On the Performance of *k*-Anonymity Against Inference Attacks With Background Information

Ping Zhao, Hongbo Jiang, *Senior Member, IEEE,* Chen Wang, *Member, IEEE,*
Haojun Huang, Gaoyang Liu, and Yang Yang

***Abstract*—Internet of Things (IoT) applications bring in a great convenience for human's life, but users' data privacy concern is the major barrier toward the development of IoT. *k*-anonymity is a method to protect users' data privacy, but it is presently known to suffer from inference attacks. Thus far, existing work only relies on a number of experimental examples to validate *k*-anonymity's performance against inference attacks, and thereby lacks of a theoretical guarantee. To tackle this issue, in this paper we propose the first theoretical foundation that gives a nonasymptotic bound on the performance of *k*-anonymity against inference attacks, taking into consideration of adversaries' background information. The main idea is to first quantify adversaries' background information, and from the point of the view of adversaries, classify users' data into four kinds: 1) independent with unknown data values; 2) local dependent with unknown data values; 3) independent with certain known data values; and 4) local dependent with certain known data values. We then move one step further, theoretically proving the bound on the performance of *k*-anonymity corresponding to each of the four kinds of users' data through cooperating with the noiseless privacy. We argue that such a theoretical foundation links *k*-anonymity with noiseless privacy, theoretically proving *k*-anonymity provides noiseless privacy. Additionally, this paper theoretically explains why *k*-anonymity is vulnerable to inference attacks using the modified Stein method. Simulations on real check-in dataset from the location-based social network have validated our results. We believe that this paper can bridge the gap between design and evaluation, enabling a designer to construct a more practical *k*-anonymity technique in real-life scenarios to resist inference attacks.**

***Index Terms*—Inference attacks, *k*-anonymity, noiseless privacy, nonasymptotic bound.**

I. Introduction

In the era of Internet of Things (IoT), an increasing number of devices embedded with electronics, software, sensors, and actuators, are connected via the Internet, enabling various IoT applications, e.g., smart grid, smart cities, smart transportation system, etc., that offer a great benefit for human's life [2]–[4]. However, such convenience does not come for free, as users' data created by these IoT devices is collected in these IoT applications, via, e.g., data aggregation, crowdsensing, etc. [5], [6]. As a result, users' data privacy may be disclosed to the untrusted data aggregator, and more seriously, more sensitive personal information implied in users' data such as one's social relationship and political beliefs can be invaded.

A. *k*-Anonymity and Inference Attacks

k-anonymity is proposed to protect users' data privacy in such a scenario, which blurs a user's data into a cloaked data set such that the user's data cannot be distinguished from at least $(k-1)$ data of other users in this set [7]. Fig. 1(a) shows an example of *k*-anonymity, where users' ambulatory care data collected by National Association of Health Data Organizations is released to researchers or industry [7]. Assume Allen, Bob, and Alice issue three-anonymity and the other four users request for four-anonymity. To protect these users' data privacy, Allen, Bob, and Alice's ambulatory care data are cloaked together (i.e., three-anonymity), and therefore researchers and industry cannot distinguish each of the three users' ambulatory care data. Likewise, the other four users' ambulatory care data are cloaked together (i.e., four-anonymity) and thus cannot be identified. As a result, all the users' data privacy is protected.

However, *k*-anonymity is susceptible to inference attacks where adversaries identify every user's data utilizing the background information about users' data, and thus cannot fully protect users' privacy in IoT [8]–[12]. Still in Fig. 1(a), if the data aggregator has the background information that Allen has checked in the gynecological hospital, then it can further identify Allen's ambulatory care data. Another example

Manuscript received April 22, 2018; revised June 27, 2018; accepted July 18, 2018. Date of publication July 23, 2018; date of current version February 25, 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 61502192, Grant 61572219, Grant 61502193, Grant 61671216, Grant 61702204, Grant 51479159, and Grant 41701479 and in part by the Hubei Key Laboratory of Transportation Internet of Things under Grant 2016III028-01. Part of this work was presented at the Proceedings of the IEEE HPCC 2018 [1]. *(Corresponding author: Chen Wang.)*

P. Zhao is with the School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan 430074, China, and also with the College of Information Science and Technology, Donghua University, Shanghai 201620, China (e-mail: pingzhao@hust.edu.cn).

H. Jiang is with the College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China (e-mail: hongbojiang2004@gmail.com).

C. Wang and G. Liu are with the School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan 430074, China (e-mail: chenwang@hust.edu.cn; liugaoyang@hust.edu.cn).

H. Huang is with the School of Computer, China University of Geosciences, Wuhan 430074, China (e-mail: hhj0704@hotmail.com).

Y. Yang is with the School of Computer Science and Information Engineering, Hubei University, Wuhan 430062, China (e-mail: yangyang@hubu.edu.cn).

Digital Object Identifier 10.1109/JIOT.2018.2858240

of inference attacks is shown in Fig. 1(b) and (c), according to the friendships among users, 12 users' data in cloaked data are selected as landmarks [i.e., the red nodes in Fig. 1(b)], and are first mapped to the users in background information [i.e., red nodes in Fig. 1(c)] by the untrusted data aggregator. Then, the untrusted data aggregator searches for the global optimal match between cloaked data and the background information. As a result, the data privacy of users mapped to the background information is disclosed at last.

B. Existing Work Against Inference Attacks

To protect users' data privacy against inference attacks, most studies have focused on refining the data cloaked in the same set via inserting or removing edges (or nodes) into or from the cloaked data [13]–[15] cloaking users' data with same attributes and structural information in a set [16]–[19] generalizing users' data in terms of structural features [20], [21], or considering a wide range of users' data and quantifying both privacy and utility measurements of the cloaked data [22]. However, all the work has no rigorous theoretical analysis of the performance of the proposed techniques, only relying on a number of experimental examples to validate the performance against inference attacks. The question then naturally rises as what the performance of *k*-anonymity exactly is when suffering from inference attacks.

C. Our Contributions

In this paper, we propose the first theoretical foundation that gives a nonasymptotic bound on the performance of *k*-anonymity against inference attacks, taking into consideration of adversaries' background information. The intuition stems from the observation that the deterioration of the performance of *k*-anonymity is largely resulted from adversaries' background information about the cloaked data. Informally speaking, when adversaries have no prior knowledge of the cloaked data, and the data is randomized, then such randomness can effectively hide data values. For instance, as shown in Fig. 1(a), when adversaries have no background information about Allen, e.g., gender, ZIP, etc., the data value of Allen's ambulatory care data is randomized to the adversaries, thus protecting Allen's data privacy. Conversely, when adversaries know Allen frequently visits gynecology, they can infer the data value of Allen's ambulatory care data is uterine fibroid. In summary, the adversarial uncertainty about the cloaked data can be leveraged to evaluate the performance of *k*-anonymity against inference attacks.

Motivated by this intuition, the main idea is to first quantify the background information of adversaries. Then, from the point of the view of adversaries, we analyze the input of *k*-anonymity, i.e., users' data, and classify the input into four kinds: 1) independent with unknown data values; 2) local dependent with unknown data values; 3) independent with some known data values; and 4) local dependent with some known data values. For example, as analyzed above, when the data value of Allen's ambulatory care data is randomized in the view of adversaries, the data value of Allen's ambulatory care data is an unknown data value. In turn, when adversaries infer the data value of Allen's ambulatory care data is uterine fibroid, the data value of Allen's ambulatory care data is a known data value. In addition, if adversaries get the background information that Allen and Rose suffer from the same disease, the data values of ambulatory care data of Allen and Rose are dependent; otherwise independent. Then on these basis, we can thus theoretically bound the performance of *k*-anonymity corresponding to each of the four kinds of users' data, through cooperating with the noiseless privacy that exploits the inherently uncertainty in the cloaked data without injecting noise into the cloaked data to achieve privacy preservation.

The contributions of this paper are summarized as follows.

1) To the best of our knowledge, this is the first work that gives the nonasymptotic bound on the performance of *k*-anonymity against inference attacks.
2) We propose to link *k*-anonymity with noiseless privacy, and theoretically prove "cloaking in a set of size no less than *k*" offers noiseless privacy.
3) We thoroughly and theoretically analyze why *k*-anonymity is susceptible to inference attacks employing the modified Stein method.
4) We fill up the gap between design and evaluation, enabling a designer to propose a more practical privacy preserving *k*-anonymity technique in real-life scenarios to resist inference attacks.

The remainder of this paper is organized as follows. Section II introduces some preliminary knowledge we use in this paper. Section III describes this paper in detail, followed by the performance evaluation in Section IV. Finally, Section V concludes this paper. The notations throughout this paper are summarized in Table I.

II. PRELIMINARY

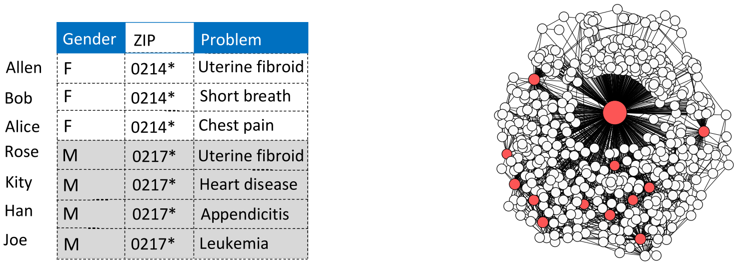
A. Syntactic Sensitivity

Definition 1: The syntactic sensitivity s of k-anonymity $\mathcal{F}$ with respect to the input data set $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_n\}$ is [23]

$$s = \max\left|\mathrm{Vol}(\mathcal{F}(\mathcal{D})) - \mathrm{Vol}\big(\mathcal{F}\big(\mathcal{D}^*\big)\big)\right| \tag{1}$$

where $\mathcal{D}^*$ is any a data set with one data is removed from or added to $\mathcal{D}$ (hereafter $\mathcal{D}^*$ is called adjacent data of $\mathcal{D}$); $\mathcal{F}(\mathcal{D})$ is the output of $\mathcal{F}$ with respect to $\mathcal{D}$; and $\mathrm{Vol}(\mathcal{F}(\mathcal{D}))$ is the number of users' data cloaked in one set by k-anonymity $\mathcal{F}$.

For instance, assume $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_n\}$ is n users' friendship data, $\mathcal{D}_i$ is user u_i's friendship data, and each tuple in $\mathcal{D}_i$ is the digital label (i.e., the pseudo-identity) of one of u_i's friends (e.g., 1 in $\mathcal{D}_i = \{1, 2, 3, \ldots\}$). Denote the set of adjacent data of $\mathcal{D}$ as $\Omega = \{\mathcal{D}_1^*, \mathcal{D}_2^*, \ldots, \mathcal{D}_n^*\}$, where $\mathcal{D}_i^* = \{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_{i-1}, \mathcal{D}_{i+1}, \ldots \mathcal{D}_n\}$ is a adjacent data of $\mathcal{D}$. Assume $\mathcal{F}(\mathcal{D}) = \{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_k\}$, namely friendship data of $u_1, \ldots, u_k$ are cloaked in one dataset. For example, if $\mathcal{F}$ cloaks $(k+1)$ users' friendship data in one dataset with respect to any a adjacent data of $\mathcal{D}$, $s = 1$. Also, if $\mathcal{F}$ cloaks $(k+3)$ users' friendship data in one dataset when input is a specific adjacent data $\mathcal{D}_i^*$, and it cloaks k users' friendship data in one dataset with respect to each of the remaining adjacent data, according to Definition 1, $s = 3$.



	Gender	ZIP	Problem
Allen	F	0214*	Uterine fibroid
Bob	F	0214*	Short breath
Alice	F	0214*	Chest pain
Rose	M	0217*	Uterine fibroid
Kity	M	0217*	Heart disease
Han	M	0217*	Appendicitis
Joe	M	0217*	Leukemia

(a) (b) (c)

Fig. 1. (a) Illustration of k-anonymity in crowdsensing. Illustration of inference attacks. (b) Contact graph in Gowalla dataset deduced from the cloaked users' traces, where nodes refer to users and the edges mean contacts. (c) Relationship graph in Gowalla dataset, where the edges mean friendships.

TABLE I
SUMMARY OF NOTATIONS

Notations	Descriptions
$\mathcal{F}$	k-anonymity technique
$\mathcal{D}$	users' data $\mathcal{D} = \{\mathcal{D}_1, \ldots, \mathcal{D}_i, \ldots, \mathcal{D}_n\}$
s	syntactic sensitivity
λ_1	λ_1 percents of users
λ_2	λ_2 percents of users
δ, ϵ	parameters in (δ, ϵ)-noiseless privacy
π_i, φ_i	$mean(\mathcal{D}_i) = \pi_i$, $mean(\mathcal{D}_i^2) = \varphi_i^2$
χ_i, ξ_i	$mean(\mathcal{D}_i^3) = \chi_i^3$, $mean(\mathcal{D}_i^4) = \xi_i^4$
N_i	dependent neighborhoods

TABLE II
INFERENCE ATTACKS WITH DIFFERENT BACKGROUND INFORMATION

Inference attacks	Sensitivity s	Dependency λ_1	Value λ_2
Level-I	√		
Level-II	√	√	
Level-III	√		√
Level-IV	√	√	√

B. Adversary Model

We consider users' data cloaked by a specific k-anonymity technique are collected by a data aggregator in IoT applications, e.g., data aggregation, crowdsensing, etc. The data aggregator may be untrusted and interested in identifying the data of each user through launching inference attacks, using its background information. On the other hand, the aggregator may also disclose the cloaked data, for some commercial interests, to researchers or industry who may be malicious and conduct inference attacks to distinguish users' data. Note that hereafter, untrusted data aggregator, malicious researchers, and industry, etc. are called adversaries, for the ease of description.

Adversaries can obtained background information through various means.

1) Many companies share users' data, e.g., Twitter shares data with its partner IBM [24].
2) A large number of data in, e.g., Twitter [25] and YouTube [25] can be crawled.
3) Users' data is widely available on, e.g., SNAP, CMU datasets [26], etc.

These available background information enables adversaries to get the access to the exact value of users' data or the dependencies among users' data. For example, in Fig. 1(a), the background information, ambulatory care data of Allen enables adversaries to identify Allen's traces (i.e., *exact value*); in Fig. 1(b) and 1(c) adversaries can infer the *dependencies* among cloaked locations employing the structure similarity between the cloaked locations and the background information (i.e., friendships in social networks). Moreover, the *syntactic sensitivity* s can also be disclosed to adversaries, since the outputs of k-anonymity techniques are known to the untrusted data aggregator, and it thus can compute the syntactic sensitivity s through observing the number of users' data cloaked in one set.

C. Quantification of Adversaries' Background Information

We quantify adversaries' background information as follows.

1) The syntactic sensitivity s.
2) The dependencies among λ_1 percents of users' data, and the syntactic sensitivity s ($\lambda_1 < 1$).
3) The exact value of λ_2 percents of users' data, and the syntactic sensitivity s ($\lambda_2 < 1$).
4) The exact value of λ_2 percents of users' data, the dependencies among λ_1 percents of users' data, and the syntactic sensitivity s.

For the ease of description, we denote level-I–IV inference attacks corresponding to the above four kinds of background information, which are shown in Table II.

On the basis of the qualified adversaries' background information, users' data can be classified into the following four kinds, from the perspective of adversaries.

1) Independent data $\mathcal{D}$ with known syntactic sensitivity s.
2) Local dependent data $\mathcal{D}$ with disclosed syntactic sensitivity s and dependencies of λ_1 percent of data.
3) Independent data $\mathcal{D}$ with known syntactic sensitivity s and a subset Θ ($\Theta \subseteq \mathcal{D}$) containing λ_2 percent of data.
4) Local dependent data $\mathcal{D}$ with a known subset Θ ($\Theta \subseteq \mathcal{D}$) containing λ_2 percent of data, the disclosed syntactic sensitivity s, and the dependencies of λ_1 percent of data.

D. Noiseless Privacy

Noiseless privacy makes efforts toward answering the question "Is it always necessary to add noise to the output to achieve provable privacy guarantees?" [27], and provides an alternative approach to achieve privacy preservation. It exploits the inherently uncertainty in the database without injecting noise into the output. Its formal definition is as follows.

Definition 2: Denote $\mathcal{F} : \mathcal{D}^n \to \mathcal{Y}$ a privacy mechanism. $\mathcal{F}$ meets (ϵ, δ)-noiseless privacy, if for all $\mathcal{O} \in \mathcal{Y}$ and all $X \in \mathcal{D}$, $X^* \in \mathcal{D}$ (X^* is obtained by removing or adding a tuple from or to X), the following holds [27]:

$$\Pr[\mathcal{F}(X) \in \mathcal{O}] \leq \exp(\epsilon)\Pr\big[\mathcal{F}\big(X^*\big) \in \mathcal{O}\big] + \delta. \tag{2}$$

It implies that the input $\mathcal{D}^n$ inherently results in the uncertainty of adversaries and thus can be protected by such uncertainty instead of the randomness of mechanisms. So even deterministic mechanisms can guarantee data privacy, satisfying noiseless privacy without adding external noise. Motivated by Definition 2, we concentrate on theoretically proving the privacy guarantees that the deterministic mechanism k-anonymity provides.

E. Theoretical Basis

We first consider an impractical case where adversaries do not have any background information about the cloaked data. To be more concrete, adversaries do not know the values of users' data, the dependencies among users' data, and even the syntactic sensitivity. In this case, from the respective of adversaries, any a k-anonymity technique $\mathcal{F}$ works as follows: randomly selecting no less than k tuples from the set of users' data $\mathcal{D}$, and cloaking these tuples into one cloaked set. Furthermore, we theoretically prove the performance of the k-anonymity technique $\mathcal{F}$ via cooperating with noiseless privacy as follows.

Theorem 1: Denote $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_n\}$. $\mathcal{F}$ randomly selects α ($\alpha \geq k$) tuples in $\mathcal{D}$ with probability p.

1) For all $\delta \geq [(n!p^k q^{n-k})/(k!(n-k)!)] + q^n$, $\mathcal{F}$ meets (ϵ, δ)-noiseless privacy with

$$\epsilon = \max\left\{\ln\left(\left(\frac{n+1}{np - \sqrt{-\frac{1}{2}n\ln\left[\delta + \exp\left(\frac{-2(np-k+1)^2}{n}\right)\right]}} - 1\right) \times \frac{p}{1-p}\right)\right.$$
$$\left. \times \ln\left(\left(\frac{n+1}{n - np - \sqrt{-\frac{1}{2}n\ln\left[\delta + \exp\left(\frac{-2(np-k+1)^2}{n}\right)\right]}} - 1\right)\frac{1-p}{p}\right)\right\}.$$

2) For all $\epsilon > 0$, $\mathcal{F}$ meets (ϵ, δ)-noiseless privacy where

$$\delta = \max\left\{\exp\left[\frac{-2\left(np - \frac{p(n+1)}{\exp(\epsilon)(1-p)+p}\right)^2}{n}\right]\right.$$
$$- \exp\left[\frac{-2(np-(k-1))^2}{n}\right]$$
$$\left. \times \exp\left[\frac{-2\left(\frac{\exp(\epsilon)np-1+p}{\exp(\epsilon)p+1-p}\right)^2}{n}\right]\right\}.$$

Proof: See Appendix A. ■

Theorem 1 gives an explicitly bound on the performance of k-anonymity when adversaries do not have any background information. However, Theorem 1 only considers a trivial scenario where the adversaries do not have any background information about the cloaked data. In practical scenario, adversaries can obtained background information through various means, thereby deteriorating the performance of k-anonymity techniques. Therefore, in the following, we consider strategic adversaries that get background information about the cloaked data, and bound the performance of k-anonymity techniques against such adversaries on the basis of Theorem 1.

III. Performance Bounds Analysis

As regard to the performance of the various k-anonymity techniques against inference attacks, we propose to bound their performance utilizing the background information of adversaries. Such a proposal stems from the observation in Theorem 1 that the sophisticatedly selected data will be the ones that are randomly selected when adversaries do not have any background information about these selected data. That is, adversarial uncertainty about the cloaked data can be leveraged to protect users' data privacy.

A. Bounds on Performance Against Level-I Inference Attacks

In this part, we consider any a k-anonymity technique $\mathcal{F}$ that selects no less than k users' data from the dataset $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_n\}$ and cloak these selected data into a set. Since only the syntactic sensitivity s is disclosed to adversaries, the cloaked data (i.e., the output of the k-anonymity technique $\mathcal{F}$) is independent with unknown values. For example, in cloaked social relationship data, each user's friendships are independent with others, and are with unknown values, since adversaries only have the background information s. In such a case, motivated by Theorem 1, we theoretically prove the performance of $\mathcal{F}$ using noiseless privacy as follows.

Lemma 1: For variable $Q \sim \mathcal{N}(0, \sigma^2)$, $\sigma \geq (cs/\epsilon_1)$, and c meets

$$\begin{cases} \ln\frac{2c^2-1}{2c} + \frac{4c^4-4c^2+1}{8c^2} > \ln\frac{1}{\sqrt{2\pi}\delta_1} \\ \frac{c^2 s}{\epsilon_1} - \frac{s}{2} > k \end{cases}$$

we get

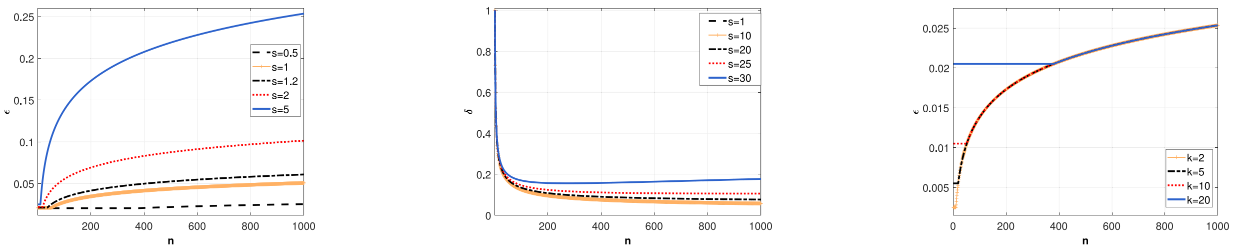
$$\Pr[u + Q \in \mathcal{O}] \leq \exp(\epsilon_1)\Pr[v + Q \in \mathcal{O}] + \delta_1$$

where S is the output of k-anonymity-based technique $\mathcal{F}$.

Proof: See Appendix B. ■

Lemma 1 extends the theory of differential privacy in [23], by considering the constraints of k-anonymity techniques (i.e., more than k tuples) and giving a tighter bound on privacy parameters (ϵ_1, δ_1).

Lemma 2: Denote variables $X = \{X_1, \ldots, X_n\}$ with variances $\sigma_1^2, \ldots, \sigma_n^2$ and finite third absolute moments



(a) (b) (c)

Fig. 2. Parameter (a) ϵ varies with syntactic sensitivity s, where $k = 10$, $\epsilon_1 = 0.1$, and $\sqrt{\sum_{i=1}^n(\varphi_i^2 - \pi_i^2)} = 50$, (b) δ varies with syntactic sensitivity s, where $\sqrt{\sum_{i=1}^n(\varphi_i^2 - \pi_i^2)} = 50$, $\sum_{i=1}^n(\chi_i^3 - 3\varphi_i^2\pi_i + 2\pi_i^3) = 1$, and $\sum_{i=1}^n(\varphi_i^2 - \pi_i^2)^{(3/2)} = 100$, and (c) ϵ varies with privacy parameter k, where $s = 1$, $\epsilon_1 = 0.1$, and $\sqrt{\sum_{i=1}^n(\varphi_i^2 - \pi_i^2)} = 50$.

$\rho_1, \ldots, \rho_n$. For the normed sum function S_n of X and the standard normal random variable N, the following holds [28]:

$$\sup_{x \in R} |\Pr[S_n \leq x] - \Pr[N \leq x]| \leq \frac{\varpi \sum_{i=1}^n \rho_i^2}{\sum_{i=1}^n \sigma_i^2}$$

where $\varpi \leq 0.5591$.

On the basis of Lemmas 1 and 2, we theoretically analyze the performance of k-anonymity technique $\mathcal{F}$ as follows.

Theorem 2: The k-anonymity technique $\mathcal{F}$ meets (ϵ, δ)-noiseless privacy with $\delta = [(1.1182 \sum_{i=1}^n(\chi_i^3 - 3\varphi_i^2\pi_i + 2\pi_i^3))/(\sum_{i=1}^n(\varphi_i^2 - \pi_i^2)^{(3/2)})](1 + \exp(\sqrt{[(s^2 \ln n)/(\sum_{i=1}^n(\varphi_i^2 - \pi_i^2))]})) + (1/\sqrt{n})$ and $\epsilon = [(c's)/(\sqrt{\sum_{i=1}^n(\varphi_i^2 - \pi_i^2)})]$, where $\mathrm{mean}(\mathcal{D}_i) = \pi_i$, $\mathrm{mean}(\mathcal{D}_i^2) = \varphi_i^2$, $\mathrm{mean}(\mathcal{D}_i^3) = \chi_i^3$, and c' is the minimum value of c that meets

$$\begin{cases} \ln \frac{2c^2-1}{2c} + \frac{4c^4-4c^2+1}{8c^2} > \ln \frac{\sqrt{n}}{\sqrt{2\pi}} \\ \frac{c^2 s}{\epsilon_1} - \frac{s}{2} > k. \end{cases}$$

Proof: See Appendix C. ■

Theorem 2 enables a designer to construct a practical and optimal k-anonymity technique in real-life scenarios to resist inference attacks, considering the background information of adversaries. As shown in Fig. 2(a) and (b), the privacy parameters ϵ and δ increase with the syntactic sensitivity s of the designed k-anonymity technique $\mathcal{F}$. That is because the output of the proposed $\mathcal{F}$ with a larger syntactic sensitivity s is sharply changed, thus resulting in a larger probability that breaches (2). Moreover, it can be observed in Fig. 2(a) and (b), privacy parameter δ is more robust to the syntactic sensitivity s than ϵ. In addition, in Fig. 2(c), the performance of the designed k-anonymity technique $\mathcal{F}$ is affected by the privacy requirement k of users. That is not surprising, as more users' data cloaked in a set results in more generalization of the cloaked data, i.e., a larger ϵ.

B. Bounds on Performance Against Level-II Inference Attacks

In level-II attacks, the dependence among λ_1 percents of users' data is disclosed to adversaries, except for the syntactic sensitivity s, which enables adversaries to launch more offensive inference attacks, e.g., de-anonymity attacks. For instance, in cloaked social relationship data, all users are labeled by pseudo-identities, and the friendships among λ_1 percent of users marked by pseudo-identity are disclosed to adversaries. Since attackers only know the friendships among these users without knowing their identities, the dependencies among the λ_1 percent of users are disclosed to adversaries. In such a scenario, accordingly, the performance of the k-anonymity-based technique $\mathcal{F}$ follows.

Theorem 3: The k-anonymity-based technique $\mathcal{F}$ meets (ϵ, δ)-noiseless privacy with $\epsilon = [(c's)/\sigma]$ and

$$\delta = 2\left(\frac{2}{\pi}\right)^{1/4}\sqrt{\frac{\lambda_1^2}{\sigma^3}\sum_{i=1}^n \chi_i^3 + \frac{\lambda_1^{\frac{3}{2}}\sqrt{26}}{\sigma^2\sqrt{\pi}}\sqrt{\sum_{i=1}^n \xi_i^4}(1+\exp(\epsilon))} + \frac{1}{\sqrt{n}}$$

where $\sigma^2 = \mathrm{var}[\sum_{i=1}^n \mathcal{D}_i]$, $\mathrm{mean}(\mathcal{D}_i^3) = \chi_i^3$, $\mathrm{mean}(\mathcal{D}_i^4) = \xi_i^4$, and $\lambda_1 = \max_{1 \leq i \leq n} | N_i |$, N_i $(i = 1, \ldots, n)$ are dependent neighborhoods, and c' is the minimum value of c satisfying

$$\begin{cases} \ln \frac{2c^2-1}{2c} + \frac{4c^4-4c^2+1}{8c^2} > \ln \frac{\sqrt{n}}{\sqrt{2\pi}} \\ \frac{c^2 s}{\epsilon_1} - \frac{s}{2} > k. \end{cases}$$

Proof: See Appendix D. ■

Theorem 3 theoretically bounds the performance of the k-anonymity-based technique $\mathcal{F}$ [see (33) and (36)]. Examples of the bounds, i.e., privacy parameters ϵ and δ are shown in Fig. 3. It can be observed in Fig. 3(a), δ increases with the amount of adversaries' background information, as adversaries can disclose more users' data when they have more background information, thereby resulting in a larger δ. In addition, as shown in Fig. 3(b), δ decreases with the decreasing ϵ, since it is more likely for adversaries to identify a specific user's data through observing the output when ϵ has a larger value. Furthermore, ϵ increases with the syntactic sensitivity s, as the output of $\mathcal{F}$ is more significantly changed with respect to the same input when $\mathcal{F}$ has a larger syntactic sensitivity s.

On the other hand, Theorem 3 motivates the designer to select quantified users' data to lower the bound of the performance of the k-anonymity-based technique $\mathcal{F}$ to be proposed. To concrete, the designer can decrease numerator and increase denominator of the formulas that formalize privacy parameters

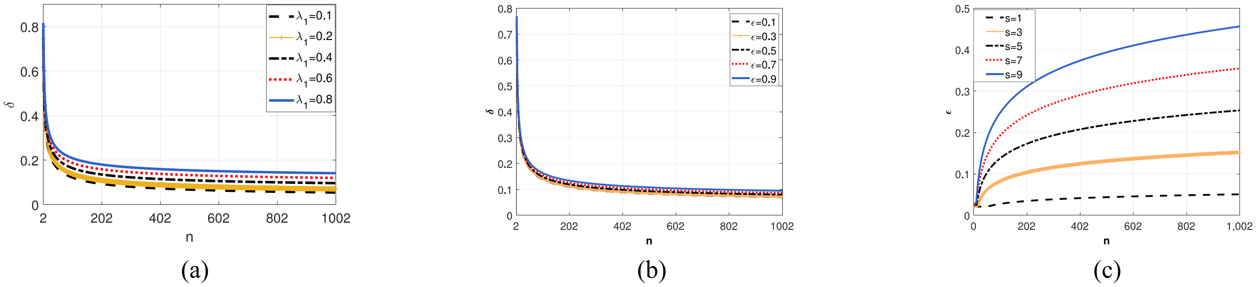


Fig. 3. Privacy parameter (a) δ varies with λ_1, where $\sigma = 50$, $\sum_{i=1}^{n} \chi_i^3 = 5$, $\sqrt{\sum_{i=1}^{n} \xi_i^4} = 1$, and $\epsilon = 0.1$, (b) δ varies with ϵ, where $\sigma = 50$, $\sum_{i=1}^{n} \chi_i^3 = 5$, $\sqrt{\sum_{i=1}^{n} \xi_i^4} = 1$, and $\lambda_1 = 0.2$, and (c) ϵ varies with s, where $\varepsilon_1 = 0.1$ and $k = 10$.

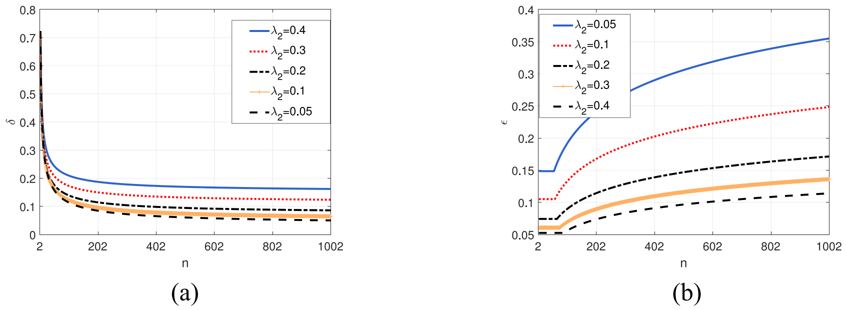


Fig. 4. Privacy parameter (a) δ varies with λ_2, where $s = 1$, $\sum_{i=1, i\notin\Gamma}^{n} (\chi_i^3 - 3\varphi_i^2\pi_i + 2\pi_i^3) = 10\lambda_2$, $\sum_{i=1, i\notin\Gamma}^{n} (\varphi_i^2 - \pi_i^2)^{(3/2)} = 100\lambda_2$, and $\sum_{i=1, i\notin\Gamma}^{n} (\varphi_i^2 - \pi_i^2) = 10\lambda_2$ and (b) ϵ varies with λ_2, where $\varepsilon_1 = 0.1$, $k = 10$, $\sum_{i=1, i\notin\Gamma}^{n} (\varphi_i^2 - \pi_i^2) = 10\lambda_2$, and $s = 1$.

ϵ and δ, through selecting quantified users' data. As such, more users' data privacy can be protected against inference attacks.

C. Bounds on Performance Against Level-III Inference Attacks

In level-III attacks, λ_2 percents of data and syntactic sensitivity s are known to adversaries. As analyzed in level-I attacks, we consider any a k-anonymity technique $\mathcal{F}$ that selects no less than k users' data from the dataset $\mathcal{D} = \{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_n\}$ and cloaks these selected data into a set. In the example of the cloaked social relationship data, friendships of λ_2 percent of users and their real identities are disclosed to adversaries. That is, adversaries have obtained the exact values of users' cloaked data. In such a scenario, the remaining $(1 - \lambda_2)$ percents of data are randomized in adversaries' perspective, and such randomness can effectively hide other data values. Therefore, we have the following theorem.

Theorem 4: The k-anonymity-based technique $\mathcal{F}$ meets (ϵ, δ)-noiseless privacy with $\delta = [(1.1182 \sum_{i=1, i\notin\Gamma}^{n} (\chi_i^3 - 3\varphi_i^2\pi_i + 2\pi_i^3))/(\sum_{i=1, i\notin\Gamma}^{n} (\varphi_i^2 - \pi_i^2)^{(3/2)})] (1 + \exp(\sqrt{[(s^2 \ln(n(1-\lambda_2)))/(\sum_{i=1, i\notin\Gamma}^{n} (\varphi_i^2 - \pi_i^2))]})) + [1/(\sqrt{n(1-\lambda_2)})]$ and $\epsilon = [(c's)/(\sqrt{\sum_{i=1, i\notin\Gamma}^{n} (\varphi_i^2 - \pi_i^2)})]$, where mean $(\mathcal{D}_i) = \pi_i$, mean $(\mathcal{D}_i^2) = \varphi_i^2$, mean $(\mathcal{D}_i^3) = \chi_i^3$, Γ is the set of the indexes of the $n\lambda_2$ users' data that is known to adversaries, and c' is the minimum value c satisfying

$$\begin{cases} \ln \frac{2c^2-1}{2c} + \frac{4c^4-4c^2+1}{8c^2} > \ln \frac{\sqrt{n(1-\lambda_2)}}{\sqrt{2\pi}} \\ \frac{c^2 s}{\epsilon_1} - \frac{s}{2} > k. \end{cases}$$

The proof of Theorem 4 is similar to that of Theorem 2, but only differ in the number of data that are not disclosed to adversaries. That is, in the proof of Theorem 4, $n(1 - \lambda_2)$ data contributes to the uncertainness of adversaries while in the proof of Theorem 2, the n data brings in the privacy preservation.

Theorem 4 qualities the deterioration of the k-anonymity technique $\mathcal{F}$ cased by adversaries' background information in level-III inference attacks (see Fig. 4). It can be observed in Fig. 4(a), privacy parameter δ increases with the amount of adversaries' background information λ_2. That is not surprising, as more background information enables adversaries to disclose more users' data, thereby increasing δ. As shown in Fig. 4(b), privacy parameter ϵ decreases with the amount of adversaries' background information λ_2. The reason is that more background information leads to a larger probability that (2) does not hold, and thus the privacy parameter ϵ is decreased.

Theorem 4 also inspires the designer to propose a practical k-anonymity-based privacy preserving technique that achieves the best performance against inference attacks, given the adversaries' background information λ_2 and s. To be more concrete, the designer can deliberately select these users' data to be cloaked in a set to decrease the numerator of the formula of parameter δ and increase the denominator of the formulas of both δ and ϵ in Theorem 4. The decreased parameter δ means less probability that users' data privacy is disclosed, and the decreased parameter ϵ means that it is more difficult for adversaries to infer users' data privacy through observing the output of the proposed k-anonymity technique $\mathcal{F}$. As a result, more users' data privacy is protected.

D. Bounds on Performance Against Level-IV Inference Attacks

In this section, we consider stronger adversaries that have the prior knowledge of the exact values of $n\lambda_2$ users' data, the dependence among $n\lambda_1$ users' data, and the syntactic sensitivity s. Still in the example of the cloaked social relationship data, the friendships among λ_1 percent of users marked by pseudo-identity and the friendships of λ_2 percent of users marked by their real identities are disclosed to adversaries. That is, adversaries get the exact values of users' cloaked data and the dependence among the cloaked data. The performance of the proposed privacy preserving technique $\mathcal{F}$ against such adversaries is presented as follows.

Theorem 5: The k-anonymity-based technique $\mathcal{F}$ meets (ϵ, δ)-noiseless privacy with $\epsilon = [(c's)/\sigma]$ and

$$\delta = 2\left(\frac{2}{\pi}\right)^{1/4} \sqrt{\frac{\lambda_1^2}{\sigma^3} \sum_{i=1, i \notin \Gamma}^{n} \chi_i^3 + \frac{\lambda_1^{\frac{3}{2}} \sqrt{26}}{\sigma^2 \sqrt{\pi}} \sqrt{\sum_{i=1, i \notin \Gamma}^{n} \xi_i^4}} \times (1 + \exp(\epsilon)) + \frac{1}{\sqrt{n(1-\lambda_2)}}$$

where $\sigma^2 = \text{var}[\sum_{i=1, i\notin\Gamma}^{n} \mathcal{D}_i]$, mean $(\mathcal{D}_i^3) = \chi_i^3$, mean$(\mathcal{D}_i^4) = \xi_i^4$, and $\lambda_1 = \max_{1\leq i\leq n} \mid N_i \mid$, N_i $(i = 1, \ldots, n)$ are the dependent neighborhoods, and c' is the minimum value c that meets

$$\begin{cases} \ln \frac{2c^2-1}{2c} + \frac{4c^4-4c^2+1}{8c^2} > \ln \frac{\sqrt{n(1-\lambda_2)}}{\sqrt{2\pi}} \\ \frac{c^2 s}{\epsilon_1} - \frac{s}{2} > k. \end{cases}$$

The proof of Theorem 5 is analogous to the proof of Theorem 3, only differing in the number of users' data that contributes to the uncertainness of adversaries.

Examples of the bound on the performance of $\mathcal{F}$ are shown in Fig. 5. The privacy parameter δ decreases with the increasing λ_2 when $\lambda_2 \leq 0.2$, and increases with increasing λ_2 when $\lambda_2 \geq 0.3$, as shown in Fig. 5(a). That is because, δ is affected by both λ_2 and ϵ, and ϵ is affected by λ_2 at the same time. Moreover, the background information λ_2 contributes to the probability that adversaries successfully disclose users' data privacy. In addition, Fig. 5(c) shows that δ increases with λ_1, since adversaries benefit from the background information. Furthermore, in Fig. 5(d), ϵ decreases with λ_2, since more background information leads to a larger probability that (2) does not hold. Lastly, as analyzed above, Theorem 5 also motivates the designer to select quantified users' data to achieve better performance against inference attacks.

IV. Performance Evaluation

A. Setup

We employ check-in dataset from the location-based social network, Gowalla, which collects friendships among 196 591 users from February 2009 and October 2010. We first cloak each user's friendships using the two existing k-anonymity techniques [29] (hereafter CA) and [16] (hereafter IA). CA generalizes users' associated structural information (i.e., friendships) so that every user is indistinguishable with at least other $(k-1)$ users. In contrast, IA cloaks users' friendships via adding or deleting edges (edge means friendship between two users) to prevent each user's identity from being identified. In addition, we propose the k-anonymity technique, baseline (hereafter BE) that cloaks a specific user's data with no less than $(k-1)$ other users' data that minimize both δ and ϵ, given adversaries' background information.

TABLE III
FU Varies With Background Information ($k = 6$)

Background information	Level-I inference attacks		
k-anonymity technique	IA	CA	BE
FU (MLE)	18%	17.8%	17%
FU (BAS)	17.9%	17.4%	16.9%

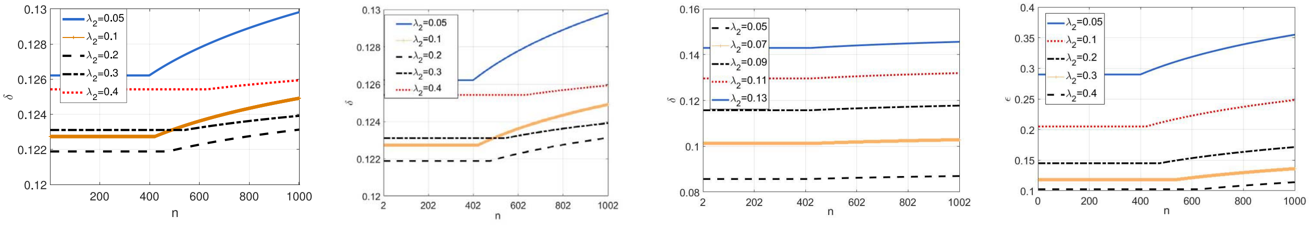
FU means the fraction of identified users.

Adversaries launch the existing inference attacks, MLE and BAS [30], to identify each user's identity in Gowalla dataset, and thus further get the knowledge of its friends (i.e., the cloaked friendships). The friendships among λ_1 percent of users marked by pseudo-identity are disclosed to adversaries in level-II and IV. In such a case, adversaries in level-II and IV only know the friendships among these users without knowing their identities. That is, the dependencies among the λ_1 percent of users are disclosed to adversaries in level-II and IV. The friends of λ_2 percent of users marked by their real identity, i.e., exact values, are randomly selected as the background information and disclosed to adversaries in level-III and IV. In addition, in level-I–IV inference attacks, adversaries are allowed to observe outputs of the three k-anonymity techniques, so they can know the syntactic sensitivity s.

B. Performance Varies With Background Information

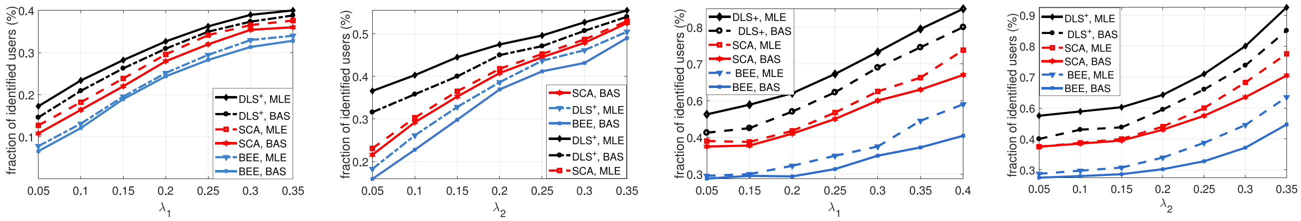
Table III shows the fraction of identified users in level-I inference attacks. As expected, the fraction of identified users in both CA and IA is larger than that in BE. The reason is that CA and IA heuristically change the structural information, while BE outputs the cloaked data to minimize both δ and ε according to the adversarial uncertainty.

Fig. 6 shows the fraction of identified users both in level-II–IV inference attacks, where the fraction of identified users in level-IV [see Fig. 6(c) and (d)] is larger than that both in level-II [see Fig. 6(a)] and level-III [see Fig. 6(b)], and the fraction of identified users in level-III is larger than that in level-II at the same time. The reason is that more background information enables adversaries to identify more users' data. Moreover, it can be observed from Fig. 6(a) and (b), more users' data can be identified when adversaries have the knowledge of λ_2 percent of users' data than the dependencies among λ_1 percent of users' data. In addition, more users' data is identified by adversaries in MLE than BAS, because MLE is more aggressive as it excludes a trace from further consideration as soon as it determines that the trace cannot be the revealed locations of the victim. In contrast, BAS returns lower fractions of identified users as it gives equal weights to traces that agree with the side information. Furthermore, the fraction



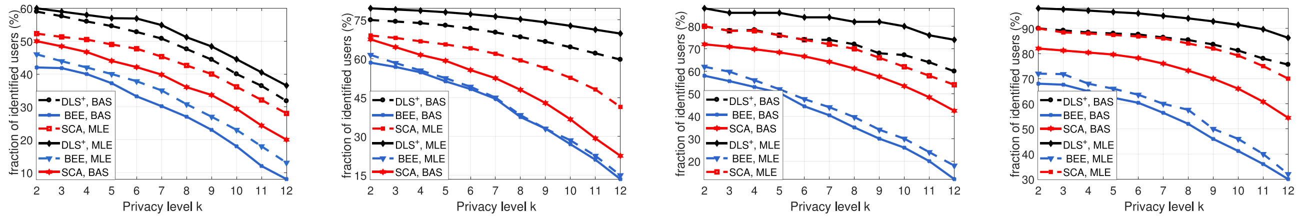
(a) (b) (c) (d)

Fig. 5. Privacy parameter (a) and (b) δ varies with λ_2 and λ_1, where $\sum_{i=1,i\notin\Gamma}^{n} \chi_i^3 = 5\lambda_2$, $\sqrt{\sum_{i=1,i\notin\Gamma}^{n} \xi_i^4} = 5\lambda_2$, $\sigma^2 = 1000\lambda_2$, $k = 20$, $s = 1$, $\epsilon_1 = 0.1$, and $\lambda_1 = 0.1$ in (a) [$\lambda_2 = 0.1$ in (b)] and (c) ϵ varies with λ_2, with $k = 20$, $\sigma^2 = 1000\lambda_2$, $s = 1$, and $\epsilon_1 = 0.1$.



(a) (b) (c) (d)

Fig. 6. Fraction of identified users varies with background information, where $k = 6$. (a) Fraction of identified users varies with λ_2 in level-II inference attacks. (b) Fraction of identified users varies with λ_2 in level-III inference attacks. (c) and (d) Fraction of identified users varies with λ_2 and λ_1 in level-IV inference attacks.



(a) (b) (c) (d)

Fig. 7. Fraction of identified users varies with privacy parameter k, where $\lambda_1 = \lambda_2 = 0.2$. Impact of k in (a) level-I inference attacks, (b) level-II inference attacks, (c) level-III inference attacks, and (d) level-IV inference attacks.

of identified users in CA and IA is larger than that in BE both in level-II–IV inference attacks. Lastly, Fig. 6 motivates designers to propose a k-anonymity-based privacy preserving technique that achieves the best performance against inference attacks, considering the adversaries' background information.

C. Performance Varies With Privacy Parameter k

This part investigates the impact of privacy parameter k. Fig. 7 shows the fraction of identified users when users perform different k. The results show that the fraction of identified users in level-I–IV inference attacks decreases with k. It is not surprising, as when a specific user issues a larger k, more users' data will be cloaked with the user's data. As a result, adversaries have less probability to disclose the user's data privacy. Furthermore, it can be observed that the fraction of identified users is less affected by k when adversaries have more background information, as background information enables adversaries to distinguish each user's data. In addition, as we expected, users' data cloaked by BE is more difficult to be identified when increasing privacy parameter k. This is attributed to the fact that BE protects users' data privacy using the adversarial uncertainty about the cloaked data, and that the increasing privacy parameter k significantly increases the adversarial uncertainty. Lastly, Fig. 7 inspires designers to set appropriate k and select quantified users' data to protect more users' data privacy against inference attacks.

V. Conclusion

In this paper, we have presented the first theoretical foundation that gives a nonasymptotic bound on the performance of k-anonymity against inference attacks. In addition, this paper thoroughly and theoretically analyses why k-anonymity is susceptible to these attacks employing the modified Stein method. Simulations on real check-in dataset from the location-based social network have validated that there exists a nonasymptotic bound on the performance of k-anonymity, given attacks' background information. Furthermore, the background information, exact values of users' data enable attackers to disclose more users' data privacy than the prior knowledge of dependencies among users' data. We believe that this paper can bridge the gap between design and evaluation, enabling a designer to propose a more practical k-anonymity technique in real-life scenarios to resist inference attacks.

Appendix A
Proof of Theorem 1

Since $\mathcal{F}$ selects each tuple in $\mathcal{D}$ with probability p, $\mathcal{F}$ can be mapped to the mechanism $\mathcal{M}$ that meets: $\mathcal{M} = \sum_1^n X_i$, $X_i \sim B(1,p)$, $\mathcal{M} \in [np-\mu, np+\mu]$, $np+\mu < n$, and $np-\mu > k$.

1) For statement 1, denote $\|\alpha-\alpha^*\|_1 = 1, \alpha \in [np-\mu, np+\mu]$. We first have to bound $[(\Pr[\mathcal{M}=\alpha])/(\Pr[\mathcal{M}=\alpha^*])]$. When $0 < p < (1/2)-(k/2n)$, $\alpha = \lceil np-\mu \rceil$, and $\alpha^* = \alpha - 1$, $[(\Pr[\mathcal{M}=\alpha])/(\Pr[\mathcal{M}=\alpha^*])]$ achieves the maximum value. Otherwise, when $\alpha = \lfloor np+\mu \rfloor$, and $\alpha^* = \alpha+1$, $[(\Pr[\mathcal{M}=\alpha])/(\Pr[\mathcal{M}=\alpha^*])]$ achieves the maximum value.

Case 1: $0 < p < (1/2)-(k/2n)$ and $X_i \sim B(1,p)$. Then we get

$$\begin{aligned}\frac{\Pr[\mathcal{M}=\alpha]}{\Pr[\mathcal{M}=\alpha^*]} &= \frac{\Pr[\mathcal{M}=\alpha]}{\Pr[\mathcal{M}=\alpha-1]}\\ &= \frac{n-\lceil np-\mu\rceil+1}{\lceil np-\mu\rceil}\frac{p}{1-p}\\ &< \frac{n-(np-\mu)+1}{np-\mu}\frac{p}{1-p}.\end{aligned} \tag{3}$$

Denote $\exp(\epsilon) = [(n-(np-\mu)+1)(np-\mu)][p/(1-p)]$, and thus we get $\epsilon = \ln([(n-(np-\mu)+1)/(np-\mu)][p/(1-p)])$.

Case 2: $1 > p > (1/2)-(k/2n)$ and $X_i \sim B(1,p)$. Similarly,

$$\begin{aligned}\frac{\Pr[\mathcal{M}=\alpha]}{\Pr[\mathcal{M}=\alpha^*]} &= \frac{\Pr[\mathcal{M}=\alpha]}{\Pr[\mathcal{M}=\alpha+1]}\\ &= \frac{\lfloor np+\mu\rfloor+1}{n-\lfloor np+\mu\rfloor}\frac{1-p}{p}\\ &< \frac{np+\mu+1}{n-(np+\mu)}\frac{1-p}{p}.\end{aligned} \tag{4}$$

Denote $\exp(\epsilon) = [(np+\mu+1)/(n-(np+\mu))]\ [(1-p)/p]$. So $\epsilon = \ln([(np+\mu+1)/(n-(np+\mu))][(1-p)/p])$.

So far, we have proved for $\alpha \in [np-\mu, np+\mu] \cap \mathbb{Z}$ and $\|\alpha-\alpha^*\|_1 = 1$, the following holds:

$$\Pr[\mathcal{M}=\alpha] < \exp(\epsilon)\Pr\big[\mathcal{M}=\alpha^*\big] \tag{5}$$

where

$$\epsilon = \begin{cases}\ln\Big(\frac{n-(np-\mu)+1}{np-\mu}\frac{p}{1-p}\Big), & p < \frac{1}{2}-\frac{k}{2n}\\ \ln\Big(\frac{np+\mu+1}{n-(np+\mu)}\frac{1-p}{p}\Big), & p \geq \frac{1}{2}-\frac{k}{2n}.\end{cases} \tag{6}$$

Next, we focus on the probability δ that the above inequality is violated. According to the Chernoff bounds, we have

$$\Pr\big[\mathcal{M} < np-\mu\big] + \Pr\big[\mathcal{M} > np+\mu\big] \leq 2\exp\Big(-2\mu^2/n\Big). \tag{7}$$

Since $\mathcal{F}$ selects no less than k tuples in $\mathcal{D}$, $\delta = 2\exp(-2\mu^2/n) - \exp(-2(np-(k-1))^2/n)$. We get $\mu = \sqrt{-(1/2)n\ln[\delta+\exp([(-2(np-k+1)^2)/n])]}$. We further get

$$\epsilon = \begin{cases}\ln\left(\frac{n+1}{np-\sqrt{-\frac{1}{2}n\ln\Big[\delta+\exp\Big(\frac{-2(np-k+1)^2}{n}\Big)\Big]}}-1\right)\\ \quad + \ \ln\frac{p}{1-p}, p < \frac{1}{2}-\frac{k}{2n}\\ \ln\left(\frac{n+1}{n-np-\sqrt{-\frac{n}{2}\ln\Big[\delta+\exp\Big(\frac{-2(np-k+1)^2}{n}\Big)\Big]}}-1\right)\\ \quad +\ln\frac{1-p}{p}, p \geq \frac{1}{2}-\frac{k}{2n}.\end{cases} \tag{8}$$

2) For statement 2, when $p < (1/2)-(k/2n)$, we aim to find the maximum value of α so that $\Pr[\mathcal{M}=\alpha] \geq \exp(\epsilon)\Pr[\mathcal{M}=\alpha^*]$. Similar to the analysis of statement 1, we have

$$\begin{aligned}\frac{\Pr[\mathcal{M}=\alpha]}{\Pr[\mathcal{M}=\alpha^*]} &= \frac{\Pr[\mathcal{M}=\alpha]}{\Pr[\mathcal{M}=\alpha-1]}\\ &= \frac{n-\alpha+1}{\alpha}\frac{p}{1-p} \geq \exp(\epsilon).\end{aligned} \tag{9}$$

So we get

$$\alpha \leq \frac{p(n+1)}{\exp(\epsilon)(1-p)+p}. \tag{10}$$

According to the Chernoff bounds

$$\Pr\big[\mathcal{M} < np-(np-\alpha)\big] \leq \exp\left(\frac{-2\Big(np-\frac{p(n+1)}{\exp(\epsilon)(1-p)+p}\Big)^2}{n}\right). \tag{11}$$

As no less than k tuples are selected, we denote $\delta_1 = \exp([(-2(np-[(p(n+1))/(\exp(\epsilon)(1-p)+p)])^2)/n]) - \exp([(-2(np-(k-1))^2)n])$.

When $p \geq (1/2)-(k/2n)$, we want to find the minimum value of α so that $\Pr[\mathcal{M}=\alpha] < \exp(\epsilon)\Pr[\mathcal{M}=\alpha^*]$ does not hold

$$\frac{\Pr[\mathcal{M}=\alpha]}{\Pr[\mathcal{M}=\alpha^*]} = \frac{\Pr[\mathcal{M}=\alpha]}{\Pr[\mathcal{M}=\alpha+1]} = \frac{\alpha+1}{n-\alpha}\frac{1-p}{p} \leq \exp(\epsilon). \tag{12}$$

We get $\alpha \geq [(\exp(\epsilon)np-(1-p))/(\exp(\epsilon)p+1-p)]$.

According to the Chernoff bounds, we get

$$\Pr\big[\mathcal{M} > np+(\alpha-np)\big] \leq \exp\left(\frac{-2\Big(\frac{\exp(\epsilon)np-(1-p)}{\exp(\epsilon)p+1-p}-np\Big)^2}{n}\right). \tag{13}$$

Thus we get $\delta_2 = \exp([(-2([(\exp(\epsilon)np-(1-p))/(\exp(\epsilon)p+1-p)]-np)^2)/n])$.

Finally, $\delta = \max\{\delta_1, \delta_2\} = \max\{\exp[[(-2(np-[(p(n+1))/(\exp(\epsilon)(1-p)+p)])^2)/n]] - \exp[(-2(np-(k-1))^2)/n], \exp[[(-2([(\exp(\epsilon)np-1+p)/(\exp(\epsilon)p+1-p)]-np)^2)/n]]\}$. Overall, Theorem 1 holds.

APPENDIX B
PROOF OF LEMMA 1

We first prove the bounds of parameters σ and c.

The ratio of probabilities that $\mathcal{F}$ outputs the same outcome when the input is $\mathcal{D}$ and $\mathcal{D}^*$ is

$$\left|\ln\frac{\exp\left(-\frac{1}{2\sigma^2}u^2\right)}{\exp\left(\left(-\frac{1}{2\sigma^2}\right)(u+s)^2\right)}\right| = \left|\frac{1}{2\sigma^2}\left(2us+s^2\right)\right| \tag{14}$$

which is bounded by ϵ_1, so we get $u \le [(\sigma^2\epsilon_1)s] - (s/2)$. In addition, since more than k data is selected to perform k-anonymity, $[(\sigma^2\epsilon_1)s] - (s/2) > k$. Moreover, (14) is bounded by ϵ_1 with probability at least $(1-\delta_1)$, and thus

$$\Pr\left[x \ge \frac{\sigma^2\epsilon_1}{s} - \frac{s}{2}\right] < \frac{\sigma}{\sqrt{2\pi}}\exp\left(-\frac{\left(\frac{\sigma^2\epsilon_1}{s}-\frac{s}{2}\right)^2}{2\sigma^2}\right) < \delta_1. \tag{15}$$

Denote $\sigma = cs/\epsilon_1$. According to (15), we get

$$\ln\left(c - \frac{\epsilon_1}{2c}\right) + \frac{1}{2}\left(c^2 - \epsilon_1 + \frac{\epsilon_1^2}{4c^2}\right) > \ln\frac{1}{\sqrt{2\pi}\delta_1}. \tag{16}$$

Since function $g(\epsilon_1) = \ln(c - (\epsilon_1/2c)) + (1/2)(c^2 - \epsilon_1 + (\epsilon_1^2/4c^2))$ decreases with ϵ_1 and $0 < \epsilon_1 < 1$

$$\ln\frac{2c^2-1}{2c} + \frac{4c^4-4c^2+1}{8c^2} > \ln\frac{1}{\sqrt{2\pi}\delta_1}. \tag{17}$$

Since $[(\sigma^2\epsilon_1)/s] - (s/2) > k$ and $\sigma = cs/\epsilon_1$, $[(c^2s)/\epsilon_1] - (s/2) > k$.

Then we prove $\Pr[u+Q \in \mathcal{O}] \le \exp(\epsilon_1)\Pr[v+Q \in \mathcal{O}] + \delta_1$ as follows:

$$\begin{aligned}\Pr[u+Q\in\mathcal{O}] &= \Pr\left[u+Q\in\mathcal{O} \mid u \le \frac{\sigma^2\epsilon_1}{s} - \frac{s}{2}\right]\\ &\quad + \Pr\left[u+Q\in\mathcal{O} \mid u > \frac{\sigma^2\epsilon_1}{s} - \frac{s}{2}\right]\\ &\le \Pr\left[u+Q\in\mathcal{O} \mid u \le \frac{\sigma^2\epsilon_1}{s} - \frac{s}{2}\right] + \delta_1\\ &\le \exp(\epsilon_1)\Pr\left[v+Q\in\mathcal{O} \mid u \le \frac{\sigma^2\epsilon_1}{s} - \frac{s}{2}\right] + \delta_1\\ &\le \exp(\epsilon_1)\Pr[v+Q\in\mathcal{O}] + \delta_1.\end{aligned} \tag{18}$$

In summary, Lemma 1 holds.

APPENDIX C
PROOF OF THEOREM 2

Denote $W_i = \mathcal{D}_i - \pi_i$, then $\text{mean}(W_i) = 0$, $\text{mean}(W_i^2) = \varphi_i^2 - \pi_i^2$, $\text{mean}(W_i^3) = \chi_i^3 - 3\varphi_i^2\pi_i + 2\pi_i^3$, and $\text{var}(W_i) = \varphi_i^2 - \pi_i^2$. Denote $Q \sim (0, \sum_{i=1}^n(\varphi_i^2 - \pi_i^2))$. According to Lemma 2, we get

$$\begin{aligned}\Pr[W \in B_u] &\le \Pr[Q \in B_u]\\ &\quad + \frac{1.1182\sum_{i=1}^n\left(\chi_i^3 - 3\varphi_i^2\pi_i + 2\pi_i^3\right)}{\sum_{i=1}^n\left(\varphi_i^2-\pi_i^2\right)^{\frac{3}{2}}}.\end{aligned} \tag{19}$$

According to Lemma 1, we get

$$\begin{aligned}\Pr[Q \in B_u] &+ \frac{1.1182\sum_{i=1}^n\left(\chi_i^3 - 3\varphi_i^2\pi_i + 2\pi_i^3\right)}{\sum_{i=1}^n\left(\varphi_i^2-\pi_i^2\right)^{\frac{3}{2}}}\\ &\le \exp(\epsilon)\Pr[Q\in B_v]\\ &\quad + \frac{1.1182\sum_{i=1}^n\left(\chi_i^3 - 3\varphi_i^2\pi_i + 2\pi_i^3\right)}{\sum_{i=1}^n\left(\varphi_i^2-\pi_i^2\right)^{\frac{3}{2}}} + \delta_1.\end{aligned} \tag{20}$$

Let $\delta_1 = (1/\sqrt{n})$, from Lemma 1, we get

$$\epsilon_1 \ge \frac{c's}{\sqrt{\sum_{i=1}^n\left(\varphi_i^2-\pi_i^2\right)}} \tag{21}$$

where c' is the minimum value c satisfying

$$\begin{cases}\ln\frac{2c^2-1}{2c} + \frac{4c^4-4c^2+1}{8c^2} > \ln\frac{\sqrt{n}}{\sqrt{2\pi}}\\ \frac{c^2s}{\epsilon_1} - \frac{s}{2} > k.\end{cases} \tag{22}$$

Thus, we get the privacy parameter ϵ as

$$\epsilon = \frac{c's}{\sqrt{\sum_{i=1}^n\left(\varphi_i^2-\pi_i^2\right)}}. \tag{23}$$

Again from Lemma 2, we get

$$\begin{aligned}\exp(\epsilon)\Pr[Q \in B_v] &+ \frac{1.1182\sum_{i=1}^n\left(\chi_i^3 - 3\varphi_i^2\pi_i + 2\pi_i^3\right)}{\sum_{i=1}^n\left(\varphi_i^2-\pi_i^2\right)^{\frac{3}{2}}} + \frac{1}{\sqrt{n}}\\ &\le \exp(\epsilon)\Pr[Q\in B_v]\\ &\quad + \frac{1.1182\sum_{i=1}^n\left(\chi_i^3 - 3\varphi_i^2\pi_i + 2\pi_i^3\right)}{\sum_{i=1}^n\left(\varphi_i^2-\pi_i^2\right)^{\frac{3}{2}}}\\ &\quad \times\left(1 + \exp\left(\sqrt{\frac{s^2\ln n}{\sum_{i=1}^n\left(\varphi_i^2-\pi_i^2\right)}}\right)\right) + \frac{1}{\sqrt{n}}.\end{aligned} \tag{24}$$

So we get privacy parameter δ

$$\begin{aligned}\delta = &\frac{1.1182\sum_{i=1}^n\left(\chi_i^3 - 3\varphi_i^2\pi_i + 2\pi_i^3\right)}{\sum_{i=1}^n\left(\varphi_i^2-\pi_i^2\right)^{\frac{3}{2}}}\\ &\times\left(1 + \exp\left(\sqrt{\frac{s^2\ln n}{\sum_{i=1}^n\left(\varphi_i^2-\pi_i^2\right)}}\right)\right) + \frac{1}{\sqrt{n}}.\end{aligned} \tag{25}$$

Lastly, we get

$$\Pr[W \in B_u] \le \exp(\epsilon)\Pr[W \in B_v] + \delta. \tag{26}$$

So we get

$$\Pr[\mathcal{D} \in B_{u'}] \le \exp(\epsilon)\Pr[\mathcal{D} \in B_{v'}] + \delta. \tag{27}$$

According to Definition 2, Theorem 2 holds.

APPENDIX D
PROOF OF THEOREM 3

Denote $B_u = \{b + u : b \in B\}$, $B_u/\sigma = \{b/\sigma : b \in B_u\}$, and $Q \sim N(0, n\sigma^2)$. According to Lemma 2

$$\Pr\left[\frac{S}{\sigma} \in \frac{B_u}{\sigma}\right] \le \Pr\left[\frac{Q}{\sigma} \in \frac{B_u}{\sigma}\right] + 2d_K\left(\frac{S}{\sigma}, Q\right) \tag{28}$$

where $d_K((S/\sigma), Q) = \sup_{t\in R} \mid F_S(t) - F_Q(t) \mid$ is the Kolmogorov metric [31]. According to Lemma 1

$$\Pr\left[\frac{Q}{\sigma} \in \frac{B_u}{\sigma}\right] + 2d_K\left(\frac{S}{\sigma}, Q\right) \le \exp(\epsilon)\Pr\left[\frac{Q}{\sigma} \in \frac{B_v}{\sigma}\right] + 2d_K\left(\frac{S}{\sigma}, Q\right) + \delta_1. \quad (29)$$

According to Lemma 2

$$\exp(\epsilon)\Pr\left[\frac{Q}{\sigma} \in \frac{B_v}{\sigma}\right] + 2d_K\left(\frac{S}{\sigma}, Q\right) + \delta_1 \le \exp(\epsilon) \times \Pr\left[\frac{S}{\sigma} \in \frac{B_v}{\sigma}\right] + 2d_K\left(\frac{S}{\sigma}, Q\right)(1 + \exp(\epsilon)) + \delta_1. \quad (30)$$

So, combining (28)–(30), we get

$$\Pr\left[\frac{S}{\sigma} \in \frac{B_u}{\sigma}\right] \le \exp(\epsilon)\Pr\left[\frac{S}{\sigma} \in \frac{B_v}{\sigma}\right] + 2d_K\left(\frac{S}{\sigma}, Q\right)(1 + \exp(\epsilon)) + \delta_1. \quad (31)$$

Denote $\delta = 2d_K([S/\sigma], Q)(1 + \exp(\epsilon)) + \delta_1$, we have

$$\Pr\left[\frac{S}{\sigma} \in \frac{B_u}{\sigma}\right] \le \exp(\epsilon)\Pr\left[\frac{S}{\sigma} \in \frac{B_v}{\sigma}\right] + \delta. \quad (32)$$

Next, we focus on computing parameters ϵ and δ. δ_1 and ϵ are parameters in Lemma 1. According to the proof of Lemma 1, we let $\delta_1 = (1/\sqrt{n})$ and thus get

$$\epsilon = \frac{c's}{\sqrt{\mathrm{var}\left[\sum_{i=1}^{n} \mathcal{D}_i\right]}} \quad (33)$$

where c' is the minimum value c satisfying

$$\begin{cases} \ln \frac{2c^2-1}{2c} + \frac{4c^4-4c^2+1}{8c^2} > \ln \frac{\sqrt{n}}{\sqrt{2\pi}} \\ \frac{c^2 s}{\epsilon_1} - \frac{s}{2} > k. \end{cases} \quad (34)$$

According to [31, Th. 3.6]

$$d_K\left(\frac{S}{\sigma}, Q\right) \le \left(\frac{2}{\pi}\right)^{1/4} \sqrt{d_W\left(\frac{S}{\sigma}, Q\right)} \le \left(\frac{2}{\pi}\right)^{1/4} \sqrt{\frac{\lambda_1^2}{\sigma^3} \sum_{i=1}^{n} \chi_i^3 + \frac{\lambda_1^{\frac{3}{2}}\sqrt{26}}{\sigma^2\sqrt{\pi}} \sqrt{\sum_{i=1}^{n} \xi_i^4}} \quad (35)$$

where d_W is the Wasserstein metric [31]. So we get

$$\delta = 2\left(\frac{2}{\pi}\right)^{1/4} \sqrt{\frac{\lambda_1^2}{\sigma^3} \sum_{i=1}^{n} \chi_i^3 + \frac{\lambda_1^{\frac{3}{2}}\sqrt{26}}{\sigma^2\sqrt{\pi}} \sqrt{\sum_{i=1}^{n} \xi_i^4}} \times (1 + \exp(\epsilon)) + \frac{1}{\sqrt{n}}. \quad (36)$$

In summary, Theorem 3 holds.

References

[1] P. Zhao, H. Jiang, C. Wang, and H. Huang, "Non-asymptotic bound on the performance of k-anonymity against inference attacks," in *Proc. 20th IEEE HPCC*, Exeter, U.K., 2018.

[2] C. Wang, H. Lin, and H. Jiang, "CANS: Towards congestion-adaptive and small stretch emergency navigation with wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 15, no. 5, pp. 1077–1089, May 2016.

[3] Q. Yang *et al.*, "Towards data integrity attacks against optimal power flow in smart grid," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1726–1738, Oct. 2017.

[4] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[5] X. Yao, Y. Chen, R. Zhang, Y. Zhang, and Y. Lin, "Beware of what you share: Inferring user locations in Venmo," *IEEE Internet Things J.*, to be published.

[6] W. Zhou, Y. Zhang, and P. Liu, "The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *CoRR*, arXiv preprint arXiv:1802.03110, 2018.

[7] L. Sweeney, "k-anonymity: A model for protecting privacy," *Int. J. Uncertainty Fuzziness Knowl. Based Syst.*, vol. 10, no. 5, pp. 557–570, 2002.

[8] S. Nilizadeh, A. Kapadia, and Y.-Y. Ahn, "Community-enhanced de-anonymization of online social networks," in *Proc. ACM CCS*, 2014, pp. 537–548.

[9] J. Song, S. Lee, and J. Kim, "Inference attack on browsing history of Twitter users using public click analytics and Twitter metadata," *IEEE Trans. Depend. Secure Comput.*, vol. 13, no. 3, pp. 340–354, May/Jun. 2016.

[10] S. Ji, W. Li, M. Srivatsa, and R. Beyah, "Structural data de-anonymization: Theory and practice," *IEEE/ACM Trans. Netw.*, vol. 24, no. 6, pp. 3523–3536, Dec. 2016.

[11] J. Qian, X.-Y. Li, C. Zhang, and L. Chen, "De-anonymizing social networks and inferring private attributes using knowledge graphs," in *Proc. IEEE INFOCOM*, San Francisco, CA, USA, 2016, pp. 1–9.

[12] P. Zhao *et al.*, "ILLIA: Enabling k-anonymity-based privacy preserving against location injection attacks in continuous LBS queries," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1033–1042, Apr. 2018.

[13] B. Zhou and J. Pei, "Preserving privacy in social networks against neighborhood attacks," in *Proc. IEEE ICDE*, 2008, pp. 506–515.

[14] E. Zheleva and L. Getoor, *Preserving the Privacy of Sensitive Relationships in Graph Data* (Lecture Notes in Computer Science), vol. 4890. Heidelberg, Germany: Springer, 2008, pp. 153–172.

[15] M. Yuan, L. Chen, and P. S. Yu, "Personalized privacy protection in social networks," *Proc. VLDB Endowment*, vol. 4, no. 2, pp. 141–150, 2010.

[16] K. Liu and E. Terzi, "Towards identity anonymization on graphs," in *Proc. ACM SIGMOD*, 2008, pp. 93–106.

[17] J. Cheng, A. W.-C. Fu, and J. Liu, "k-isomorphism: Privacy preserving network publication against structural attacks," in *Proc. ACM SIGMOD*, Indianapolis, IN, USA, 2010, pp. 459–470.

[18] H. Jiang, P. Zhao, and C. Wang, "RobLoP: Towards robust privacy preserving against location dependent attacks in continuous LBS queries," *IEEE/ACM Trans. Netw.*, vol. 26, no. 2, pp. 1018–1032, Apr. 2018.

[19] F. Qiu, F. Wu, and G. Chen, "Privacy and quality preserving multimedia data aggregation for participatory sensing systems," *IEEE Trans. Mobile Comput.*, vol. 14, no. 6, pp. 1287–1300, Jun. 2015.

[20] M. Hay, G. Miklau, D. Jensen, D. Towsley, and P. Weis, "Resisting structural re-identification in anonymized social networks," *Proc. VLDB Endowment*, vol. 1, no. 1, pp. 102–114, 2008.

[21] L. Zou, L. Chen, and M. T. Özsu, "k-automorphism: A general framework for privacy preserving network publication," *Proc. VLDB Endowment*, vol. 2, no. 1, pp. 946–957, 2009.

[22] X.-Y. Li, C. Zhang, T. Jung, J. Qian, and L. Chen, "Graph-based privacy-preserving data publication," in *Proc. IEEE INFOCOM*, San Francisco, CA, USA, 2016, pp. 1–9.

[23] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, nos. 3–4, pp. 211–407, 2014.

[24] S. Perez. *Twitter Partners With IBM to Bring Social Data to the Enterprise*. Accessed: Sep. 13, 2017. [Online]. Available: https://techcrunch.com/2014/10/29/twitter-partners-with-ibm-to-bring-social-data-to-the-enterprise/

[25] *Stanford SNAP Datasets*. Accessed: Sep. 13, 2017. [Online]. Available: http://snap.stanford.edu/data/index.html

[26] *CMU Datasets*. Accessed: Sep. 13, 2017. [Online]. Available: http://www.casos.cs.cmu.edu/computational-tools/data2.php

[27] R. Bhaskar, A. Bhowmick, V. Goyal, S. Laxman, and A. Thakurta, "Noiseless database privacy," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security*, Seoul, South Korea, 2011, pp. 215–232.

[28] I. S. Tyurin, "A refinement of the remainder in the Lyapunov theorem," *Theory Probab. Appl.*, vol. 56, no. 4, pp. 693–696, 2012.

[29] A. Campan and T. M. Truta, "A clustering approach for data and structural anonymity in social networks," in *Proc. Privacy Security Trust KDD Workshop (PinKDD)*, 2008, pp. 33–54.

[30] C. Y. T. Ma, D. K. Y. Yau, N. K. Yip, and N. S. V. Rao, "Privacy vulnerability of published anonymous mobility traces," *IEEE/ACM Trans. Netw.*, vol. 21, no. 3, pp. 720–733, Jun. 2013.

[31] N. Ross *et al.*, "Fundamentals of Stein's method," *Probab. Surveys*, vol. 8, pp. 210–293, Sep. 2011.

Ping Zhao received the B.E. degree from the Tianjin University of Science and Technology, Tianjin, China, in 2013. She is currently pursuing the Ph.D. degree at the School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan, China.

Her current research interests include wireless networking, especially privacy protection in mobile networks.

Hongbo Jiang (M'08–SM'14) received the Ph.D. degree from Case Western Reserve University, Cleveland, OH, USA, in 2008.

He is currently a Full Professor with the College of Computer Science and Electronic Engineering, Hunan University, Changsha, China. He was a Professor with the Huazhong University of Science and Technology, Wuhan, China. His current research interests include computer networking, especially algorithms and protocols for wireless and mobile networks.

Dr. Jiang serves as an Editor for the IEEE/ACM TRANSACTIONS ON NETWORKING, an Associate Editor for the IEEE TRANSACTIONS ON MOBILE COMPUTING, and an Associate Technical Editor for *IEEE Communications Magazine*.

Chen Wang (S'10–M'13) received the B.S. and Ph.D. degrees from the Department of Automation, Wuhan University, Wuhan, China, in 2008 and 2013, respectively.

From 2013 to 2017, he was a Post-Doctoral Research Fellow with the Networked and Communication Systems Research Laboratory, Huazhong University of Science and Technology, Wuhan, China. Thereafter, he joined the faculty of Huazhong University of Science and Technology, where he is currently an Associate Professor. His current research interests include wireless networking, Internet of Things, and mobile computing, with a recent focus on privacy issues in wireless and mobile systems.

Haojun Huang received the B.S. degree from the School of Computer Science and Technology, Wuhan University of Technology, Wuhan, China, in 2005, and the Ph.D. degree from the School of Communication and Information Engineering, University of Electronic Science and Technology of China, Chengdu, China, in 2012.

He is currently a Professor with the Department of Network Engineering, College of Computer, China University of Geosciences, Beijing, China. He was a Post-Doctoral Researcher with the Research Institute of Information Technology, Tsinghua University, Beijing, from 2012 to 2015, and an Assistant Professor of communication engineering with the College of Electronic Information Engineering, Wuhan University, Wuhan, China, from 2015 to 2017. His current research interests include wireless communication, ad hoc networks, big data, and software-defined networking.

Gaoyang Liu received the B.S. degree in information engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2015, where he is currently pursuing the Ph.D. degree.

His current research interests include mobile sensing and data privacy protection.

Yang Yang received the B.E. and M.S. degrees from the Wuhan University of Technology, Wuhan, China, in 2009 and 2012, respectively, and the Ph.D. degree from the Huazhong University of Science and Technology, Wuhan, in 2017.

He is currently an Assistant Professor with the School of Computer Science and Information Engineering, Hubei University, Wuhan. His current research interests include wireless networks, mobile computing, and edge computing.