on mutual information, the dependency graph between attributes can be constructed as follows. First, an adjacent matrix \( G_{d \times d} \) is initialized with all 0. Then, all the attribute pairs \((A_m, A_n)\) are chosen to compare their mutual information with an threshold \( \tau_{m,n} \), which is defined as

\[
\tau_{m,n} = \min(|\Omega_m| - 1, |\Omega_n| - 1) \times \phi^2/2
\]

and \( \phi (0 \leq \phi \leq 1) \) is a flexible parameter determining the desired correlation level. \( G_{m,n} \) and \( G_{n,m} \) are both set to be 1 if and only if \( I_{m,n} > \tau_{m,n} \).

Example 12: By comparing the correlation matrix \( I \) with the dependency threshold \( \tau_{m,n} \), a dependency graph represented by the adjacent matrix \( G \) can be built.

\[
G_{4 \times 4} =
\begin{bmatrix}
1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 \\
1 & 0 & 0 & 1
\end{bmatrix}
\]  

3) **Compact Clusters Building.** By triangulation, the dependency graph \( G_{d \times d} \) can be transformed to a junction tree, in which each node represents an attribute \( A_j \). Then, based on the junction tree algorithm, several clusters \( C_1, C_2, \ldots, C_l \) can be obtained as the compact clusters of attributes, in which attributes are mutually correlated. Hence, the whole attributes set can be divided into several compact attribute clusters and the number of dimensions can be effectively reduced.

Example 13: By triangulation, the dependency graph can be transformed to a junction tree, in which nodes are split into different clusters. Figure 5 demonstrates an example of the junction tree built from the dependency graph. The attribute set \{A_1, A_2, A_3, A_4, A_5, A_6\} is split into 4 clusters \( A_1A_2A_3, A_2A_4A_5, A_2A_4A_5, \) and \( A_6 \), where \( A_2 \) and \( A_2A_5 \) is the separators and clusters \( A_1A_2, A_2A_3A_5, A_2A_4A_5, \) and \( A_6 \) are also called cliques.

**Complexity:**

Theorem 8: The time complexity of Algorithm[4] is

\[ O(d^2(v^6 + 2mv^4 + 2Nm + tN(v')^2 + 2Nm(v'))). \]  

**Proof** The core of the dimension reduction process is the \( d \) times of 2-dimensional joint distribution estimation. The complexity of each 2-dimensional joint distribution estimation can be derived from Equation (22) when adopting the hybrid algorithm (Algorithm[3]). The complexity of building junction tree on \( d \times d \) dependency graph is negligible when compared with the joint distribution estimation.

Theorem 9: The space complexity of Algorithm[4] is

\[ O(2Nm + 2v^2m + 2Nv'). \]  

**Proof** When we compute the mutual correlations between any pairs, a 2-dimensional joint distribution estimation algorithm will be triggered with the space complexity of \( O(2Nm + 2m2v^2 + 2Nv') \), since \( k = 2 \) is substituted into Equation (23). This maximum complexity dominates Algorithm[4]. The space complexity of building junction tree on \( d \times d \) dependency graph is negligible when compared with the joint distribution estimation.

2) **Entropy based Pruning Scheme:** In existing work[22],[42] on homogeneous data, the correlations can be simply captured by distance metrics. However, in our work, mutual information is used to measure general correlations since heterogeneous attributes (a.k.a., attributes with different domains) are also considered.

As shown in Equation (24), to calculate the mutual information of variables \( X \) and \( Y \), the joint probability on the joint combination is inevitable, thus making the pairwise computation of dependency necessary. Although mutual information is already simple than Kendall rank coefficients in the similar work[25], here, we still propose a pruning-based heuristic to boost this pairwise correlation learning process.

Intuitively, there are different situations in Algorithm[4] 1. When \( \phi = 0 \) or \( \phi = 1 \), all attributes will be considered mutually correlated or independent. Thus, there is no need to compute pairwise correlation. 2. With the increase of \( \phi \) (0 < \( \phi < 1 \)), less dependencies will be included in the adjacent matrix \( G_{d \times d} \) of dependency graph, which will become sparser. This also means that we may selectively neglect some pairs. Inspired by the relationship between mutual information and information entropy[3], we first heuristically filter out some portion of attributes \( A_x \) with least relative information entropy \( RH(A_x) = H(A_x)/|\Omega_x| \), and then verify the mutual information among the remaining attributes, thus reducing the pairwise computations.

Furthermore, the adjacent matrix \( G_{d \times d} \) of dependency graph varies in different datasets. For example, the adjacent matrix \( G_{d \times d} \) is rarely sparse in binary datasets but very sparse in non-binary datasets. Based on this observation, we can further simplify the calculation by finding the independency in binary datasets or finding the dependency in non-binary datasets. For example, we first set all entries of \( G_{d \times d} \) for a binary datasets as 1’s and start from the attributes with least relative information entropy \( RH(A_x) = H(A_x)/|\Omega_x| \) to find the uncorrelated attributes. While for non-binary datasets, we first set \( G_{d \times d} \) as 0’s and then start from the attributes with largest average entropy to find the correlated attributes.

The relationship between mutual information and information entropy can be represented as \( I(X;Y) = H(X) + H(Y) - H(X,Y) \), where \( H(X) \) and \( H(X,Y) \) denote the information entropy of variable \( X \) and their joint entropy of \( X \) and \( Y \), respectively.
Algorithm 5: Entropy based Pruning Scheme

Input: \( A_j \): \( k \)-dimensional attributes \( 1 \leq j \leq k \),
\( \Omega_j \): domain of \( A_j \) \( 1 \leq j \leq k \),
\( s_i^j \): observed Bloom filters \( 1 \leq i \leq N \) \( 1 \leq j \leq k \),
\( f \): flipping probability,
\( \phi \): dependency degree

Output: \( G_{d \times d} \): adjacent matrix \( G_{d \times d} \) of dependency graph of attributes

1: initialize \( G_{d \times d} = 0 \)
2: for each \( j = 1, 2, \ldots, k \) do
3: compute \( P(A_j) = JD(A_j, \Omega_j, \{s_i^j\}_{i=1}^N) \)
4: compute \( RH(A_j) = -\frac{1}{\sum_{p \in P(A_j)} p \log p} \)
5: end for
6: sort \( \text{list}_A = \{A_1, A_2, \ldots, A_k\} \) according to entropy \( H(A_j) \)
7: pick up the previous \( \lfloor \text{length}(\text{list}_A) \ast (1 - \phi) \rfloor \) items from \( \text{list}_A \) as a new list \( \text{list}'_A \)
8: compute pairwise mutual information among \( \text{list}'_A \) and set dependency graph \( G_{d \times d} \), as in Algorithm 4
9: return \( G_{d \times d} \)

Algorithm 6: New Dataset Synthesizing

Input: \( C \): a collection of attribute index clusters \( C_1, \ldots, C_l \),
\( A_j \): \( k \)-dimensional attributes \( 1 \leq j \leq k \),
\( \Omega_j \): domain of \( A_j \) \( 1 \leq j \leq k \),
\( s_i^j \): observed Bloom filters \( 1 \leq i \leq N \) \( 1 \leq j \leq k \),
\( f \): flipping probability,

Output: \( X \): Synthetic Dataset of \( X \)

1: initialize \( R = \emptyset \)
2: repeat
3: randomly choose an attribute index cluster \( C \in C \)
4: estimate joint distribution \( P(A_C) \) by JD
5: sample \( X_C \) according to \( P(A_C) \)
6: \( C = C - C' \), \( R = R \cup C' \), \( D = \{D \in C | D \cap R \neq \emptyset \} \)
7: for each \( D \in D \) do
8: estimate joint distribution \( P(A_D) \) by JD
9: obtain conditional distribution \( P(A_{D-R} | A_{D-R}) \) from \( P(A_{D}) \)
10: sample \( X_{D-R} \) according to \( P(A_{D-R} | A_{D-R}) \) and \( X_{D-R} \)
11: \( C = C - D \), \( R = R \cup D \), \( D = \{D \in C | D \cap R \neq \emptyset \} \)
12: end for
13: until \( C = \emptyset \)
14: return \( X \)

F. Synthesizing New Dataset

For brevity, we first define \( A_C = \{A_j | j \in C \} \) and \( \hat{X}_C = \{x_j | j \in C \} \). Then the process of synthesizing the new dataset via sampling is shown in the following Algorithm 5.

Theorem 10: The time complexity of Algorithm 6 is
\[ O\left(l(v^{3k} + kmv^{2k} + Nkm + tN(v')^2 + Nkm(v'))\right), \]
where \( l \) is the number of clusters after dimension reduction and \( k \) here refers to average number of dimensions in these clusters.
Proof
The core of the dataset synthesizing is actually multiple \( l \)-dimensional joint distribution estimation. ■

Theorem 11: The space complexity of Algorithm 6 is
\[ O(Nkm + v^k km + 2Nv' + Nd). \]
Proof
Every time, a \( k \)-dimensional joint distribution estimation algorithm (with space complexity of \( O(Nkm + v^k km + 2Nv') \)) is processed to draw a new dataset. A new dataset with the size \( O(Nd) \) is maintained while synthesizing. ■

VI. Evaluation

In this section, we conducted extensive experiments on real datasets to demonstrate the efficiency of our algorithms in terms of computation time and accuracy.

We used three real-world datasets: Retail [1], Adult [5], and TPC-E [2]. Retail is part of a retail market basket dataset. Each record contains distinct items purchased in a shopping visit. Adult is extracted from the 1994 US Census. This dataset contains personal information, such as gender, salary, and education level. TPC-E contains trade records of “Trade type”, “Security”, “Security status” tables in the TPC-E benchmark. It should be noted that some continuous domain were binned in the pre-process for simplicity.

| Datasets   | Type  | #. Records (N) | #. Attributes (d) | Domain Size |
|------------|-------|----------------|-------------------|-------------|
| Retail     | Binary| 27,522         | 16                | 2^{16}      |
| Adult      | Integer| 45,222        | 15                | 2^{16}      |
| TPC-E      | Mixed | 40,000         | 24                | 2^{17}      |

All the experiments were run on a machine with Intel Core i5-5200U CPU 2.20GHz and 8GB RAM, using Windows 7. We simulated the crowdsourced environment as follows. First, users read each data record individually and locally transform it into privacy-preserving bit strings. Then, the crowdsourced bit strings are gathered by the central server for synthesizing and publishing the high-dimensional dataset.

LoPub can be realized by combining distribution estimations and data synthesizing techniques. Thus, we implemented different LoPub realizations using Python 2.7 with the following three strategies.

1) **EM-JD**, the generalized EM-based multivariate joint distribution estimation algorithm.
2) **Lasso-JD**, our proposed Lasso-based multivariate joint distribution estimation algorithm.
3) **Lasso+EM-JD**, our proposed hybrid estimation algorithm that uses the Lasso-JD to filter out some candidates to reduce the complexity and replace the initial value to boost the convergence of EM-JD.

It is worth mentioning that we compared only the above algorithms since our algorithm adopts a novel local privacy
The efficiency is measured by computation time, and the Multivariate Distribution Estimation is large. This is because the computation time includes CPU time and IO cost. Each set of experiments is run 100 times, and the average running time is reported. To measure accuracy, we used the distance metrics AVD (average variant distance) on the three datasets, as suggested in \[7\], to quantify the closeness between the estimated joint distribution \(P(\omega)\) and the origin joint distribution \(Q(\omega)\). The AVD error is defined as

\[
Dist_{AVD}(P, Q) = \frac{1}{2} \sum_{\omega \in \Omega} |P(\omega) - Q(\omega)|.
\] (32)

The default parameters are described as follows. In the binary dataset Retail, the maximum number of bits and the number of hash functions used in the bloom filter are \(m = 32\) and \(h = 4\), respectively. In the non-binary datasets Adult and TPC-E, the maximum number of bits and the number of hash functions used in bloom filter are \(m = 128\) and \(h = 4\), respectively. The convergence gap is set as 0.001 for fast convergence.

### A. Multivariate Distribution Estimation

Here, we show the performance of our proposed distribution estimations in terms of both efficiency and effectiveness. The efficiency is measured by computation time, and the effectiveness is measured by estimation accuracy.

1) **Computation Time**: We first evaluate the computation time of EMJD, LassoJD, and Lasso+EMJD for the \(k\)-dimensional joint distribution estimation on three real datasets.

Figures 9 and 10 compare the computation time on the binary dataset Retail with both \(k = 3\) and \(k = 5\). It can be noticed that, for each dimension \(k\), LassoJD is consistently much faster than EMJD and Lasso+EMJD, especially when \(k\) is large. This is because EMJD has to repeatedly scan each user’s bit string. Particularly, the time consumption of EMJD increases with \(f\) because there will be more iterations for the fixed convergence gap. In contrast, LassoJD uses the regression to estimate the joint distribution more efficiently.

Furthermore, the complexity of Lasso+EMJD is much less than EMJD as the initial estimation of LassoJD can greatly reduce the candidate attribute space and the number of iterations needed. When \(k\) is growing, the computation time of LassoJD increases slowly, unlike EMJD that has a dramatic increase. This is because the time complexity of LassoJD is mainly subject to the number of users.

Figures 9, 10, 11, and 12 depict the computation time on non-binary datasets (Adult and TPC-E) when \(k = 2\) and \(k = 3\). As we can see, EMJD runs with acceptable complexity on low dimension \(k = 2\). When \(k = 3\), the time complexity of EMJD increases sharply by several times. When \(k\) further increases, it does not return any result within an unacceptable time during our experiment. However, LassoJD takes less than a few seconds. This discrepancy is consistent with our complexity analysis, where we envision that the exponential growth of the candidate set will have a significant impact on EMJD. So, with the initial estimation of LassoJD, the combined estimation Lasso+EMJD can run relatively faster than EMJD with limited candidate set. The computation time of EMJD and LassoJD on TPC-E dataset with different \(k = 2\) and \(k = 3\) exhibits a similar tendency, as shown in Figures 11 and 12. We omitted the detailed report here due to the space constraint. It should be noted that the general time complexity on TPC-E is larger than Adult since the average candidate domain of TPC-E is larger.

2) **Accuracy**: Next, we compare the estimation accuracy of EMJD, LassoJD, and Lasso+EMJD on real datasets.

Figures 13 and 14 report the AVD error of EMJD, LassoJD, and Lasso+EMJD on binary dataset Retail with different dimensions \(k = 3\) and \(k = 5\). The AVD error of EMJD is very small when \(f\) is small, but when \(f\) grows, it will sharply increase to as high as 0.28. In contrast, LassoJD retains the error around 0.1 even when \(f = 0.9\). However, in practice, when \(f\) is small, i.e., \(f = 0.5\), the differential privacy an individual can achieve is \(\epsilon = 8.79\) for each dimension, which is insufficient in general. So, when \(f\) is large, the AVD error of LassoJD is comparable to or even better than that of EMJD. This is because Lasso regression is insensitive to \(f\) when estimating the coefficients from the aggregated bit sum vectors. Nonetheless, EMJD is sensitive to \(f\) and prone to some local optimal value because it scans each record of bit strings. In comparison, Lasso+EMJD achieves a better tradeoff between LassoJD and EMJD. For example, it has less AVD error than LassoJD when \(f\) is small and outperforms EMJD when \(f\) is large. We can also
see that, the AVD error of all estimation algorithms increases with $k$, since the average frequency on $k$-dimensional combined attributes is $N/u^k$ and its statistical significance decreases with $k$ exponentially.

Figures 15, 16, 17 and 18 also compare the AVD error of $\text{EM} + \text{JD}$, $\text{Lasso} + \text{JD}$, and $\text{Lasso} + \text{EM} + \text{JD}$ on the non-binary datasets Adult and TPC-E with $k = 2$ and $k = 3$. As can be seen, when $k = 2$, the AVD error of $\text{Lasso} + \text{JD}$ does not change with $f$ as the aggregated bit sum vector is insensitive to small $f$. While $\text{EM} + \text{JD}$ increases with $f$ gradually due to the scan of each individual bit string. Similar to the conclusion in the binary dataset, when $f$ is large, the trend of $\text{Lasso} + \text{JD}$ is very close to $\text{EM} + \text{JD}$. Besides, $\text{Lasso} + \text{EM} + \text{JD}$ shows very similar performance to $\text{EM} + \text{JD}$ and incurs relatively small bias. Therefore, $\text{Lasso} + \text{EM} + \text{JD}$ achieves a good balance between utility and efficiency as it runs much faster than the baseline $\text{EM} + \text{JD}$. In addition, when $k$ increases ($k = 3$), the estimation error increases as well. However, $\text{Lasso} + \text{EM} + \text{JD}$ can further balance between $\text{Lasso} + \text{JD}$ and $\text{EM} + \text{JD}$ because the candidate set is much more sparse when $k$ is larger and $\text{Lasso} + \text{EM} + \text{JD}$ can effectively reduce the redundant of candidate set and iterations. Similar conclusion can be made from the dataset TPC-E. Nonetheless, because of larger candidate domain, the AVD error on TPC-E is generally larger than that on Adult.

B. Correlation Identification

In this section, we present correlations between the multiple attributes that we can learn from locally privacy-preserved user data. Particularly, we evaluated loss ratio of dependency relationship of attributes in three datasets. The parameters used in the simulation are set as follows. The dependency threshold is generally larger than that among attributes.

1) Accuracy: Figures 19, 20 and 21 show both the ratio of correct identification (accuracy), added (false positive) and lost (true negative) correlated pairs after estimation, respectively. From these figures, we can see all these estimation algorithms can have a relatively accurate identification among the attributes, especially $\text{EM} + \text{JD}$ and $\text{Lasso} + \text{EM} + \text{JD}$ algorithms. Nevertheless, generally, the accurate rate decreases with $f$ (i.e., privacy level). In Figure 19 the general accuracy identified rate is about 85% when the privacy is small ($f$ is less than 0.9). While in Figures 20 and 21 the accuracy rate is as high as 95% because the dependency threshold is relatively loose as 0.4. High accurate identification guarantees the basic correlations among attributes.

However, the incorrect identification is considered sepa-
TABLE VII: Dependency Loss Ratio and Complexity Reduction Ratio (Adult)

| ϕ   | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 |
|-----|-----|-----|-----|-----|-----|
| #. Dep (Pruning) | 88  | 38  | 22  | 12  | 6   |
| #. Dep         | 102 | 42  | 24  | 14  | 8   |
| Loss Ratio     | 0.137  | 0.095  | 0.083  | 0.143  | 0.250  |
| #. Pairs (Pruning) | 91  | 66  | 55  | 36  | 28  |
| #. Pairs       | 105 | 105 | 105 | 105 | 105 |
| Reduction Ratio | 0.133  | 0.371  | 0.476  | 0.657  | 0.733  |

TABLE VIII: Dependency Loss Ratio and Complexity Reduction Ratio (TPC-E)

| ϕ   | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 |
|-----|-----|-----|-----|-----|-----|
| #. Dep (Pruning) | 44  | 16  | 16  | 8   | 8   |
| #. Dep         | 46  | 24  | 20  | 10  | 10  |
| Loss Ratio     | 0.043  | 0.333  | 0.200  | 0.200  | 0.200  |
| #. Pairs (Pruning) | 231 | 171 | 130 | 66  | 45  |
| #. Pairs       | 276 | 276 | 276 | 276 | 276 |
| Reduction Ratio | 0.103  | 0.380  | 0.507  | 0.761  | 0.837  |

rately with false positive rate and true negative, which reflect the efficiency and effectiveness of dimension reduction. Since false positive identification just adds the correlated rules that were not exists, this kind of misidentification only incurs no errors but redundant correlations and extra distribution learning. Instead, true negative identification implies the loss of some correlations among attributes, thus causing information loss in our dimension reduction. For false positive identification, we can see that EM_JD algorithm and Lasso+EM_JD are less than Lasso. That is because Lasso estimation will choose the sparse probabilities and the mutual information estimated is generally high due to the concentrated probability distribution. Especially in non-binary datasets Adult and TPC-E, the sparsity is much higher, so the estimated probability distribution is more concentrated and the false positive identification rate is high.

The true negative identification in both Adult and TPC-E is small because the true correlations are not very high itself because all attributes have a large domain. Instead, the true correlations in Retail are high and almost any two attributes are dependent. Therefore, the true negative identification is comparatively higher.

2) Effectiveness of Pruning Scheme: We also validated the pruning scheme proposed in Section V.C with simulations on the three datasets. We first defined the dependency loss ratio as the ratio between the dependency loss after pruning with the original number of dependencies in the adjacent matrix $G_{d \times d}$ of dependency graph. The complexity reduction ratio is defined as the ratio of reduced pairwise comparisons.

Tables VII, VIII, and IX illustrate the effectiveness of our proposed heuristic pruning scheme. Particularly, as shown in Tables VII and VIII, with the increase of $\phi$, which shows

TABLE IX: Dependency Loss Ratio and Complexity Reduction Ratio (Retail)

| ϕ   | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 |
|-----|-----|-----|-----|-----|-----|
| #. Dep (Pruning) | 256 | 256 | 256 | 256 | 256 |
| #. Dep         | 240 | 240 | 238 | 220 | 200 |
| Loss Ratio     | $-0.007$  | $-0.007$  | $-0.076$  | $-0.136$  | $-0.220$  |
| #. Pairs (Pruning) | 91  | 91  | 78  | 66  | 55  |
| #. Pairs       | 120 | 120 | 120 | 120 | 120 |
| Reduction Ratio | 0.242  | 0.242  | 0.350  | 0.450  | 0.512  |

the strength of correlations, the number of original dependencies in dataset Adult decreases dramatically. Also, the dependencies after the heuristic pruning decrease accordingly and their number is quite close to the original. However, when $\phi$ increases, the number of pairwise comparison becomes less compared to the full pairwise comparison. So, it shows that the heuristic pruning scheme can effectively reduce the complexity with fairly small sacrifice of dependency accuracy. Similar conclusion can be found in Table VIII on non-binary dataset TPC-E. On the binary dataset Retail, due to the prior knowledge that binary datasets normally have strong mutual dependency, we changed the pruning scheme a little. Particularly, we assume all the attributes are dependent with each other and our pruning scheme aims at finding the non-dependency from that attributes $A_j$ with less entropy $H(A_j)$. According to Table IX, the number of dependencies after pruning decreases slowly and the minus symbol in the dependency loss ratio means that there is no loss of dependencies but there are redundant dependencies that should not exist in original datasets. It should be noted that redundant dependencies cover all the original dependencies. Therefore, the redundancy will not cause the degrade of data utility since more correlations are kept. However, the efficiency of dimension reduction, which should cut off as many unnecessary correlations as possible, is hindered. So, according to Table IX we can also say that the heuristic pruning scheme can achieve up to 50% complexity reduction without loss of dependencies.

C. SVM and Random Forest Classifications

To show the overall performance of LoPub, we evaluated both the SVM and random forest classification error rate in the new datasets synthesized by different versions of LoPub. We first sampled from the three original datasets Retail, Adult, and TPC-E to get both the training sets and test sets. Then, we generated the privacy-preserving synthetic datasets from the training data. Next, we trained three different SVM classifiers and three random forest classifiers on the synthetic datasets. Lastly, we evaluated the classification rate on the original sampled test sets. Particularly, the average random forest classification rate is computed on all the original attributes and the average SVM classification rate is computed on all the original binary-state attributes in each dataset, for example, all attributes in binary dataset Retail, the 10th (gender) and 15th (marital) attribute in Adult, and the 2nd, 10th, 23rd, and 24th attribute in TPC-E. For comparison, we also trained the corresponding SVM and random forest classifiers on each sampled training set and measured their classification rate each time.

Figures 22, 23, and 24 show the average accurate SVM classification rate on three datasets Retail, Adult, and TPC-E. In all figures, the average SVM classification rate decreases with $f$, which reflects the privacy level. Generally, when $f$ is small $f < 0.9$, the classification rate drops slowly. Nevertheless, when $f = 0.9$, there will be a large gap. This is because the differential privacy level changes as shown in Equation 8. For SVM, the classification rate is relatively close to the that of non-privacy case. This is because SVM classification only considers binary-state attributes and the distribution estimation on binary-state attributes can be more
accurate than non-binary attributes, which have sparser distribution. In all figures, we can see that Lasso based estimation has generally smaller classification rate because its biased estimation. EM-based estimation generally outperforms others but still showed performance degradation when \( f \) is large, while Lasso+EM+JD could find a better balance between alternative methods.

However, in Figures 25, 26, and 27 due to the high sparsity in the distribution of non-binary attributes, the joint distribution estimation on non-binary attributes may be biased and that is why the random forest classification on our synthetic datasets is not as good as SVM classification. Nonetheless, the synthetic data still keeps sufficient information of original crowdsourced datasets. For example, the worst random forest classification rate in the three datasets is 67\%, 42\%, and 26\%, which are much larger than the average random guess rate of 50\%, 15\%, and 13\%, respectively. In detail, EM-based estimation worked relatively well to generate the synthetic datasets and Lasso estimation caused larger bias in the random forest classification. However, with the initial estimation of Lasso estimation, Lasso+EM+JD works also well and degrades slowly with \( f \).

For reference, the overall computational time for synthesizing new datasets are also presented in Figures 28, 29, and 30. Despite the worst utility, Lasso-based algorithm is the most efficient solution, which achieves approximately three orders of magnitudes faster than the EM-based method. As mentioned before, that is because it can estimate the joint distribution regardless of the number of bit strings. With the initial estimation of Lasso+JD, the EM+JD can then be effectively simplified from two aspects: the sparse candidates can be limited and the initial value is well set. Instead, the baseline EM+JD not only needs to build prior probability distribution for all candidates but also begins the convergence with a randomness value.

VIII. CONCLUSION

In this paper, we propose a novel solution, LoPub, to achieve the high-dimensional data release with local privacy in crowdsourced systems. Specifically, LoPub learns from the distributed data records to build the correlations and joint distribution of attributes, synthesizing an approximate dataset for privacy protection. To realise the effective multi-variate distribution estimation, we proposed EM-based and Lasso-based joint distribution estimation algorithms. The experiment results on the real datasets show that LoPub is an efficient and effective mechanism to release a high-dimensional dataset while providing sufficient local privacy guarantee for crowdsourced users.

REFERENCES

[1] Frequent itemset mining dataset. [http://fimi.ua.ac.be/data/]
[2] Trans. processing performance council. [http://www.tpc.org/]
[3] G. Acu, C. Castelluccia, and R. Chen. Differentially private histogram publishing through lossy compression. In Proc. of IEEE ICDM, pages 1–10, 2012.
[4] M. Akgn, A. O. Bayrak, B. Ozer, and M. a. Sa?tro?la. Privacy preserving processing of genomic data: A survey. Journal of Biomedical Informatics, 56:103–111, 2015.
[5] K. Bucu and M. Lichman. Uci machine learning repository. [https://archive.ics.uci.edu/ml/datasets.html/]
[6] R. Chen, H. Li, A. K. Qin, S. P. Kasiviswanathan, and H. Jin. Private spatial data aggregation in the local setting. In Proc. IEEE ICDE, pages 289–300, 2016.
[7] R. Chen, Q. Xiao, Y. Zhang, and J. Xu. Differentially private high-dimensional data publication via sampling-based inference. In Proc. of ACM KDD, pages 129–138, 2015.
[8] W. Day and N. Li. Differentially private publishing of high-dimensional data using sensitivity control. In Proc. of the ASIACCS, pages 451–462. ACM, 2015.
[9] J. C. Duchi, M. I. Jordan, and M. J. Wainwright. Local privacy and statistical minimax rates. In Proc. of IEEE FOCS, pages 429–438, 2013.
[10] C. Dwork. Differential privacy. In Proc. of ICALP, pages 1–12, 2006.
[11] C. Dwork. Differential privacy: A survey of results. In Proc. Springer TAMP, pages 1–19, 2008.
[12] C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. Proc. of TCC, pages 265–284, 2006.
[13] F. Eigner, A. Kate, M. Maftei, F. Pampaloni, and I. Pryvalov. Differentially private data aggregation with optimal utility. In Proceedings of the 30th Annual Computer Security Applications Conference, pages 316–325. ACM, 2014.
[14] U. Erlingsson, V. Pihur, and A. Korolova. Rappor: Randomized aggregatable privacy-preserving ordinal response. In Proc. of ACM CCS, 2014.
[15] L. Fan and L. Xiong. An adaptive approach to real-time aggregate monitoring with differential privacy. IEEE Trans. Knowl. Data Eng., 26(9):2094 – 2106, 2014.
[16] F. Fanti, V. Pihur, and U. Erlingsson. Building a rappor with the unknown: Privacy-preserving learning of associations and data dictionaries. Proceedings on Privacy Enhancing Technologies, 2016(3):41–61, 2016.
[17] M. M. Groat, B. Edwards, J. Horey, W. He, and S. Forrest. Enhancing privacy in participatory sensing applications with multidimensional data. In Proc. of IEEE PerCom, pages 144–152. IEEE, 2012.
[18] N. Holohan, D. J. Leith, and O. Mason. Optimal differentially private mechanisms for randomised response. IEEE Trans. Inf. Forensics Security, 12(11):2726–2735, Nov 2017.
[19] J. Hua, A. Tang, Y. Fang, Z. Shen, and S. Zhong. Privacy-preserving utility verification of the data published by non-interactive differentially private mechanisms. IEEE Trans. Inf. Forensics Security, 11(10):2298–2311, Oct 2016.
[20] P. Kairouz, K. Bonawitz, and D. Ramage. Discrete distribution estimation under local privacy. arXiv preprint: 1602.07387, 2016.
[21] P. Kairouz, S. Oh, and P. Viswanath. Extremal mechanisms for local differential privacy. In Proc. of NIPS, pages 2879–2887, 2014.
[22] G. Kellaris and S. Papadopoulos. Practical differential privacy via grouping and smoothing. Vldb, 65(3):301–312, 2015.
[23] W. Z. Khan, Y. Xiang, M. Y. Aasalem, and Q. Arshad. Mobile phone sensing systems: A survey. IEEE Commun. Survys Tuts., 15(1):402–427, 2013.
[24] G. Li, J. Wang, Y. Zheng, and M. J. Franklin. Crowdsourced data management: A survey. IEEE Trans. Knowl. Data Eng., 28(9):2290–2319, 2016.
[25] H. Li, L. Xiong, and X. Jiang. Differentially private synthesis of multi-dimensional data using copula functions. In Proc. EDBT, pages 475–486, 2014.
[26] H. Li, L. Xiong, X. Jiang, and J. Liu. Differentially private histogram publication for dynamic datasets: an adaptive sampling approach. In Proc. of ACM CIKM, pages 1001–1010. ACM, 2015.
[27] L. Li, R. Lu, K. K. R. Choo, A. Dutta, and J. Shao. Privacy-preserving-outsourced association rule mining on vertically partitioned databases. IEEE Trans. Inf. Forensics Security, 11(8):1847–1861, Aug 2016.
[28] N. Li, W. Qardaji, and D. Su. On sampling, anonymization, and differential privacy or, k-anonymization meets differential privacy. In Proc. of ACM ASIACCS, pages 32–33, 2012.
[29] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen. Udp: Usage-based dynamic pricing with privacy preservation for smart grid. IEEE Trans. Smart Grid, 4(1):141–150, 2013.
[30] C. Liu, S. Chakraborty, and P. Mittal. Dependence makes you vulnerable: Differential privacy under dependent tuples. In Proc. of NDSS, 2016.
[31] F. D. McSherry. Privacy integrated queries: an extensible platform for privacy-preserving data analysis. In Proc. of ACM SIGMOD, 2009.
[32] M. Naveed, E. Ayday, E. W. Clayton, J. Felleay, C. A. Gunter, J. Hubaux, B. A. Malin, and X. Wang. Privacy in the genomic era. ACM Comput. Surv., 48(1):6, 2015.
[33] N. Pham, R. K. Ganti, Y. S. Udinn, S. Nath, and T. Abdelzaher. Privacy-preserving reconstruction of multidimensional data maps in vehicular participatory sensing. In European Conference on Wireless Sensor Networks, pages 114–130. Springer, 2010.
Add the following references:

[34] W. Qardaji, W. Yang, and N. Li. Priview: practical differentially private release of marginal contingency tables. In *Proc. of ACM SIGMOD*, pages 1435–1446, 2014.

[35] R. Sarathy and K. Muralidhar. Evaluating laplace noise addition to satisfy differential privacy for numeric data. *Transactions on Data Privacy*, 4(1):1–17, 2011.

[36] H. Shen, M. Zhang, and J. Shen. Efficient privacy-preserving cube-data aggregation scheme for smart grids. *IEEE Trans. Inf. Forensics Security*, 12(6):1369–1381, 2017.

[37] J. Soria-Comas, J. Domingo-Ferrer, D. Sanchez, and D. Meğlas. Individual differential privacy: A utility-preserving formulation of differential privacy guarantees. *IEEE Trans. Inf. Forensics Security*, 12(6):1418–1429, June 2017.

[38] D. Starobinski, A. Trachtenberg, and S. Agarwal. Efficient pdv synchronization. *IEEE Trans. Mobile Comput.*, 2(1):40–51, 2003.

[39] S. Su, P. Tang, X. Cheng, R. Chen, and Z. Wu. Differentially private multi-party high-dimensional data publishing. In *Proc. of IEEE ICDE*, pages 205–216, 2016.

[40] J. Sun, R. Zhang, J. Zhang, and Y. Zhang. Pristream: Privacy-preserving distributed stream monitoring of thresholded percentile statistics. In *Proc. of IEEE INFOCOM*, pages 1–9, 2016.

[41] R. Tibshirani. Regression shrinkage and selection via the lasso. *Journal of the Royal Statistical Society. Series B (Methodological)*, pages 267–288, 1996.

[42] Q. Wang, Y. Zhang, X. Lu, Z. Wang, Z. Qin, and K. Ren. Rescuedp: Real-time spatio-temporal crowd-sourced data publishing with differential privacy. In *Proc. of IEEE INFOCOM*, pages 1–9, 2016.

[43] W. Wang and Q. Zhang. Privacy-preserving collaborative spectrum sensing with multiple service providers. *IEEE Trans. Wireless Commun.*, 14(2):1011–1019, 2015.

[44] S. L. Warner. Randomized Response: A Survey Technique for Eliminating Evasive Answer Bias. *J. Am. Stat. Assoc.*, 60:63–69, 1965.