TRANSACTIONS ON DATA PRIVACY 12 (2019) 197–225

Bayesian-based Anonymization Framework against Background Knowledge Attack in Continuous Data Publishing

Fatemeh Amiri*, Nasser Yazdani, Azadeh Shakery**,***, Shen-Shyang Ho*****

* Department of Computer Engineering and Information Technology, Hamedan University of Technology, Hamedan, Iran.

** School of Electrical and Computer Engineering, College of Engineering, University of Tehran, Tehran, Iran.

*** School of Computer Science, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran.

**** Department of Computer Science, Rowan University, Glassboro, US.

E-mail: f.amiri@hut.ac.ir, yazdani@ut.ac.ir, shakery@ut.ac.ir, hos@rowan.edu

Received 11 October 2018; received in revised form 19 May 2019; accepted 29 October 2019

Abstract. In many real world situations, data are updated and released over time. In each release, the attributes are fixed but the number of records may vary, and the attribute values may be modified. Privacy can be compromised due to the disclosure of information when one combines different release versions of the data. Preventing information disclosure becomes more difficult when the adversary possesses two kinds of background knowledge: correlations among sensitive attribute values over time and compromised records. In this paper, we propose a Bayesian-based anonymization framework to protect against these kinds of background knowledge in a continuous data publishing setting. The proposed framework mimics the adversary's reasoning method in continuous release and estimates her posterior belief using a Bayesian approach. Moreover, we analyze threat deriving from the compromised records in the current release and the following ones. Experimental results on two datasets show that our proposed framework outperforms *JS*-reduce, the state of the art approach for continuous data publishing, in terms of the adversary's information gain as well as data utility and privacy loss.

Keywords. Anonymization, background knowledge attack, generalization, Bayesian estimator

1 Introduction

The growing demand for personal data and their public release have made individual privacy a major concern. Anonymization is one possible privacy preserving method to conceal associations between individuals and records in a microdata table. Privacy models such as k-anonymity [1], β-likeness [2], and differential privacy [1] [3] assume that only a single static

[1] Differential privacy has received considerable attention. Some works have also applied the model to republishing scenarios [39-43]

dataset is published. In many real world situations, data sources are dynamic and datasets could be updated and re-published. After multiple re-publishing of a dataset, a privacy breach may appear from one of the releases or due to the combination of information in these re-published datasets over time. There are several scenarios of data re-publishing [4-10], namely: multiple data publishing, sequential data publishing and continuous data publishing. The focus of this paper is on continuous data publishing in which released attributes are fixed while the number of records might vary due to insert/delete or update operations[2]. *JS*-reduce [8], m-invariance [5], and *HD*-composition [7] are the state of the art anonymization approaches in continuous data publishing.

Moreover, the presence of the adversary's additional knowledge increases the difficulty to preserve individual privacy [11-15,20,34]. Often researchers assume that I) whether the adversary's targets exist in a microdata table and II) Quasi Identifier[3] (QI) attribute values of their targets are available [1-3]. If an adversary has additional knowledge (usually called background knowledge), most privacy models in either single publishing [1,2] or re-publishing scenarios [4-7,9-10] cannot preserve individual privacy. In particular, correlations among attribute values serve as an important piece of adversary knowledge resulting in a privacy breach. For instance, data of disease progression, behavior analysis of individuals over time, or the investigation of the safety and effectiveness of a drug in slowing down the progression of some diseases might be published periodically. In these domains, the adversary can easily acquire background knowledge about correlations among attribute values. Our example in Section 4.1 shows that existing techniques are not effective when an adversary may obtain background knowledge on the correlation among sensitive attribute values in a continuous data publishing setting. The adversary may also have some specific knowledge, which is available to the adversary for some reason. For example, an adversary may know some targeted record respondent in person and have partial knowledge on the sensitive values of that individual. We call this type of adversary's knowledge as the *compromised record knowledge*.

In this paper, we present an anonymization framework for continuous data publishing when the adversary has background knowledge about correlations among attribute values and also exploits the compromised records to make more precise inferences. The proposed framework recreates the adversary's reasoning method to estimate her posterior beliefs about associations between individuals and sensitive values after observing each release. Moreover, the framework revises the adversary's beliefs based on a history of sensitive values in past releases. The main contribution of this paper is a Bayesian method to estimate the adversary's posterior beliefs. The Bayesian method allows an adversary to incorporate prior information (e.g. the compromised records) to reveal the individuals' sensitive attribute values.

To guard against background knowledge attack, we extend a privacy model based on k-anonymity and β-likeness to be used in a continuous release scenario. The privacy model ensures that the adversary's beliefs about associations within each QI group are similar as well as the k-anonymity and β-likeness are satisfied. Towards that end, we propose an anonymization algorithm to satisfy the privacy model as the microdata is re-published. The anonymization algorithm orders the records based on QI values and then selects at

[2]The insertion and deletion correspond to the situation in which a record appears in the microdata table for the first time or is removed from it and the updates correspond to either the modification in the attribute value or reinsertion of the record after a while.

[3]It should be noted that microdata is stored in a relational data model and each record are divided into identifiers, quasi-identifiers, and sensitive attributes[1-2]. Quasi identifiers are those attributes that individually are not an identifier, but when combined with each other, they become identifiers.

least *k* records that are close in the order and satisfy the privacy model.

JS-reduce[8] is close to ours in the sense that they considered the background knowledge on correlations among attribute values in a continuous release scenario . It does not consider threats deriving from the compromised records. *Cor*-split[16] studies threats deriving from compromised records in continuous data publishing. It does not support the correlations among sensitive attribute values as the adversary's background knowledge. They considered insert and delete operations, while no update operations occurred over time.

Experimental results on two datasets: Adult dataset [17] and Bkseq dataset [8] are used to verify the effectiveness of our anonymization framework. The performance of our anonymization framework is evaluated according to the framework parameters and background knowledge with different lengths of released history. Our empirical results show that the performance of our proposed algorithm is better than the state of the art anonymization algorithms such as *JS*-reduce in terms of gain of knowledge when the adversary possesses knowledge related to the compromised records and correlations among attribute values.

Our contributions are summarized as:

•We propose an anonymization framework for continuous releases, which takes into account the adversary's background knowledge. We analyze the threats deriving from the correlations among attribute values and the compromised records.

•The anonymization framework recreates the adversary's reasoning method in continuous publishing and estimates her posterior beliefs based on a Bayesian estimator.

•We extend a privacy model in single publishing to be used in continuous publishing. We propose an anonymization algorithm to satisfy the privacy model and conduct extensive experiments on different aspects of the algorithm, such as data utility, privacy and gain of knowledge.

The rest of the paper is organized as follows. We describe related work and preliminary in Sections 2 and 3. In Section 4, we formally define the problem including the privacy attack, the adversary's background knowledge and how she infers the actual associations between individuals and attribute values. Section 5 illustrates our proposed anonymization framework including a privacy model and an anonymization algorithm which experimentally evaluated in Section 6. In Section 7, we discuss more results and contributions. In Section 8, we conclude the paper and discuss some future work.

Open challenge: like other anonymization methods, our proposed method is based on a specific adversary model. An open research issue is how much the abilities of the adversary should be limited in the model, and how realistic these constraints are. Background knowledge can vary significantly among different adversaries. Our work significantly extends the state of the art by integrating correlational background knowledge and compromised record knowledge into the anonymization framework. However, we emphasize that, while our proposed framework provides a defense against the particular adversary model, it does not provide any formal guarantee of defense against arbitrary background knowledge attacks.

2 Related Work

To limit information disclosure, many privacy models have been proposed. k-anonymity and its refinements (e.g. β-likeness [2] and t-closeness [18]) are syntactic privacy models which partition records into groups, called QI-groups. Few works proposed a combination of privacy models to prevent identity and attribute disclosures [19, 20, 38]. The privacy models are implemented using different anonymization algorithms. These algorithms

can be categorized into generalization [21-24], microaggregation [19,25] and anatomization [26]. Generalization replaces real QI attribute values with less specific values while microaggregation creates small clusters from microdata and publishes the aggregate values of each cluster. Anatomization releases QI and sensitive attributes in two separate tables.

A dynamic dataset can be re-published in three extended scenarios: 1) *Multiple publishing*: In this scenario, different attributes of the same data are published for different purposes at the same time [4]. 2) *Sequential data publishing*: different sets of attributes are releases over time [9,10,36,38]. 3) *Continuous data publishing*: A data publisher has previously released $T_1, ..., T_{j-1}$ in times $t_1, ..., t_{j-1}$. Now she wants to publish the next release T_j where all $T_1, ..., T_j$ have the same schema. T_j is an updated release of T_{j-1} with insert/delete or update operations [5-8]. It should be noted that data re-publishing is different from multiple independent data publication where a data publisher does not know all data sets that can be used for a composition attack [37].

Several privacy preserving approaches have been proposed in continuous data publishing. Xiao and Tao [5] proposed m-invariance, where both insertions and deletions are allowed. m-invariance ensures that records are placed into QI-groups where patterns of sensitive attribute values are the same. Thus, adding counterfeit records is unavoidable and this no longer preserves data truthfulness at record level. This model does not support updating over time. Anjum *et al.*[6] proposed t-safety to support the update operations. Bu *et al.* [7] proposed *HD*-composition to limit the risk of information disclosure in re-published datasets. *HD*-composition protects records with permanent sensitive attribute values from disclosure. Wang *et al.* [27] developed a general method to derive an adversary's posterior belief in continuous data publishing. Their method may not scale well to scenarios where several microdata are published over time.

When an adversary has background knowledge, most privacy models fail to preserve individual privacy. Different types of adversary knowledge have been considered in the literature. Although several works have focused on background knowledge in a single publishing [11-15,20,34], it is not easy to adopt them for re-publishing in the presence of the adversary's background knowledge. Data correlation is an important type of adversary knowledge that makes privacy preservation difficult[13,15,20]. JS-reduce [8] is the framework in continuous data publishing which considers correlations between QI and sensitive attribute values. They proposed a Hilbert index-based anonymization algorithm to satisfy the privacy requirements. The algorithm sorts records based on the Hilbert index and chooses at least k-record clusters that are close to each other based on Hilbert index. All clusters satisfy t-closeness. Cor-Split [16] which satisfies an extension of m-invariance, overcomes threats derived from compromised records in continuous data publishing. It assumes that the values of attributes are fixed over time.

Differential privacy as a semantic privacy model received considerable attention. It provides a rigorous and quantifiable notion of privacy [3]. However, it is shown in [12,35] that the model may be ineffective if an adversary has background knowledge about data, in particular, when sensitive values are correlated. Some works show that it can be applied to republishing scenarios but introducing more noise than in single releases [39-43]. Our work focuses on syntactic privacy models like k-anonymity and β-likeness.

3 Bayes Estimation In Multinomial Distribution

In the Bayesian framework, the parameters of a statistical problem are treated as realization of random variables with known distribution rather than as unknown constants. The past

knowledge is represented as a prior distribution. In the Bayesian framework, Dirichlet distribution is conjugate prior of a multinomial distribution.

Definition 1. Let X=$(x_0, ..., x_q)$ follow the multinomial distribution M with parameters n and Θ, where Θ=$(\theta_0, ..., \theta_q)$. We define a Dirichlet prior distribution $D(a_0, ..., a_q)$ on Θ. If the loss function is squared error, *Bayes estimation* of Θ is the expectation of Dirichlet distribution $D(a_0 + x_0, ..., a_{q-1} + x_{q-1}, a_q + x_q)$ [28]. Therefore, the *Bayes estimator* of θ_i, $0 \leq i \leq q$, is

$$\bar{\theta_i} = E(\theta_i) = \frac{a_i + x_i}{\sum_{j=0}^{q} a_j + n} \tag{1}$$

4 Problem Definition

Let the original microdata table at time t_i be denoted by T_i=$\{r_1, r_2, ..., r_n\}$ and its anonymized version by T_i^*=$\{r_1^*, r_2^*, ..., r_n^*\}$. A history of t anonymized microdata tables is denoted by H_t^*= $<T_1^*, T_2^*, ..., T_t^*>$. Each record $r_j \in T_i$ corresponds to an individual v, called a record respondent. We assume that at most one record per person can appear in each table. Each r_j contains an identifier attribute (ID), d quasi-identifier attributes $A_1, A_2, ..., A_d$ and a single sensitive attribute S. Let $D[A_{i'}]$, $1 \leq i' \leq d$, denote attribute domain of $A_{i'}$ and $D[S]$=$\{s_0, s_1, ..., s_{m-1}\}$ denote the attribute domain of S.

The anonymization removes the identifier attribute and partitions records into some QI-groups. The QI values within each QI-group are generalized. An anonymization framework should specify an adversary model. An adversary is characterized by her knowledge and attack. It is assumed that: 1) The adversary knows the set of record respondents and their QI values. 2) The adversary observes a history of anonymized microdata tables over time. In each T_i^*, some new records may be inserted for the first time. Some records that already presented in the previous tables may be deleted in current table. Sensitive attribute values of some records in the previous tables may be updated and then these records are observed in the current table. 3) The adversary has background knowledge on correlations between QI and sensitive attribute values and also the correlations among sensitive attribute values over time. 4) The adversary knows the actual sensitive attribute values of some record respondents in each release. It is worth to note that most of the works proposed so far on continuous data publishing share the first two assumptions. The background knowledge considered in third and fourth assumptions, have been considered by related work but not in combination.

In the presence of background knowledge, the adversary runs an inference attack to reconstruct a record respondent's association with her actual sensitive attribute value. The details of the background knowledge attack are described in Section 4.1. The adversary's background knowledge and reasoning method are addressed in Sections 4.2 and 4.3, respectively. Table 1 summarizes the notations we use here.

4.1 Background Knowledge Attack

The following example shows a violation of individual privacy in the presence of an adversary's background knowledge in continuous data publishing.

Example 1. Suppose that a hospital collects original microdata tables T_1 and T_2 at time t_1 and t_2 (Tables 2 and 4) and releases their anonymized versions (Tables 3 and 5). Each microdata table contains a record for each patient. Each record includes an ID: *name*, three QIs: *sex*, *age*, and *zip code* as well as a sensitive attribute: *disease*. Both anonymized tables

H_t^*	a history of t anonymized microdata tables
T_i	original microdata table at time t_i
A_i	the i^{th} QI attribute
$D[A_i]$	domain of A_i
S	A sensitive attribute
$D[S]$	domain of S
m	the size of $D[S]$
d	the number of QI attributes
PD^{sv}	sensitive Background knowledge
PD_j^{cor}	j-step correlational Background knowledge
RPD_i^{sv}	Adversary's revised prior belief at time t_i
PB_i^{sv}	Adversary's posterior belief at time t_i

Table 1: Summary of notations used in paper

satisfy state of the art privacy models, e.g. 3-anonymity and 3-invariance. Assume that an adversary wants to predict Cayla's disease. She knows Cayla's QI values. Cayla is observed in both QI-groups 1 and 3. Without any additional information for Cayla, at time t_1, Cayla's sensitive value is Bronchitis, Alzheimer or Cancer-I with equal probability (i.e., $\frac{1}{3}$). At time t_2, the associations between Cayla and the diseases in QI-group 3 are equiprobable.

name	age	sex	zipcode	disease
Alice	65	F	12040	Bronchitis
Beth	66	F	12040	Alzheimer
Cayla	65	F	12040	Cancer-I
Dior	66	F	12041	Gastric ulcer
Elisa	66	F	12041	Flu
Fiona	67	F	12041	Diabetes-I

Table 2: Original microdata table T_1 at t_1

QI-group	age	sex	zipcode	disease
1	[65-66]	F	12040	Bronchitis
1	[65-66]	F	12040	Alzheimer
1	[65-66]	F	12040	Cancer-I
2	[66-67]	F	12041	Gastric ulcer
2	[66-67]	F	12041	Flu
2	[66-67]	F	12041	Diabetes-I

Table 3: Anonymized table T_1^* at t_1

name	age	sex	zipcode	disease
Cayla	65	F	12040	Cancer-II
Dior	66	F	12041	GERD
Elisa	66	F	12041	Depression
Fiona	65	F	12041	Diabetes-II
Ganya	66	F	12041	Flu
Harriet	67	F	12041	Alzheimer

Table 4: Original microdata table T_2 at t_2

QI-group	age	sex	zipcode	disease
3	[65-66]	F	1204*	Cancer-II
3	[65-66]	F	1204*	GERD
3	[65-66]	F	1204*	Depression
4	[65-67]	F	12041	Diabetes-II
4	[65-67]	F	12041	Flu
4	[65-67]	F	12041	Alzheimer

Table 5: Anonymized table T_2^* at t_2

In the presence of background knowledge, these associations are not equiprobable. Analogous to [8], the adversary is assumed to have two types of background knowledge: *sensitive background knowledge* (PD^{sv}) and *correlational background knowledge* (PD^{cor}) which are modeled as probability distributions over D[S]. PD^{sv} represents the prior probabilities associating sensitive attribute values to a record respondent, given the QI values. For example, one can have the probability that women with Alzheimer's disease are diagnosed at age 65 or older [29]. PD^{cor} represents the probabilities of modifying the sensitive attribute values in sequential times. For example, one can have the probability of prevalence of kidney failure in people with Diabetes [30]. The respondents in QI-groups 1 and 3 have similar QI values thus the adversary cannot exploit PD^{sv} to find the most likely sensitive attribute values of Cayla at t_1 or t_2. According to PD^{cor}, the assignment in which one got Cancer-I at t_1 and Cancer-II at t_2 is more probable than the other possible assignments. Therefore Cayla's privacy is violated at t_2. □

Given a QI group $Q \in T_i^*$ and the sensitive attribute value s observed in Q, a privacy viola-

tion occurs when probabilities of linking s to individuals whose records residing in Q, are not the same. These probabilities are defined as the adversary's posterior belief [13].

According to the adversary model, it is also assumed that an adversary may know some respondents in each release and have partial knowledge on their sensitive values. It is not an unreasonable assumption, since at least each respondent (a potential adversary) knows her own sensitive value. This knowledge affects the adversary's posterior beliefs and cascades over different releases. We call this type of adversary's knowledge as the *compromised record knowledge*.

4.2 Background Knowledge

It is assumed that an adversary has three types of background knowledge: sensitive background knowledge, correlational background knowledge and compromised record knowledge.

Definition 2. *Sensitive background knowledge* is a function PD^{sv}:$D[QI] \rightarrow \sum$, where $D[QI]$= $D[A_1]\times....\times D[A_d]$ is the set of all possible QI values and $\sum = \{(p_1, p_2, ..., p_m)\ |p_i \in \mathbb{R}, \sum_{i=1}^{m} p_i$ =1 , $0 \leq p_i \leq 1\}$ is the set of all possible probability distributions where m is the number of distinct sensitive attribute values.□

Thus, for a record respondent v with QI values $q \in D[QI]$, PD^{sv} is modeled as a probability distribution $(p_1, p_2, ..., p_m)$ over $D[S]$ such that p_i is the probability of v being associated with s_i, given q. Table 6 shows some probabilities in the adversary's sensitive background knowledge.

Age	Sex	zip	Disease	PD^{sv}
6*	F	1204*	Flu	0.12
6*	F	1204*	Gastric ulcer	0.05
6*	F	1204*	Bronchitis	0.05
6*	F	1204*	Alzheimer	0.1
6*	F	1204*	Liver infection	0.05
6*	F	1204*	Diabetes-I	0.13
6*	F	1204*	Diabetes-II	0.12
6*	F	1204*	GERD	0.1
6*	F	1204*	Depression	0.14
6*	F	1204*	Cancer-I	0.09
6*	F	1204*	Cancer-II	0.05

Table 6: Sensitive background knowledge (PD^{sv})

Disease at t_1	Disease at t_2	PD_1^{cor}
Flu	GERD	0.005
Flu	Depression	0.001
Flu	Cancer-II	0.0001
Gastric ulcer	GERD	0.3
Gastric ulcer	Depression	0.01
Gastric ulcer	Cancer-II	0.001
Cancer-I	GERD	0.002
Cancer-I	Depression	0.1
Cancer-I	Cancer-II	0.6
Bronchitis	GERD	0.002
Bronchitis	Depression	0.003
Bronchitis	Cancer-II	0.002
Alzheimer	GERD	0.002
Alzheimer	Depression	0.1
Alzheimer	Cancer-II	0.002
Diabetes-I	GERD	0.005
Diabetes-I	Depression	0.001
Diabetes-I	Cancer-II	0.0001

Table 7: 1-step correlational background knowledge (PD_1^{cor})

Definition 3. *d-step correlational background knowledge* is a function $PD_d^{cor} : V \times \bar{\Delta} \times \bar{t} \rightarrow \sum$ where V is a set of respondents. $\bar{\Delta}$ is a set of possible sequences of sensitive attribute values in the d last observations, such that d>0. $\bar{t}$ is a set of possible sequences of time instances at which the observations were taken. $\sum = \{(p_1, p_2, ..., p_m)|p_i \in \mathbb{R},\ \sum_{i=1}^{m} p_i = 1, 0 \leq p_i \leq 1\}$ is the set of possible probability distributions where m is the number of distinct sensitive attribute values. □

For example, if v is a respondent in the anonymized table T_3^* and the adversary knows that v has been assigned to s_1 and s_2 at t_1 and t_2, respectively. PD_2^{cor} at time t_3 returns

the probability p_i which associates v with s_i for each possible sensitive value $s_i \in D[S]$. We denote the probability p_i as $PD_2^{cor}(v,s_i,<s_1, s_2>)$. Table 7 shows a simple form of 1-step correlational background knowledge at t_2. For simplicity, we assume that the distributions do not depend on the record respondents.

Definition 4. *Compromised record knowledge* is a function CR: $V \times D[S] \times t \rightarrow$ [0-1] where V denotes the set of all respondents and $D[S]$ is the domain of the sensitive attribute. t is the set of possible time instances at which records of the respondents may be released. The codomain is the set of all real numbers from 0 to 1. □

$CR(v, s,t_i)$ returns the probability of the respondent v being linked to a sensitive attribute value s at time t_i and denotes the adversary's confidence about association between v and s at time t_i. Suppose that the adversary knows the actual sensitive attribute value, s_i, of v at time t_i. Because of this adversary-specific knowledge, the record corresponding to v is compromised at t_i and $CR(v, s_i,t_i)$=1.

4.3 Adversary's Reasoning Method In Continuous Data Publishing

In this section, we model an adversary's reasoning method in the presence of background knowledge as time goes on.

At time t_i, the adversary derives two new information, *revised prior belief* and *posterior belief*, which are denoted by RPD_i^{sv} and PB_i^{sv}, respectively. The revised prior belief is a revision of the sensitive background knowledge due to the observation of a history of released records. It is obtained by including the correlational knowledge into the posterior belief.

Figure 1 depicts the adversary's reasoning method. The problem of extracting PD^{sv} and PD_d^{cor} distributions have been studied and effective methods have been proposed (e.g. [8] and [13]). In data of disease progression, Riboni et.al.[8] extracted PD^{sv} and PD_d^{cor} from medical datasets of diseases and patients. For computing PD^{sv}, they partitioned people into different categories based on QI values. For each category, they assigned a probability to have a certain disease based on statistics they found in the data set/medical literature. PD_d^{cor} is computed using sequential pattern mining methods from a set of data about the evolution of diseases. Their algorithm essentially based on a frequency count of sequences appearing in the history. Hence, in the rest of this paper, it is assumed that the adversary gains PD^{sv} and PD_d^{cor} using the methods in [8].

When the first anonymized table, T_1^*, is released, the adversary calculates PB_1^{sv} based on T_1^* and PD^{sv}. Then she computes RPD_2^{sv} for the observed respondents. When T_2^* is released, she computes PB_2^{sv} based on T_2^* and RPD_2^{sv}. This process continues. When T_j^* includes a record r_i whose respondent, v, has not appeared in previous tables, the adversary does as follows: If v is observed for the first time, the adversary computes PB_j^{sv} using PD^{sv} and T_j^*, otherwise she uses the last computed $RPD_{t'}^{sv}, 1 \leq t' \leq j-1$ to compute PB_j^{sv}.

4.3.1 Computing The Posterior Belief

The *posterior belief* at t_i represents the adversary's confidence about the associations between respondents and sensitive values after publishing T_i^*.

Definition 5. *posterior belief* is a function PB^{sv}:$V \times t \rightarrow \sum$ where V is a set of respondents. t is a set of possible time instances at which records of the respondents may be released. $\sum$=$\{(p_1, p_2, ..., p_m) | p_i \in \mathbb{R}, \sum_{i=1}^{m} p_i = 1, 0 \leq p_i \leq 1\}$ is the set of possible probability distributions of $D[S]$. m is the number of distinct sensitive attribute values. □

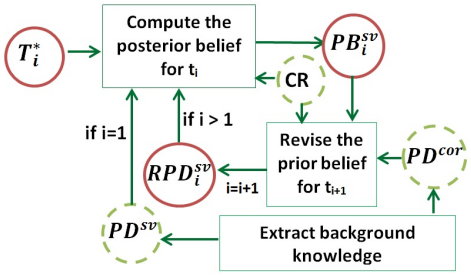

Figure 1: The adversary's reasoning method

We denote the posterior belief for the respondent v and the sensitive value s_i at time t_i as $PB^{sv}(v,s_i,t_i)$. To compute the posterior belief of the respondent v at t_i, the adversary considers a QI-group $Q \in T_i^*$ in which v's record is observed. Suppose that the set of sensitive values and respondents in Q are denoted by S_Q and V_Q, respectively. A *permutation* is a bijective function $pm : S_Q \rightarrow V_Q$. For example, the QI-group 3 in Table 5 contains Cayla's, Dior's and Elisa's records. Consequently, there are six different permutations between respondents and sensitive attribute values in this QI-group (Table 11).

Now, we describe how an adversary computes her posterior belief. Suppose that $PM=<pm_0, pm_1, ..., pm_q>$ contains the possible permutations defined between S_Q and V_Q where q is equal to $|Q|!$-1. A confidence degree, cd_j, is assigned to each possible permutation pm_j. cd_j is computed by the sum of RPD_i^{sv} (PD^{sv} at t_1) of one-to-one correspondences between the respondents and sensitive values in pm_j. Then, the adversary follows the 3-step procedure:

1) Define a vector $X=(X_0, ..., X_q)$ where each X_i, $0 \leq i \leq q$, is a random variable. Let all permutations in PM be considered as the outcomes of a trial. If X_i indicates the number of times that the outcome number i is observed over the trial, X follows a multinomial distribution $M = (1, \theta_0, ..., \theta_q)$ with q+1 outcomes. X takes a value $x=(x_0, ..., x_q)$ whose components are zero except the u^{th} component, x_u, which equals one. The u^{th} component is the permutation with maximum cd_u.

2) Estimate $E(\theta_i)$, $0 \leq i \leq q$, of the multinomial distribution M using Equation (1). The Dirichlet distribution is parameterized with $q+1$ parameters a_i which must be positive. They are equal, namely, $\forall a_i, a_j$: $a_i=a_j$, $0 \leq i, j \leq q$.

3) Given $v \in V_Q$ and $s_i \in S_Q$, $PB^{sv}(v, s_i, t_i)$ is calculated as the normalized sum of $E(\theta_i)$ of every possible permutation, pm_j, in which v is linked to s_i.

$$PB^{sv}(v, s_i, t_i) = \frac{\sum_{pm_j \in PM : pm_j(r)=v \wedge r(S)=s_i} E(\theta_i)}{\sum_{pm_j \in PM} E(\theta_i)} \quad (2)$$

where $pm_j(r)=v$ indicates that v is the respondent of the record r in pm_j. $r(S)$ shows the sensitive value of the record r.

Example 2. Consider the scenario in Example 1 and the QI-group 3 at time t_2. As mentioned in Example 1, the respondents in QI-group 1 have similar QI values, and the adversary cannot exploit PD^{sv} to find the most likely sensitive attribute values of the respondents at t_1. Therefore, after observing records released at t_1, the adversary infers that the probabilities of associations between respondents and sensitive attribute values in each released QI-group are equal (Table 8). To compute PB_2^{sv} at time t_2, the confidence degree of all possible permutations in QI-group 3 is computed. Each row of Table 11 reported a possible permutation, pm_i, and its confidence degree, cd_i. The confidence degree of

each permutation pm_i is the sum of RPD_2^{sv} of one-to-one correspondences between the respondents and sensitive values in pm_i. According to RPD_2^{sv} in Table 9, the confidence degree of pm_0 is 0.74+0.96+0.037= 1.73. According to pm_0, Cayla, Dior and Elisa are associated with Cancer-II, GERD and Depression, respectively. In this example, both of pm_0 and pm_1 are the permutations with highest cd_i. We randomly choose one of them. X takes $(1, 0, 0, 0, 0, 0)$. According to definition 1, $E(\theta_0)$=$\frac{1+1}{6+1}$=0.28, $E(\theta_i)$=$\frac{1}{7}$=0.14, 1$\leq i \leq$5 and $PB^{sv}(Cayla,Cancer-II,t_2)$=$\frac{E(\theta_0)+E(\theta_1)}{\sum_{0\leq i\leq 5} E(\theta_i)}$=0.42 (Table 10).

Name	Disease	PB^{sv}
Alice	Bronchitis	0.33
Alice	Alzheimer	0.33
Alice	Cancer-I	0.33
Beth	Bronchitis	0.33
Beth	Alzheimer	0.33
Beth	Cancer-I	0.33
Cayla	Bronchitis	0.33
Cayla	Alzheimer	0.33
Cayla	Cancer-I	0.33
Dior	Gastric ulcer	0.33
Dior	Flu	0.33
Dior	Diabetes-I	0.33
Elisa	Gastric ulcer	0.33
Elisa	Flu	0.33
Elisa	Diabetes-I	0.33
Fiona	Gastric ulcer	0.33
Fiona	Flu	0.33
Fiona	Diabetes-I	0.33

Table 8: Posterior belief at t_1 (PB_1^{sv})

	Cancer-II	GERD	Depression
Cayla	0.74	0.007	0.25
Dior	0.003	0.96	0.037
Elisa	0.003	0.96	0.037

Table 9: Revised prior belief at t_2 (RPD_2^{sv})

	Cancer-II	GERD	Depression
Cayla	0.42	0.28	0.28
Dior	0.28	0.42	0.28
Elisa	0.28	0.28	0.42

Table 10: Posterior belief at t_2 (PB_2^{sv})

	Cayla	Dior	Elisa	cd_i	X	$\bar{\theta}_i$
pm_0	Cancer-II	GERD	Depression	1.73	1	0.28
pm_1	Cancer-II	Depression	GERD	1.73	0	0.14
pm_2	GERD	Cancer-II	Depression	0.047	0	0.14
pm_3	GERD	Depression	Cancer-II	0.047	0	0.14
pm_4	Depression	Cancer-II	GERD	1.21	0	0.14
pm_5	Depression	GERD	Cancer-II	1.21	0	0.14

Table 11: Possible permutations at t_2

However, computing the exact posterior belief is intractable [13]. There are $|Q|!$ possible permutations in every QI-group, Q. Thus, an approximate algorithm can be used to compute the adversary's posterior beliefs for the large QI-groups. In our experimental evaluation, we compute posterior beliefs by the Ω-estimate method proposed by Li *et al.*[13] when a QI-group is large.

4.3.2 Computing The Revised Prior Belief

The revised prior belief is a function having the same domain and codomain as PB^{sv} defined in Definition 5. We compute the revised prior belief at time t_i (i $>$ 1) by the method proposed by Amiri et al. in [38]. Assume that a respondent v's record is released in T_i^*. For every $s_i \in D[S]$, $RPD^{sv}(v, s_i, t_i)$ can be computed as follows:

$$RPD^{sv}(v, s_i, t_i) = \sum_{\forall s_{i-d} \in D[S], ..., \forall s_{i-1} \in D[S]}$$

$$[PD_d^{cor}(v, s_i, < s_{i-d}, ..., s_{i-1} >)$$

$$\times Pr(v, (s_{i-d}, ..., s_{i-1}), (t_{i-d}, ..., t_{i-1}))] \quad (3)$$

where PD_d^{cor} is d-step correlational background knowledge and $Pr(v, (s_{i-d}, ..., s_{i-1}), (t_{i-d}, ..., t_{i-1}))$ is the joint probability of associating v with s_j at time t_j where $i - d \leq j \leq i - 1$. The joint probability is calculated as follows:

$$Pr(v, (s_{i-d}, ..., s_{i-1}), (t_{i-d}, ..., t_{i-1}))$$

$$= PB^{sv}(v, s_{i-d}, t_{i-d}) \times PD_1^{cor}(v, s_{i-d+1}, < s_{i-d} >)$$

$$\times PD_2^{cor}(v, s_{i-d+2}, < s_{i-d}, s_{i-d+1} >)$$

$$\times ... \times PD_{d-1}^{cor}(v, s_{i-1}, < s_{i-d}, ..., s_{i-2} >) \quad (4)$$

where $PB^{sv}(v, s_{i-d}, t_{i-d})$ is the posterior belief of assigning v to s_{i-d} at t_{i-d}. $PD_{d'}^{cor}$ distributions are d'-step correlational background knowledge with $1 \leq d' \leq d$-1. We approximate all $PD_{d'}^{cor}$ distributions using 1-step correlational background knowledge (PD_1^{cor}). In the following example, RPD^{sv} is computed for Cayla and Cancer-II in Table 5.

Example 3. Consider the scenario in Example 1. The probability $PB^{sv}(Cayla, s_1, t_1)$ that Cayla is the respondent of a record released at t_1 having sensitive value s_1 is given in Table 8. We use the 1-step correlational background knowledge given in Table 7. Therefore, $RPD^{sv}(Cayla, Cancer - II, t_2)$ is computed as follows:

$$RPD^{sv}(Cayla, Cancer - II, t_2) = \sum_{\forall s_1 \in D[S]}$$

$$[PB^{sv}(Cayla, s_1, t_1) \times PD_1^{cor}(Cayla, Cancer - II, < s_1 >)]$$

$$= [PB^{sv}(Cayla, Bronchitis, t_1) \times PD_1^{cor}(Cayla, Cancer - II, < Bronchitis >)]$$

$$+[PB^{sv}(Cayla, Alzheimer, t_1) \times PD_1^{cor}(Cayla, Cancer - II, < Alzheimer >)]$$

$$+[PB^{sv}(Cayla, Cancer - I, t_1) \times PD_1^{cor}(Cayla, Cancer - II, < Cancer - I >)]$$

$$= 0.199$$

According to Table 3, the posterior beliefs of associating Cayla with any possible sensitive attribute values other than Bronchitis, Alzheimer and Cancer-I are zero at t_1. Thus they are not considered for computing $RPD^{sv}(Cayla, Cancer - II, t_2)$. Table 9 shows the normalized RPD^{sv} distributions at time t_2.

4.4 Cascading Of Threats Deriving From Compromised Records In Continuous Publishing

When the record corresponding to the respondent v is compromised at time t_i, the adversary assigns v to a sensitive attribute value with high confidence and uses this knowledge to make inference about other respondents observed in the released tables. In this work, the compromised record knowledge is modeled as CR function.

According to Definition 4, $CR(v, s_i, t_i)$ are in the range of [0-1]. When $CR(v, s_i, t_i)$ is equal to 1 for some sensitive attribute value s_i, the adversary knows precisely v's sensitive attribute value. To infer the sensitive value of other record respondents, she removes v's record and s_i and then calculates the posterior beliefs for the rest. Otherwise, when $0 \leq CR(v, s_i, t_i) < 1$, we propose two methods to cascade this knowledge in continuous publishing: *prior-based cascading method* and *posterior-based cascading method*. In the former, the adversary exploits the $CR(v, s_i, t_i)$ probabilities to compute the revised prior belief. In the latter, the compromised record knowledge influences the PB^{sv} distributions at time t_i.

4.4.1 Prior-Based Cascading Method

In this method, the adversary computes the revised prior beliefs at t_i regarding the compromised record knowledge at t_i. Then she calculates the posterior beliefs at t_i using the 3-step procedure defined in Section 4.3.1.

Given the $CR(v, s_i, t_i)$ probability, the revised prior belief regarding the compromised record knowledge is denoted by CR_RPD^{sv} and computed using the law of total probability. To compute CR_RPD^{sv}, we define an event, E_{v,s_i,t_i}. The event is that v's record is compromised at t_i. The complement of E_{v,s_i,t_i} is denoted by $\bar{E}_{v,s_i,t_i}$.

$$CR\_RPD^{sv}(v, s_i, t_i) =$$

$$Pr(E_{v,s_i,t_i}) \times CR\_RPD^{sv}(v, s_i, t_i | E_{v,s_i,t_i})$$
$$+Pr(\bar{E}_{v,s_i,t_i}) \times CR\_RPD^{sv}(v, s_i, t_i | \bar{E}_{v,s_i,t_i}) \quad (5)$$

where $Pr(E_{v,s_i,t_i})$ is the probability of E_{v,s_i,t_i} occuring. The revised prior beliefs of the association between v and s_i, conditioned on E_{v,s_i,t_i} and its complement are denoted by $CR\_RPD^{sv}(v,s_i,t_i|E_{v,s_i,t_i})$ and $CR\_RPD^{sv}(v,s_i,t_i|\bar{E}_{v,s_i,t_i})$, respectively. $Pr(E_{v,s_i,t_i})$ is set to $CR(v, s_i, t_i)$ and CR_RPD^{sv} $(v,s_i,t_i|E_{v,s_i,t_i})$ is equal to 1. $Pr(\bar{E}_{v,s_i,t_i})$ is set to 1-$CR(v, s_i, t_i)$. $CR\_RPD^{sv}(v, s_i, t_i|\bar{E}_{v,s_i,t_i})$ is equal to RPD^{sv} (v, s_i, t_i) and is computed by Equation (3).

4.4.2 Posterior-Based Cascading Method

In this method, the revised prior beliefs at t_i are computed using Equation (3). To compute the posterior belief at t_i, the adversary follows the 3-step procedure defined in Section 4.3.1. She uses the $CR(v, s_i, t_i)$ probabilities to initialize the parameters $a_0, ..., a_q$ of Dirichlet distributions in the procedure. To initialize the parameters, we define the notion of $matching$ between record respondents and permutations.

Definition 6. Suppose that Q is a QI-group in which v's record is released at time t_i. V_Q is the set of respondents whose records are observed in Q. PM is the set of possible permutations in Q such that $|PM|=q+1$. For each permutation $pm_l \in PM$ and $CR(v, s_i, t_i) > RPD^{sv}(v, s_i, t_i)$, if $v \in V_Q$ is associated with s_i in pm_l, pm_l is a $matching$ of v. □

Given the $CR(v, s_i, t_i)$ probability, the adversary checks whether pm_l is a matching of v. In this case, the value of a_l must be high. Each permutation may be the matching of some respondents in V_Q. Therefore, the parameter a_l is set proportional to the sum of $CR(v', s', t_i)$ probabilities which pm_l is the matching of $v' \in V_Q$.

If $CR(v, s_i, t_i) = RPD^{sv}(v, s_i, t_i)$, there will be no additional knowledge. Thus the compromised record knowledge about v and s_i is dropped. When $CR(v, s_i, t_i) < RPD^{sv}(v, s_i, t_i)$, new knowledge could be extracted as $CR(v, s_z, t_i)$, $\forall s_z \in S_Q$, $s_z \neq s_i$ where S_Q includes all sensitive attribute values in Q and $\sum_{\forall s \in S_Q} CR(v, s, t_i) = 1$. Then the adversary ignores $CR(v, s_i, t_i)$. This situation is described in the following example.

Example 4. Suppose that the adversary knows $CR(Dior, GERD, t_2)$=0.97, $CR(Elisa, Cancer-II, t_2)$=0.02, and $CR(Elisa, GERD, t_2)$=0.03. The adversary extracts $CR(Elisa, Depression, t_2)$ =1-(0.02+0.03)=0.95. According to the compromised record knowledge at t_2, the adversary has additional knowledge about Elisa and Dior. Consider all permutations of QI-group 3 in Table 11. pm_0 and pm_5 are the matching of Dior. pm_0 and pm_2 are the matching of Elisa. According to the posterior-based cascading method, If the adversary sets $a_1 = a_3 = a_4 = 1$, she increases the values of other parameters proportional to sum of $CR(v, s_i, t_i)$ probabilities such that $a_2 = a_1 + CR(Elisa, Depression, t_2) = 1.95$, $a_5 = a_1 + CR(Dior, GERD, t_2) = 1.97$ and $a_0 = a_1 + CR(Elisa, Depression, t_2) + CR(Dior, GERD, t_2) = 2.92$. According to the X value in Example 2, $E(\theta_0) = \frac{2.92 + 1}{9.84 + 1} = 0.36$, $E(\theta_2) = 0.17$, $E(\theta_5) = 0.18$, $E(\theta_i) = 0.09$, $i = 1, 3, 4$. Then posterior beliefs are calculated using the procedure defined in Section 4.3.1.

5 Anonymization Framework

In this section, we elaborate our anonymization framework against the background knowledge attack in continuous data publishing. Section 5.1 describes the defense strategy for limiting the adversary's capability of identifying the actual respondent of a record. Section 5.2 describes the anonymization algorithm.

5.1 Defense Strategy Against The Background Knowledge Attack

To anonymize a table, it is necessary to maximize uncertainty of mapping between respondents and sensitive attribute values in each QI-group. When the adversary's posterior beliefs of records within a QI-group are similar, the adversary cannot discriminate any of possible permutations with a high degree of certainty. Therefore, we try to create QI-groups whose record respondents have similar posterior beliefs. It should be noted that the posterior beliefs at time t_i are computed after generating QI-groups, then we use the revised prior beliefs at time t_i to group the records before releasing them. We apply the restriction that the differences in the RPD_i^{sv} distributions of records in a QI-group do not exceed a given threshold J. We use Jensen Shannon divergence (JSD) [31] to measure difference among RPD_i^{sv} distributions within each QI-group. This measure is symmetric and always results in a definite number [4]. Suppose that $\bar{\rho} = \{\bar{\rho}^1, ..., \bar{\rho}^u\}$ is a set of probability distributions and $w^1, ..., w^u$ denote the weights of the probability distributions such that $\Sigma_{i=1}^u w^i = 1$. Then JSD among distributions in $\bar{\rho}$ is:

$$JSD(\bar{\rho}) = H(\Sigma_{i=1}^u w^i \times \bar{\rho}^i) - \Sigma_{i=1}^u w^i \times H(\bar{\rho}^i) \quad (6)$$

[4] Although applying Kolmogorov-Smirnov distance (KS) is more effective compared to Entropy-based JSD to measure difference between the beliefs and to achieve stronger privacy guarantee, it suffers the curse of dimensionally. Hence, JS is practical and useful for data publishing.

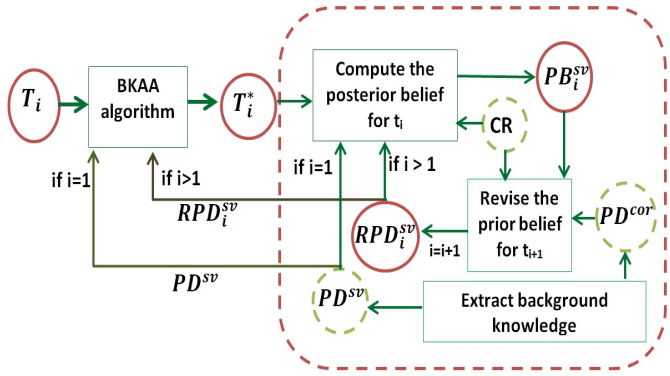

Figure 2: Our anonymization strategy against the background knowledge attack

where $H(\bar{\rho}^i)$ is Shannon entropy of $\bar{\rho}^i$. For simplicity, we assume the same value for all w^i. Since the goal having similar RPD_i^{sv} distributions in each QI group, does not consider QI and sensitive attribute values and cannot protect against identity and attribute disclosure risks, our proposed framework also satisfies k-anonymity and β-likeness to protect against them. It should be noted that this framework can be easily extended to enforce other state of the art privacy models like t-closeness [18] to prevent identity and attribute disclosures. Analogous to [20], we define the J-similarity privacy model to defend against the background knowledge attack in continuous publishing as follows:

Definition 7. Given a microdata table T_i, the anonymized QI-group Q satisfies J-similarity if :

• JSD of the RPD_i^{sv} distributions of record respondents in Q is up to J; and

• Q satisfies k-anonymity: there exist at least k records in Q; and

• Q achieves β-likeness: relative differences of probabilities of sensitive attribute values within Q from those in T_i is up to β.

An anonymized microdata T_i^* satisfies J-similarity If and only if all QI-groups in T_i^* satisfy J-similarity. □

To guard against the background knowledge attack, our anonymization framework needs to recreate what an attacker would do. Therefore, it follows the adversary's belief revision cycle presented in Section 4.3. To be effective against the attack at time t_i, $i > 1$ (i=1), our framework needs to calculate the $RPD_i^{sv}(PD^{sv})$ distribution of respondents before anonymizing data. Analogous to adversary's reasoning method, our anonymization framework (illustrated in Figure 2) computes posterior beliefs and revises prior beliefs. PD^{sv} and PD^{cor} are obtained using one of the methods illustrated in Section 4.3.

At first, for each respondent of records in all tables, RPD_1^{sv} at t_1 is initialized according to PD^{sv}. Then each table T_i is generalized by the Background Knowledge-based Anonymization Algorithm, BKAA, in order to enforce J-similarity. We call T_i^* the generalization of T_i. For each respondent observed in T_i^*, our framework calculates the posterior belief at t_i and the revised prior belief at t_{i+1}. Finally the generalized table T_i^* is published.

If a data publisher knows who are compromised in T_i before releasing its anonymized version (denoted as CR in Figure 2), she applies the prior-based cascading method to compute CR_RPD^{sv} distributions instead of RPD_i^{sv} distributions and then anonymizes T_i according to CR_RPD^{sv} distributions. Otherwise, if the compromised record knowledge corresponding to T_i is available after releasing its anonymized version, she applies the posterior-based cascading method to calculate PB_i^{sv} at t_i.

5.2 Anonymization Algorithm

In this section, we describe our proposed Background Knowledge-based Anonymization Algorithm, BKAA, to satisfy J-similarity. BKAA is motivated by the hierarchical anonymization algorithm in [20]. BKAA orders the records in T_i in terms of QI values. Then it selects at least k records which are close to each other and satisfy J-similarity.

Pseudo-code of BKAA is shown in Algorithm 1. As input, the algorithm takes the original table T_i at time t_i, PD^{sv} and RPD_i^{sv} distributions and the thresholds J, k and β. The output of algorithm is a set of QI-groups, $\tilde{\text{Q}}$, satisfying J-similarity. To anonymize the first table T_1, the algorithm applies the PD^{sv} distributions instead of the RPD_i^{sv} ones. In Line 1 of Algorithm 1, $\tilde{\text{Q}}$ is initialized as an empty set. BKAA creates a sorted list, π, of all records in T_i such that two records that are close in terms of QI values, are also close in the list (Line 2 in Algorithm 1). There are several ways to construct the list. BKAA employs the nearest point next (NPN) to create the list [32]. The list is constructed as follows:

1) Compute the centroid $\bar{\text{r}}$ of all records in T_i.

2) Compute the most distant record, r, from $\bar{\text{r}}$. r is added to π. The most distant record can be found by Euclidean distance of QI values.

3) The second record is the closest one to the first (among the remaining records). The third record is the closest one to the second (among the remaining records) and so on until all $|T_i|$ records have been added to π.

BKAA takes the first k records in π as a set of records, Q (Lines 5 to 13 in Algorithm 1) and checks whether records in Q satisfies J-similarity. When J-similarity is satisfied, the *CreateQI*() function creates a new QI-group, q, using the records in Q. It means that QI values are substituted by the generalized values i.e. the interval for numerical data and the closest common generalization for categorical data (Line 9 in Algorithm 1). q is added to the set $\tilde{\text{Q}}$. Then Q is initialized to generate next QI-group (Line 11 in Algorithm 1). The same procedure is repeated with the remaining records. Otherwise, if Q does not satisfy J-similarity, the next record in π will be added into Q until the privacy model is satisfied.

Algorithm 1: BKAA anonymization algorithm

Input:
$T_i = \{r_1, r_2, ..., r_n\}$: the original microdata at time t_i , PD^{sv}: adversary's sensitive background knowledge, RPD_i^{sv}: adversary's revised prior beliefs, *k*: k-anonymity level, β: β-likeness level, J: JSD level
Output: A set of QI groups, $\tilde{\text{Q}}$, satisfying privacy model

1 $\tilde{\text{Q}} \leftarrow \emptyset$
2 $\pi \leftarrow$ create an order of all $|T_i|$ records
3 Q$\leftarrow\emptyset$
4 *// loop to create a QI-group satisfying J-similarity. A created QI-group is added to $\tilde{\text{Q}}$*
5 **for** $\tilde{\text{r}}\leftarrow \pi_1$ to $\pi_{|T_i|}$ **do**
6 $Q\leftarrow$ Q $\cup \{\tilde{\text{r}}\}$
7 **if** ($|Q|\geq k$ and Q satisfies J-similarity)
8 *// the QI values of records in Q are generalized*
9 $q \leftarrow CreateQI$(Q)
10 $\tilde{\text{Q}} \leftarrow \tilde{\text{Q}} \cup q$
11 Q $\leftarrow \emptyset$

```
12  end if
13 end for
14 // If the set of records in Q does not satisfy the privacy model, the records are inserted into the
15 existing QI groups
16 if(Q ≠ ∅) then
17  for r ∈ Q do
18   if(∃ q ∈ Q̃ such that q ∪ {r} satisfies J-similarity ) then
19    Q̃ ← (Q̃ ∪ {q ∪ {r} }) \ q
20   else
21    remove record r
22   end if
23  end for
24 end if
25 end function
```

All records in list π would be examined before Q satisfies the privacy model (Lines 16 to 24 in Algorithm 1). In this case, BKAA tries to insert each record $r \in Q$ into one of the existing QI-groups, q, such that the new QI-group $\{q \cup \{r\}\}$ still satisfies the privacy model. However, like other privacy-preserving techniques, it is possible that some records cannot be arranged in any QI-group without violating some of the privacy requirements. In this case, BKAA removes those records outside QI-groups. Experimental results, reported in Section 6.3.4, show that the percentage of removed records is small. However, if an adversary knows the whole set of record respondents of each table (according to assumptions in Section 4), BKAA may be prone to attacks in which the adversary recognizes that some records have been removed, and infers the cause of elimination. In order to defend against this additional knowledge assumption, BKAA may be easily modified to adopt other solutions: 1) executing the algorithm using less stringent values for privacy parameters (k, β, and J); 2) counterfeiting the sensitive values of those records outside QI-groups, so that they can be inserted in existing QI-groups without violating the privacy model.

6 Experimental Results

In this section, we report the evaluation results of the anonymization framework in continuous publishing using two datasets and with different evaluation measures. In Section 6.1, we describe the configuration and datasets, then we define evaluation measures in Section 6.2. In Section 6.3, we present results on our anonymization framework.

6.1 Configuration And Evaluation Data

To the best of our knowledge, there is just one dataset[5] in continuous data publishing called Bkseq dataset [8], which considers the correlation of sensitive values over time. Bkseq is a synthetic dataset based on the domain knowledge from the medical literature and the considered background knowledge is available. This dataset contains 24 microdata tables

[5]Most of the dataset used to evaluate the anonymization framework in continuous data publishing is created from static sets of records in which each record randomly assigned to a release. Obviously, this procedure does not consider the correlation between the sensitive attribute values over time, which is one of the main points of this work.

of patient records and each microdata table contains approximately 4000 records. Each record contains 3 QI attributes: sex, age, $weight$ and a sensitive attribute *result of the exam*.

We also create a synthetic dataset using the static set of records in the Adult dataset to evaluate our anonymization framework in continuous data publishing. More details about this commonly used dataset can be found in [17]. We use four attributes: age, $gender$, $education$ as QI attributes and $occupation$ as a sensitive attribute. To make a continuous data publishing scenario, we initially take 4000 records as the first release, T_1. Then for each subsequent release T_i, we randomly delete 400 (10%) records from T_{i-1} and insert 400 new records from Adult. We also take 400 records from T_{i-1} to update their sensitive attribute values. We allow the updates in *occupation* to any other values in its domain, i.e., *occupation* of a person can remain the same or be modified. We assume the uniform distribution as the correlational background knowledge in experiments on the Adult dataset. The sensitive background knowledge is extracted by the same method proposed in [8].

All the experiments were conducted on a PC with 2.50 GHz Intel Core i7 CPU and 8.0G RAM. There are some parameters in this framework: the privacy parameters J, k and β and the attack parameters containing the probability of a record to be compromised, σ, and the probability of associating the respondent v_i with her actual sensitive value s_i at time t_i, denoted by $CR(v_i, s_i, t_i)$. The value of privacy parameters J, k and β must be selected according to domain-specific policy. In order to directly compare other works with ours, the J values are taken in the range 0.2-0.8 and the k values are taken in the range 2-8, whereas the β values are taken in the range 3-10. These parameter values cover most usual J, k and β values in [2] and [8]. The probability of a record to be compromised is small in many real world situations. Thus, we try small values of σ (from 0.01 to 0.1). To investigate the cascading effect of compromised record over different lengths of the release history, the $CR(v_i, s_i, t_i)$ values are taken sufficiently high (in the range of 0.5-0.9). The range of the parameter values is shown in Table 12.

	k	J	β	σ	$CR(v_i, s_i, t_i)$
value of parameters	[2-8]	[0.2-0.8]	[3-10]	[0.01-0.1]	[0.5-0.9]

Table 12: The value of parameters

6.2 Evaluation Measures For Utility And Privacy

To evaluate data utility and privacy of respondents, we measure information loss and privacy loss in each release. The information loss is measured using the global certainty penalty (GCP)[33]. The privacy loss is measured using the record linkage (RL)[19] and the gain of knowledge [38].

GCP[33] of a release T_i is defined by the sum of normalized certainty penalty (NCP) on all records in the microdata. Assume that T_i consists of the QI attributes A_1,...,A_D where all attributes are numeric. NCP of a record $r \in T_i$ is defined as the weighted sum of NCP on all QI attributes, $NCP(r)=\sum_{j=1}^{D}(w_j \times NCP_{A_j}(r))$. Assume that the record r=(x_1,...,x_d) is generalized to r^*=$[(y_1 - z_1), ..., (y_d - z_d)]$. NCP on the attribute A_j is given by $NCP_{A_j}(r)=\frac{z_j - y_j}{[A_j]}$ where $[A_j]$ is the range of all records on the attribute A_j in T_i. This measure will be maximized where a QI group contains all records, i.e. the total information loss.

RL[19] is defined by the amount of correct linkages between the anonymized and original tables. RL is computed as the sum of the record linkage probability, P_{RL}, of anonymized records. Suppose that the record $r \in T_i$ is anonymized to r^*.

$$RL = \sum_{r \in T_i} P_{RL}(r^*)$$

$$P_{RL}(r^*) = \begin{cases} \frac{1}{|Q|} & : r^* \in Q \\ 0 & : otherwise \end{cases} \quad (7)$$

where Q is the nearest QI-group to r. When $r^* \in Q$, the record linkage probability is calculated as $\frac{1}{|Q|}$. The lower is the record linkage; the more effective is the anonymization.

The gain of knowledge [38] in each release T_i is defined by the average of gain of knowledge on all record respondents in T_i. The measure evaluates the impact of background knowledge on an adversary's posterior belief. It measures the information obtained using background knowledge with respect to an attack based only on the observation of the frequency of sensitive values in a QI group. The gain of knowledge of each respondent v_j is defined as follows:

$$G(v_j) = \begin{cases} \frac{|PB^{sv}(v_j, s_j, t_i) - \frac{m(s_j)}{|Q|}|}{1 - \frac{m(s_j)}{|Q|}} & : \text{if } \frac{m(s_j)}{|Q|} \neq 1, \\ |1 - PB^{sv}(v_j, s_j, t_i)| & : otherwise. \end{cases} \quad (8)$$

where $PB^{sv}(v_j, s_j, t_i)$ is the posterior belief of assigning v_j to her actual sensitive attribute value, s_j, at time t_i. Q is a QI-group in T_i^* including v_j's record and $|Q|$ is the number of records within Q. $m(s_j)$ is the number of records which have the same sensitive attribute value as v_j in Q. $\frac{m(s_j)}{|Q|}$ denotes the adversary's posterior belief without any background knowledge, while $PB^{sv}(v, s_j, t_i)$ denotes the same belief in the presence of background knowledge.

6.3 Effectiveness Of Our Proposed Framework

We evaluate our proposed anonymization framework in two aspects: R-U confidentiality map and gain of knowledge. R-U confidentiality map is a graphical representation of pairs of RL and GCP. We apply the Bayesian estimator and the BKAA algorithm in the proposed framework, denoted by *BayFrame*. It should be noted that *BayFrame* does not apply any cascading method. To analyze the effect of compromised records, we denote the proposed framework applying prior-based and posterior-based cascading methods as *BayFrame+Prior* and *BayFrame+Posterior*, respectively. Moreover, we investigate the effect of correlational background knowledge with different steps. 1-step and 2-step PD^{cor} distributions are denoted as FDTMM and SDTMM, respectively. We also study the impact of different parameters k, β, J, σ and $CR()$ on the performance of proposed framework.

6.3.1 Performance Of Posterior Estimator

In these experiments, we evaluate the performance of proposed posterior estimator and compare it with the estimator proposed in the closest work, *JS*-reduce [8]. *JS*-reduce produces QI groups in which k-anonymity and t-closeness are satisfied as well as the difference of revised prior beliefs of records in each QI-groups is up to J. It applies the Hilbert index transform to sorts records in T_i. *JS*-reduce enumerates all possible assignments between

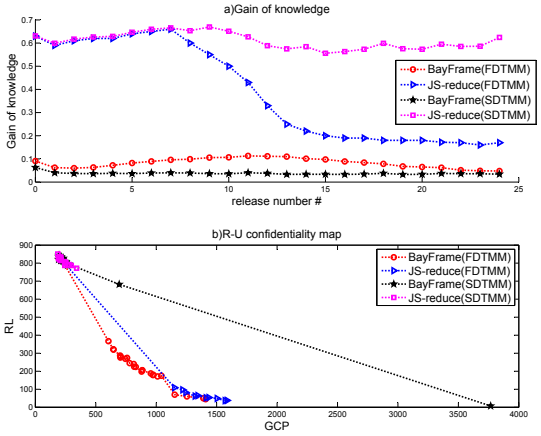

Figure 3: Comparison between the posterior beliefs of JS-reduce with that in our framework

all respondents and sensitive attribute values in a QI-group and then, normalizes the confidence degree of all permutations to compute adversary's posterior beliefs in each release. Our method considers all possible assignments as the outcomes of a trial in a Multinomial distribution and uses Bayes estimation of parameters in the Multinomial distribution.

In order to fairly compare, our framework is changed to have the same privacy model as in *JS*-reduce. Our framework also applies the anonymization method proposed in *JS*-reduce instead of BKAA. As a result, the only difference between *JS*-reduce and ours in this experiment is how to compute the posterior beliefs. Figure 3 shows comparison results on Bkseq dataset [8]. In this experiment, We do not consider any compromised record knowledge. The parameter values are set as follows: t=0.5, k=3 and J=0.6 which resulted in the best performance of *JS*-reduce on the Bkseq dataset.

Figure 3a shows the performance curve of gain of knowledge over different releases when they are anonymized using *BayFrame* and *JS*-reduce using 1-step and 2-step correlational background knowledge. It can be observed that gain of knowledge generated by *BayFrame* is lower than that by *JS*-reduce. The gain of knowledge generated by *JS*-reduce(SDTMM) is equal or higher than that by *JS*-reduce(FDTMM). *JS*-reduce(SDTMM) means that *JS*-reduce uses the 2-step correlational background knowledge to compute the adversary's posterior beliefs. We conclude that JS-reduce is not effective when the adversary exploits 2-step correlational background knowledge.

Figure 3b shows the performance curves of R-U confidentiality map. As expected, RL decreases as GCP increases. In each level of RL, *BayFrame*(FDTMM) results in lower or equal GCP compared to *JS*-reduce(FDTMM). Moreover, *JS*-reduce(SDTMM) results in narrow ranges of the RL and GCP values compared to *BayFrame*(SDTMM). The GCP and RL values of *JS*-reduce(SDTMM) are in the ranges 200-450 and 750-850, respectively while the GCP and RL values of *Bayframe*(SDTMM) are in the ranges 200-3850 and 50-850, respectively. As evident from Figure 3, the Bayesian posterior estimator used by *BayFrame* outperforms the posterior estimator used by *JS*-reduce in terms of gain of knowledge and R-U confidentiality map.

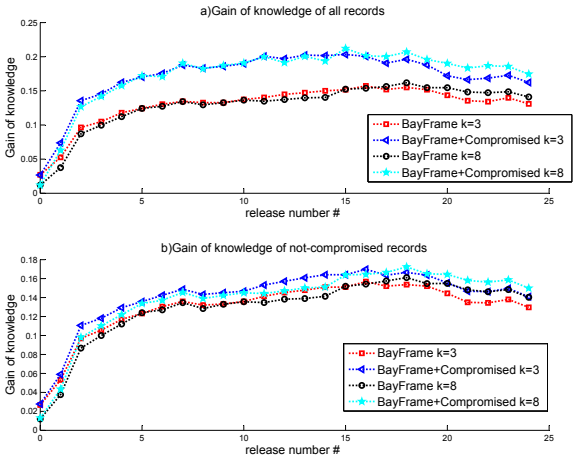

Figure 4: Impact of compromised records on the gain of knowledge for different value of k (σ=0.1). *BayFrame* applies PD_1^{cor}.

6.3.2 Impact Of Compromised Records On The Performance Of The Proposed Framework

In these experiments, we study the impact of compromised records when the proposed framework satisfies *J*-similarity. We first measure the adversary's gain of knowledge when she observes a history of releases in the Bkseq dataset. Figure 4 plots the impact of compromised records in outputs of *BayFrame* when PD_1^{cor} is applied. The curve labeled *BayFrame* corresponds to the performance of our framework not considering compromised records. The curve labeled *BayFrame+Compromised* simulates the adversary's inference ability when she exploits compromised records(σ=0.1 in each release). The figure depicts the adversary's gain of knowledge over various releases under two different values of k, (k=3 and k=8). β, J and $CR(v_i, s_i, t_i)$ are set to 5, 0.6, and 0.9, respectively.

Figure 4a shows the gain of knowledge generated by the records of each release. The results show that the adversary's gain increases in the presence of the compromised record knowledge and the gain of knowledge produced by *BayFrame+compromised* is higher than *BayFrame*. Moreover, during the first 5 releases,the resulting performance curves for k=8 are lower than those for k=3. The opposite result is obtained after the 16^{th} release. This is because the size of QI-groups for k=8 is greater than that for k=3, thus the rate of changes in the gain of knowledge for k=8 is slower than that for k=3.

Next, we study the impact of compromised record on non-compromised records in each release. Figure 4b shows the gain of knowledge generated by non-compromised records in each release. The experimental results shown in Figure 4b, confirm the previous finding. We see that, when a small percentage of records is compromised, the gain of knowledge generated by non-compromised records increases. Furthermore, it can be seen that the difference between *BayFrame* and *BayFrame+compromised* in Figure 4a is more than that in Figure 4b. The reason is that Figure 4a shows the difference among the adversary's gains generated by all records in a table (both the compromised and non-compromised records) while the difference observed in Figure 4b is generated by non-compromised records.

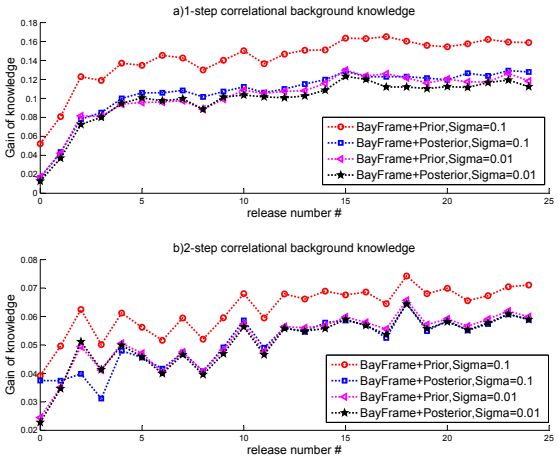

Figure 5: Impact of compromised record on the gain of knowledge for different value of σ (Bkseq dataset)

6.3.3 Performance Of Cascading Methods

In these experiments, we analyze the performance of the proposed framework when some records are compromised. We evaluate the performance of the framework when *J*-similarity is satisfied and different cascading methods are applied. We also study the impact of different values of σ. The gain of knowledge of our framework for the Bkseq and Adult datasets is shown in Figure 5 and Figure 6 as a function of the number of released tables. Each figure shows the gain of knowledge for two different values of σ (σ=0.1 and σ=0.01). For example, the curve labeled *BayFrame+Prior*, $Sigma$=0.1 corresponds to the performance of our framework using the prior-based cascading method when σ is equal to 0.1. k, β, J and $CR(v, s_i, t_i)$ are set to 3, 5, 0.6 and 0.9, respectively.

Figure 5a plots the performance of the framework using 1-step PD^{cor} distributions. The results show that when the adversary exploits the correlational background knowledge, the adversary's gain grows during the first releases. The reason is that the adversary observes the past releases and exploits the previous information to find most likely associations of individuals with sensitive values. On the other hand, anonymizing the releases using our framework causes to decrease the gain of knowledge, especially after the 18^{th} release. We conclude that the proposed framework is effective to limit the adversary's inference capabilities.

We also see in Figure 5a that the gain of knowledge of the framework for σ= 0.1 is higher than that for σ=0.01. Moreover, the gain generated by *BayFrame+Prior* is higher than that by *BayFrame+Posterior* for the same value of σ. The difference between curves labeled *BayFrame+Prior* and *BayFrame+ Posterior* for σ=0.1 is more than that for σ=0.01. The results shown in Figure 5b, confirm our previous finding when the framework applies PD_2^{cor}. It can be observed that the performance curves of *BayFrame+Posterior* for σ=0.1 is similar to that for σ=0.01 (Figure 5b). The reason is that the correlational background knowledge is extracted from the microdata in Bkseq and the 2-step PD^{cor} distributions are the coarser approximation of the exact correlational background knowledge. Thus the changes of posterior beliefs over time are negligible for two different values of σ. We see in Figure 6 that

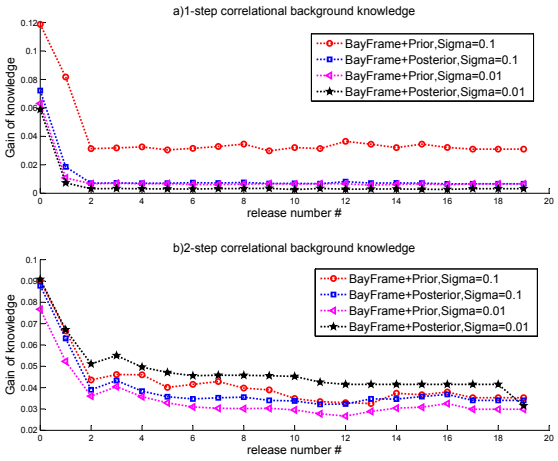

Figure 6: Impact of compromised record on the gain of knowledge for different values of σ (Adult dataset)

our anonymization framework leads to decrease rapidly the gain of knowledge during the first two releases and then the adversary's gain remains below 0.06. Since the uniform distribution is applied as the PD^{cor} distributions, the background knowledge attack is not effective.

Next, we study the performance of the framework with different cascading methods in Figure 7. Experiments are performed on a history of 24 microdata tables existing in Bkseq for σ=0.01 and σ=0.1. Figure 7a shows the performance of our framework using 1-step PD^{cor} distributions. As expected in R-U confidentiality map, GCP decreases as RL increases. It can be seen that the performance of *BayFrame+Prior* is analogous to that of *Bayframe+Posterior* for the same σ values. In each level of RL, the information loss tends to increase as the σ value increases. For example, the information loss incurred by *BayFrame+Prior* for σ=0.1 is more than that for σ=0.01. The experimental results of the framework with PD_2^{cor} are shown in Figure 7b. The performance of the posterior-based cascading method for two different σ values is similar. In the prior-based cascading method, the range of GCP values for σ=0.1 is broader than that for σ=0.01. In Figure 8, the experimental results on the Adult dataset confirm our previous findings.

6.3.4 Comparison To *JS*-reduce Approach

In these experiments, we compare our framework with the closest work, *JS*-reduce [8]. It is worth to mention that we cannot do any fair and clear comparison between our framework and the other close work, Cor-split[16], since it does not consider the correlations between QI and sensitive attribute values as well as the correlations among sensitive attribute values over time.

We conduct two experiments on Bkseq dataset provided in [8]. In these experiments, our framework satisfies the same privacy constraints as those in *JS*-reduce. The parameter values are set as follows: t=0.5, k=3, and J=0.6 which resulted in the best performance of *JS*-reduce. We first compare our framework with *JS*-reduce when our framework applies BKAA and there are no compromised records. Figure 9 shows the experimental results of

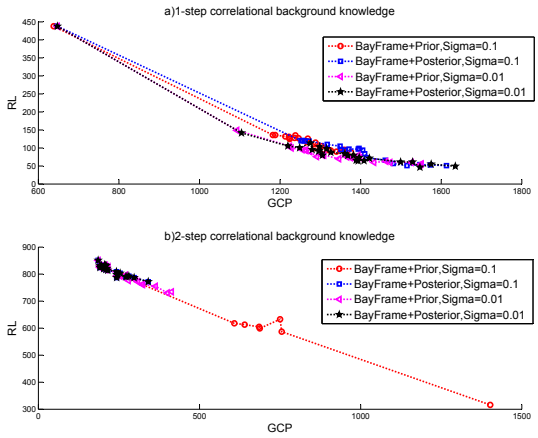

Figure 7: R-U confidentiality map for the proposed anonymization framework on Bkseq dataset for different σ values

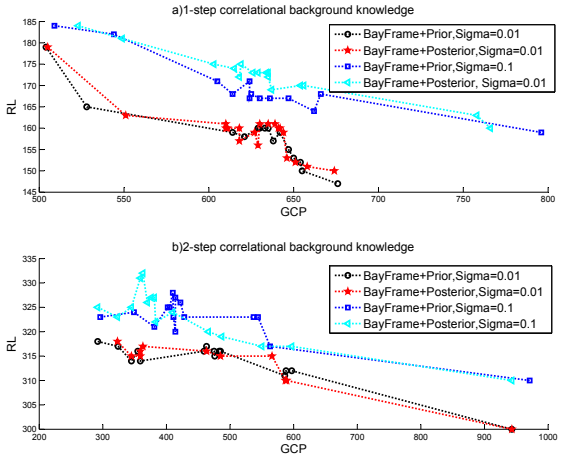

Figure 8: R-U confidentiality map for the proposed framework on Adult dataset for the different σ values

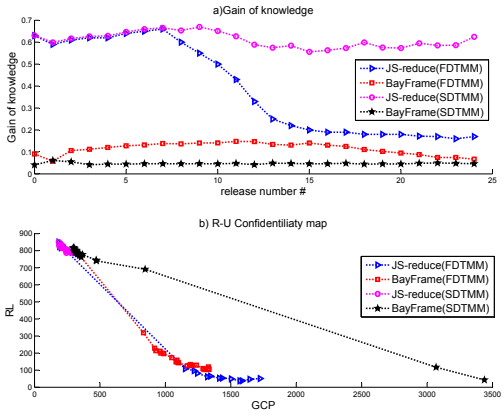

Figure 9: Compare the JS-reduce approach with our framework without any compromised record knowledge (on Bkseq dataset)

both frameworks in terms of the gain of knowledge and the R-U confidentiality map. It can be seen in Figure 9a that *BayFrame*(FDTMM) outperforms *JS*-reduce(FDTMM) in terms of the gain of knowledge. The gain of knowledge of *BayFrame*(SDTMM) is also lower than *JS*-reduce(SDTMM).

According to Figure 9b, the performance of *BayFrame* (FDTMM) is analogous to *JS*-reduce(FDTMM) in terms of GCP and RL. Moreover, the range of the GCP values incurred by *BayFrame*(SDTMM) is broader than *JS*-reduce(SDTMM) such that the GCP and RL values in *JS*-reduce(SDTMM) are in the ranges 200-400 and 750-850, respectively. In *BayFrame*(SDTMM), the range of GCP and RL values are 200-3500 and 100-850, respectively. In Figure 10, we compare the number of records suppressed by *BayFrame* (FDTMM) and JS-reduce(FDTMM) to enforce privacy requirements. Results show that a few numbers of records were suppressed by both methods to enforce privacy requirements; i.e., at most 13 ($<$0.32 %) at each release.

Next, we examine *JS*-reduce and *BayFrame* with respect to threat deriving from compromised records. We adopt *JS*-reduce to cascade the compromised records on revised prior beliefs using Equation (5). The CR probabilities and σ are set to 0.9 and 0.1, respectively. In Figure 11, we compare the results of three frameworks: *JS*-reduce with the prior-based cascading method, *BayFrame* with the prior-based cascading method and *BayFrame* with the posterior-based cascading method. They are denoted as *JS-reduce+Prior*, *BayFrame+Prior* and *BayFrame+Posterior*, respectively. They apply either PD_1^{cor} or PD_2^{cor} as the correlational background knowledge. We let three frameworks satisfy same privacy constraints as those in *JS*-reduce. Figure 11a shows the adversary's gain of knowledge over different lengths of history. Figure 11a indicates that our framework with different cascading method outperforms *JS*-reduce in terms of gain of knowledge. Figure 11b shows the evaluation results in the R-U confidentiality map. The results in Figure 11b show that the performances of three frameworks are analogous when they apply PD^{cor} distributions with equal steps.

To sum up, our framework is better than *JS*-reduce in terms of the gain of knowledge. Although *JS*-reduce can be extended to consider the compromised records knowledge, it is not able to cascade the threat deriving from compromised records within the current release after their publishing. Whereas, our posterior belief estimator cascades the impact of the compromised record knowledge even after publishing the current release. Therefore,

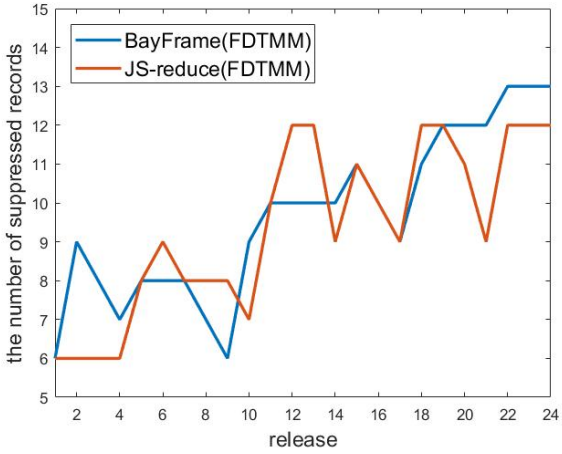

Figure 10: Compare the JS-reduce approach with our framework without any compromised record knowledge (on Bkseq dataset)

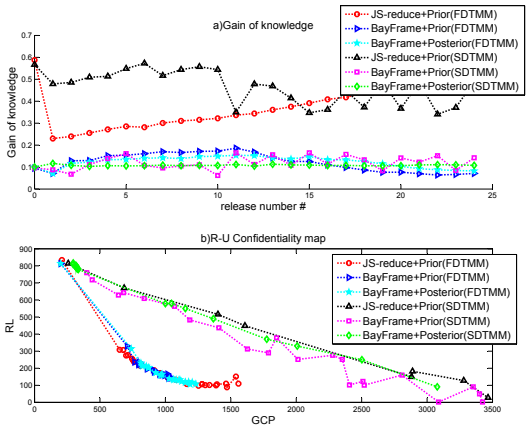

Figure 11: Compare the JS-reduce with our proposed framework in the presence of compromised record knowledge(on Bkseq dataset

our framework outperforms *JS*-reduce.

7 Discussion

The proposed framework prevents the background knowledge attack in continuous data publishing. The framework mimics the adversary's reasoning method and anonymizes each release by the BKAA algorithm to ensure the privacy model. The adversary's reasoning method computes the posterior beliefs of assignments between individuals and sensitive values in each QI-group.

Our posterior belief estimator models all possible assignments as different outcomes of a multinomial distribution and then estimates the probability that a particular outcome will occur. The proposed method uses Bayesian approaches to estimate the parameters of multinomial distributions. According to Bayesian inference, the probability of each outcome is uncertain, so a conjugate prior is put on this probability; the conjugate prior of multinomial distribution is the Dirichlet distribution.

To anonymize T_i, the cost of computing revised prior beliefs is $O(nm^{d+1})$ where n is the number of records in T_i, m is the number of distinct sensitive values and d is the length of history in the correlational background knowledge. The worst case time complexity of the BKAA algorithm is $O(n^2)$. The cost of computing posterior beliefs depends on the number of QI-groups and their size. For a QI group Q, the time complexity of computing posterior beliefs is $O(min(|Q|!, |Q|))$, since the cost of the Bayesian-based estimator is $O(|Q|!)$ while the Ω-estimator takes $O(|Q|)$ for a large QI group. BKAA creates at most $\frac{n}{k}$ equal-size QI groups. Then it takes $O(\frac{n}{k} \times min(|Q|!, |Q|))$ to compute the posterior beliefs in T_i^*. The experimental result shows that the run time of publishing 24 microdata tables existing in Bkseq is about 4 hours when the framework applies the $PD_1^{\varsigma or}$ distributions. It should be noted that this is an acceptable time, since, in most cases, microdata anonymization is performed offline. Moreover, multi-threaded programming can decrease the runtime in this framework. The proposed estimator is also enabling the data publisher to handle the situations in which some records may be compromised in each release.

Moreover, on the one hand, the appropriate approximation of PD^{cor} distributions can increase the adversary's information gain. On the other hand, our proposed framework is able to limit the adversary's inference capabilities and consequently, the information gain decreases. Thus, the information gain can be a criterion to stop or publish the current microdata based on a history of released microdata.

8 Conclusion

We proposed an anonymization framework in continuous publishing that considers the adversary's background knowledge. The adversary's background knowledge is modeled as probability distributions. We investigated a real scenario in which some records are compromised and studied the threat deriving from these compromised records in different releases. We represented two solutions to study this threat based on a Bayesian estimator: prior-based cascading method and posterior-based cascading method. To maintain the data utility, we proposed the background knowledge-based anonymization algorithm. The algorithm produces at least k-record QI-groups, in which β-likeness is satisfied and also the difference among revised prior beliefs of respondents is up to J. Achieving k-anonymity and β-likeness guarantees stronger privacy compared to either k-anonymity or

β-likeness. The experimental results showed that our proposed anonymization framework outperforms *JS*-reduce, the state of the art anonymization approach, while considering a stronger adversary with more background knowledge. Moreover, our framework is able to consider the compromised record knowledge corresponding to the current release after publishing it, while *JS*-reduce does not.

Our work opens directions for the future; one direction is to analyze other kinds of knowledge about relationships among individuals in continuous data publishing. In this work, we assumed that the respondents are independent, while an adversary may exploit the relationship among individuals to breach the individual's privacy. Another direction is to consider the different assumptions as an adversary's inference capability. Moreover, although hierarchical anonymization algorithms [20] in single publishing achieve better data utility and privacy than BKAA, their time complexity is high. We intend to extend a hierarchical anonymization algorithm like the ones in [20] that can be implemented in a continuous data publishing setting.

Acknowledgements

This research was supported in part by a grant from the Institute for Research in Fundamental Sciences (no. CS 1398-4-223).

References

[1] Samarati, P. (2001) Protecting respondents identities in microdata release, IEEE Trans. on Knowl. and Data Eng. 13:6 1010 - 1027

[2] Cao, J., Karras, P. (2012) Publishing microdata with a robust privacy guarantee, PVLDB, 5 1388 - 1399

[3] Dwork, C. (2006) Differential privacy, Proc. the 33rd Int. Conf. Colloquium on Automata, Languages and Programming (ICALP) 1 - 12

[4] Barak, B., Chaudhuri, K., Dwork, K.C., Kale, S., Mcsherry, F. and Talwar, K. (2007) Privacy, accuracy, and consistency too: A holistic solution to contingency table release, Proc. the 26th ACM Symposium on Principles of Database Systems (PODS) 273 - 282

[5] Xiao, X., Tao, Y. (2007) M-invariance: towards privacy preserving re-publication of dynamic datasets, Proc. the 2007 ACM SIGMOD Int. conf. on Management of data 689 - 700

[6] Anjum, A.D., Raschia, G. (2013) Anonymizing sequential releases under arbitrary updates, Proc. the Joint EDBT/ICDT 2013 Workshops 145 - 154

[7] Bu, Y., Fu, A.W.C., Wong, R.C.W., Chen, L. and Li, J. (2008) Privacy preserving serial data publishing by role composition, Proc. the VLDB Endowment 1:1 845 - 856

[8] Riboni, D., Pareschi, L., Bettini, C. (2012) JS-Reduce: defending your data from sequential background knowledge attacks, IEEE Trans. Dep. Sec. Comp. 9:3 387 - 400

[9] Shmueli, E., Tassa,T. (2015) Privacy by diversity in sequential releases of databases, Inf. Sci. 298 344 - 372

[10] Shmueli, E., Tassa, T., Wasserstein, R., Shapira, B., and Rokach, L. (2012) Limiting disclosure of sensitive data in sequential releases of databases, Inf. Sci. 191 98 - 127

[11] Bouna, B.Al., Clifton, C., Malluhi, Q. (2015) Efficient sanitization of unsafe data correlations, Proc. the Workshops of the EDBT/ICDT 2015 Joint Conf. 278 - 285

[12] Kifer, D. (2009) Attacks on privacy and deFinetti theorem, Proc. ACM Int. Conf. Special Interest Group on Management of Data (SIGMOD) 127 - 138

[13] Li, T., Li, N., Zhang, J. (2009) Modeling and integrating background knowledge in data anonymization, Proc. the 25st IEEE Int. Conf. on Data Engineering (ICDE) 6 - 17

[14] Miklau, G., Suciu, D. (2007) A formal analysis of information disclosure in data exchange, J. Comput. Syst. Sci. 73:3 507 - 534

[15] Wang, H., Liu, R. (2011) Privacy-preserving publishing microdata with full functional dependencies, Data & knowl. Eng. 70 249 - 268

[16] Riboni, D., Bettini, C. (2009) Cor-split: defending privacy in data re-publication from historical correlations and compromised tuples, Proc. the 21st Int. Conf. on Scientific and Statistical Database Management 562 - 579

[17] Adult dataset, https://archive.ics.uci.edu/ml/datasets/Adult, accessed April, 2015

[18] Li, N., Li, T., Venkatasubramanian, S. (2007) t-closeness: privacy beyond k-anonymity and L-diversity, Proc. the 23th IEEE Int. Conf. on Data Eng. (ICDE) 106 - 115

[19] Soria-Comas, J., Domingo-Ferrer, J., Sánchez, D., Martínez, S. (2015) t-Closeness through microaggregation: strict privacy with enhanced utility preservation, IEEE Transactions on Knowledge and Data Engineering 27:11 3098 - 3110

[20] Amiri, F., Yazdani, N., Shakery, A., Chinae, A.H. (2016) Hierarchical anonymization algorithms against background knowledge attack in data releasing, Knowl. Based Sys. 101 71 - 89

[21] Fung, B.C.M., Wang, k., Yu, P.S. (2005) Top-down specialization for information and privacy preservation, Proc. the 21st IEEE Int. Conf. on Data Eng. (ICDE) 205 - 216

[22] Ghinita, G., Karras, P., Kalnis, P., Mamoulis, N. (2007) Fast data anonymization with low information loss, Proc. the 33rd Int. Conf. on Very large databases (VLDB) 758 - 769

[23] LeFevre, K., DeWitt, D.J., Raghu, R. (2006) Mondrian multidimensional k-Anonymity , Proc. the 22nd IEEE Int. Conf. on Data Eng. (ICDE) 25 - 35

[24] Wang, H., Liu, R. (2015) Hiding outliers into crowd: privacy-preserving data publishing with outliers', Data & Knowl. Eng. 100 94 - 115

[25] Soria-Comas, J., Domingo-Ferrer, J., Sánchez, D., and Martínez, S. (2014) Enhancing data utility in differential privacy via microaggregation-based k-anonymity, The VLDB Journal, 23 771 - 794

[26] Machanavajjhala, P., Gehrke, J., Kifer, D., Venkitasubramaniam, M. (2007) L-diversity: privacy beyond k-anonymity, ACM Trans. Knowl. Discov. Data. 1:1 doi=10.1145/1217299.1217302

[27] Wang, G., Zutao, Z., Wenliang, D., Zhouxuan, T. (2008) Inference analysis in privacy-preserving data re-publishing, Proc. the Eighth IEEE Int. Conf. Data Mining 1079 - 1084

[28] Lehmann, E.L., Casella, G. (1998) Theory of point estimation, Springer, 1998

[29] Alzheimer association, 2014 Alzheimer's disease Facts and Figures, https://www.alz.org/, accessed Sep 2015

[30] National institute of diabetes and digestive and kidney diseases. At risk for kidney disease? https://www.niddk.nih.gov/health-information/health-communication-programs/nkdep/learn/causes-kidney-disease/at-risk/Pages/are-you-at-risk.aspx, accessed July 2016

[31] Lin, J. (1991) Divergence measures based on the Shannon entropy, IEEE Trans. Inf. Theory. 37:1 145 - 51

[32] Domingo-Ferrer, J., Martnez-Ballesté, A., Mateo-Sanz, J., Sebé, F. (2006) Efficient multivariate data-oriented microaggregation, VLDB J. 15:4 355 - 369

[33] Xu, J., Wang, W., Pei, J., Wang, X., Shi, B., Fu, A. (2006) Utility-based anonymization using local recoding, Proc. the 12th ACM SIGKDD Int. Conf. on Knowl. discovery and data mining 785 - 790

[34] Martin, D.J., Kifer, D., Machanavajjhala, A., Gehrke, J., Halpern, J.Y. (2007) Worst-Case background knowledge for privacy preserving data publishing, Proc. 23rd Int. Conf. Data Eng. 126 - 135

[35] Yang, B., Sato, I., Nakagawa, H. (2015) Bayesian differential privacy on correlated data, Proc. ACM SIGMOD Int. Conf. on Management of Data 747 - 762

[36] Wang, K., Fung, B. (2006) Anonymizing sequential release, Proc. Int. Conf. on Knowl. Discovery and Data Mining 414 - 423

[37] Li, J., Baig, M.M., Sattar, A.H.M.S., Ding, X., Liu, J., Vincent, M.W. (2016) A hybrid approach to prevent composition attacks for independent data releases, Inf. Sci. 367 324 - 336

[38] Amiri, F., Yazdani, N. , Shakery, A. (2018) Bottom-up sequential anonymization in the presence of adversary knowledge, Information Sciences 450 316 - 335

[39] Dwork, C., Naor, M., Pitassi, T., Rothblum,G.N. (2010) Differential privacy under continual observation, Proc. ACM symposium on Theory of computing 715-724

[40] Chan, T.H.H., Shi, E., Song, D. (2011) Private and Continual Release of Statistics. ACM Trans. Inf. Syst. Secur. 14(3) 26:1-26:24

[41] Chan T.H.H. , Shi, E., Song, D.(2012) Privacy-Preserving Stream Aggregation with Fault Tolerance. Financial Cryptography 200-214

[42] Riboni, D., Bettini, C.(2015) Incremental release of differentially-private check-in data. Pervasive and Mobile Computing 16 220-238

[43] Kellaris,G., Papadopoulos, S., Xiao,X., Papadias,D. (2014) Differentially Private Event Sequences over Infinite Streams. PVLDB 7(12) 1155-1166