氏　　名　小野 元

学位(専攻分野)　博士(統計科学)

学 位 記 番 号　総研大甲第 2405 号

学位授与の日付　2023 年 3 月 24 日

学位授与の要件　複合科学研究科 統計科学専攻
学位規則第6条第1項該当

学 位 論 文 題 目　Private Statistical Survey Avoiding Privacy Composition in the Real World

論 文 審 査 委 員　主　査　日野 英逸
統計科学専攻 教授
間野 修平
統計科学専攻 教授
南 和宏
統計科学専攻 教授
村上 隆夫
産業技術総合研究所 主任研究員

（様式３）

博士論文の要旨

氏　　名　小野　元

論文題目　Private Statistical Survey Avoiding Privacy Composition in the Real World

In recent years, data collection and use have become increasingly popular. Since data records are often tied to real individuals, it is necessary to consider the privacy of the data providers when using the data. One promising approach to balance privacy protection and data utilization is to publish perturbed data or statistics instead of raw data. Differential privacy [Dwork et al., 2006, Dwork and Roth, 2014] is a quantitative definition of privacy for such a perturbation strategy. The definition requires a data curator to perturb the publication such that an adversary cannot distinguish two neighboring datasets using the perturbed publication. Moreover, the definition regards a perturbation mechanism as safer if the adversary is less likely to distinguish two neighborhood databases. There are many differentially private algorithms, ranging from basic ones [Dwork and Roth, 2014] to complex ones such as deep learning [Abadi et al., 2016]. Differential privacy has been deployed in the real world. For example, the U.S. Census Bureau adopts differentially private perturbation mechanisms when it publishes statistics of the census [Abowd, 2018].

However, differentially private publications of statistics cannot control privacy risk when a curator publishes a large number of statistics. In the real world, many researchers access and analyze some popular datasets, and eventually publish their findings in research papers. Official microdata are an example of such popular data, which consist of highly sensitive records. As the curator publishes statistics, the privacy risk accumulates. The accumulation of privacy risk is called privacy composition and has been studied in [McSherry, 2009, Kairouz et al., 2015, Abadi et al., 2016]. Even if each publication strictly controls the privacy risk, the accumulated privacy risk caused by multiple publications can be unboundedly large. This issue also occurs on federated learning [Kairouz et al., 2021]. which is a distributed machine learning framework. In the framework, clients who possess a local dataset repeatedly communicate with a central sever to update a statistical estimation. Even if clients perturb their submissions to prevent direct disclosure of their local dataset, privacy risk accumulates communication by communication. Can we avoid the accumulation of privacy risk by multiple publications while maintaining the utility of data?

One possible solution to avoid privacy composition is to use local perturbation methods such that data providers perturb their data before supplying it to a data curator. Local differential privacy (LDP) [Kasiviswanathan et al., 2011, Duchi et al.,

2013] is a quantitative definition of privacy achieved by such a local perturbation method. Originally, local perturbation strategies and LDP are studied to ensure that user privacy is protected even if data curators are adversarial. Notably, Google and Apple have conducted statistical surveys that guarantee user privacy based on this definition [Erlingsson et al., 2014, Apple Differential Privacy Team, 2017]. Data collected while satisfying LDP automatically satisfies DP. The perturbed data can be further used without privacy composition.

Although a data collection method satisfying LDP promises strict privacy protection, the requirement by LDP raises issues concerning privacy and data utility. The LDP definition requires a data provider to perturb her record so as to be indistinguishable from the other candidate records in the domain. To satisfy the requirement, perturbation mechanisms often assume a known data domain that is finite or bounded. However, since the LDP system model allows no participant to have a complete picture of the raw data, the assumption that the data domain is known in advance is unrealistic.

When a perturbation mechanism receives an undesirable value, the mechanism can output an invalid value or nothing. Undesirable values include extremely large values, non-responses, and unintended error messages. By observing the abnormal behavior, the curator can infer that the user supplied an abnormal value. The lack of knowledge of data decreases data utility. For example, the data curator tends to fit the data to a misspecified model.

To handle the issue, we propose an LDP protocol for Quasi-MLE using truncation. Truncation is a technique that projects real values into a bounded interval. Quasi-MLE is an estimator for a model parameter and works even if we misspecified the model. We analyze the QMLE's asymptotic behavior. The analysis helps a curator to understand the data without directly observing the data. The contribution corresponding this paragraph has been published in a conference proceeding [Ono et al., 2022].

Although truncation is helpful for handling extremely large values, it cannot cope with other undesirable values. Since it is necessary to implement a secure exception-handling mechanism to handle various unexpected inputs, we have proposed a modified LDP that includes this exception-handling mechanism. We also analyzed the benefits of including the exception-handling mechanism.

Another possible way to avoid privacy composition is the use of synthetic data that mimics the statistical properties of the original data. Synthetic data are not necessarily discussed in relation to DP, but, in recent years, a framework has been established to quantitatively discuss the degree of protection in relation to DP [Neunhoeffer et al., 2021].

However, it is not obvious that estimators evaluated using synthetic data are always useful as those of population statistics. We identify sufficient conditions

under which estimators evaluated using synthetic do not match the population statistics that we truly wish to estimate. We also show that there may be problems that satisfy sufficient conditions.

This thesis is organized as follows. In Chapter 2, we introduce some knowledge that is necessary to read this thesis. In Chapter 3, we study a locally private quasi-MLE that is feasible in the real world. In Chapter 4, we study the privacy risk in the presence of unexpected values. In Chapter 5, we study the inconsistency of estimators caused by the use of synthetic data. In Chapter 6, we offer conclusion of this thesis.

Form8 : Separate Sheet
（様式８・別紙１）

Results of the doctoral thesis defense

博士論文審査結果

Name in Full
氏 名　　小野　元

Title
論文題目　　Private Statistical Survey Avoiding Privacy Composition in the Real World

小野元氏の博士論文審査を，2023 年 1 月 27 日 15 時から約２時間にわたって，本人および４名の委員全員の出席のもとに行った．論文発表および審査の結果，小野元氏が博士論文の審査および試験に出願することを可とする旨，決定した．

[論文の概要]

論文は６章84ページからなり，英語で書かれている．本論文の目的はランダム性の導入によるプライバシー保護の安全性指標である差分プライバシーの実社会への展開に向け，継続的なデータ利用から漏洩リスクが高まるプライバシー合成の問題の解決策を確立し，その有効性と限界を明らかにすることである．

第１章では差分プライバシーにおけるプライバシー合成の問題を指摘し，その有望な解決策として差分プライバシーの枠組みを分散環境に拡張する局所差分プライバシーの手法，元データの統計的性質を保持する擬似データ生成の２つを取り上げ，それらの利点と課題について述べている．

第２章は本論文の主な解析の対象である統計的推定におけるMinimaxリスク，Quasi-Maximum Likelihood Estimator (QMLE) の漸近正規性等に関する前提知識を解説する．

第３章ではデータの生成分布が未知の状況で，あるモデル族の中からデータを生成した分布として最も尤もらしいモデルのパラメータを推定量とする QMLE に対し，局所差分プライバシーの要件を実現する分散プロトコルを考案している．提案手法が，既存の確率的勾配降下法（SGD）ベースの手法の通信コスト，長い待ち時間，目的関数の勾配のノルムが有界かつ既知とする要件の３つの課題を解決する高い実用性を有することを示し，提案アルゴリズムによる推定量が漸近正規性を持つための十分条件を特定している．さらに分位点回帰について，主定理の十分条件を満たす場合の漸近正規性を実証的に検証している．

第４章ではデータ提供者自身が秘匿処理を行う局所差分プライバシーの枠組みにおいて，プライバシー・メカニズムが想定しない異常値（例えば，欠損値）が入力されると既存のプライバシーモデルにおける安全性が侵害される問題に対し，異常値の例外処理を包含する形にプライバシー・モデルを拡張し，推定量の有用性に関する Minimax リスクを解析している． その解析においては秘匿処理プロセスのマルコフ過程における相互情報量に着目して Minimax リスクの下界を導出している．

第５章ではデータの統計的性質を保持する擬似データを対象に，特定の分析に対する

擬似データの個別有用性を理論的に解析している．擬似データの有用性は分布の類似性に基づく指標が一般的であり，特定の分析に対する有用性を適切に示す保証はないという課題を踏まえ，Minimax リスク解析に基づき目的とする統計量について一致推定量が存在しない十分条件を導出している．

第６章は本論文のまとめである．

［論文の評価］

本論文では，差分プライバシーの実社会への適用に向け，プライバシー合成の問題への対策が不可欠であることを指摘し，その有望な解決策である局所差分プライバシー，擬似データ生成の２つのプライバシー保護技術を対象にそれらの有用性を統計的な推定問題の枠組みで定式化し，厳密な理論的解析を行っている．本論文で得られた理論的結果の適用範囲は広く，否定的な結果を含め，今後の差分プライバシーの実装に有用な知見を示すものであり，統計科学の博士論文として十分な意義を持つと判断される．

なお，第３章の内容は，査読付き英文国際会議 The 25th International Conference on Artificial Intelligence and Statistics (AISTATS 2022)に掲載されている．