（ 続紙 1 ）

京都大学	博士（情報学）	氏名	高木　駿
論文題目	Enhancing Data Utilization through Advanced Differential Privacy Mechanisms （有用性を向上させる高度な差分プライバシ機構）		

（論文内容の要旨）

本論文は、データの利活用における、強固なプライバシ保証を与える手法である差分プライバシにおける課題に取り組んでいる。差分プライバシは2006年に提案されて以来、学術界で高く評価されているものの、実世界での本格的な応用には至っていない。これは主に、差分プライバシが要求する大量のノイズの追加と制約によるデータ利用性の損失が原因である。本研究は、データの利用・公開・中央的分析・分散的分析の4つの重要な領域での差分プライバシの適用に関するものである。各領域において、データ利用性に関連する具体的な課題を特定し、独自の解決策を提案している。

利用の領域では、Uberのような位置情報サービスでの差分プライバシの応用を検討している。ここでの目標は、サービス品質とプライバシ保護の間の最適なトレードオフを見つけることである。この研究は初めて、差分プライバシの原則の下での位置情報プライバシに道路網の構造を取り入れている。差分プライバシ機構に道路網の情報を直接考慮することで、提案された機構は位置情報プライバシをより効果的に保護し、データの有用性を向上する。その際の機構の実用的な最適化手法を提案し、実世界上のデータを用いた実験により、既存手法と比較して、同じプライバシ保護度合いの時に、より有用性が高いことを示した。

公開の領域では、差分プライバシのもとでの応答の正確性に焦点を当てる。 まず、差分プライバシの対称性によって正確性を保証することができないことを証明した。この性質は、公衆衛生のような正確性の高いデータ公開を必要とする状況で特に問題となる。本研究では、差分プライバシを非対称化することを提案している。これはプライバシ保護の部分的な緩和であることを証明し、具体的にどのようなプライバシ漏洩が起こるかを定式化した。これによりプライバシ保護と正確性の保証を両立した。また、このプライバシ保護の緩和が正当化される実際の状況に対する具体的な解決策を提示している。

分散分析の領域では、高いデータ利用性を生み出すことができる差分プライバシのシャッフリングモデルに焦点を当てる。この研究では、まず、シャッフリングモデルがフィルタリングなどの重要なデータ操作を実行できないという大きな制限を明らかにした。そこで、それを可能にするシャッフリングモデルへの修正を提案する。その修正の数学的な分析を行い、最適な修正方法を提案している。これにより、有用性を大きく損なうことなく、フィルタリングが可能な分散分析の手法を提案している。

集中分析の領域では、信頼できる機関によって収集されたデータセットを信頼できない当事者が分析する状況に取り組んでいる。この文脈では、差分プライバシの制約下での深層生成モデルを使用した合成データの生成が、近年注目されている手法である。この研究は、人間の移動データを合成する深層生成モデルに差分プライバシを直接適用した場合に低品質の合成データが生成されることを発見した。この原因を明らかにし、それらに対処する、差分プライバシの特性に基づいた人間の移動データ用の新しい深層生成モデルと訓練手法を考案した。実世界のデータを用いた実験により、既存の手法と比べて、同じプライバシ保護度合いの時に、質の高いデータを生成できることを示した。

各領域は独立した貢献を持っているが、最後に、この研究を通じて一般的に使用さ

れる3つの設計方法論を議論している。この研究は、差分プライバシの厳格なプライバシ基準を損なうことなくデータの利用可能性を高めることに成功し、差分プライバシの理論的側面と実践との間のギャップを埋めることに貢献している。

（続紙 ２ ）

（論文審査の結果の要旨）

個人データの利活用が加速している中で、個人のプライバシの懸念・プライバシに関する法律の制定等がその障壁となっている。それを解決するプライバシ保護技術が必要とされており、その汎用的な手法として差分プライバシが学術上注目されている。しかし、現実世界への幅広い応用にはまだ至っていない。その大きな要因として、差分プライバシ機構によって加えられるノイズによってデータの有用性を大きく損なってしまうことがある。

本論文は、データの利活用領域を四つ挙げ、差分プライバシを適用する際の課題に取り組んだ研究成果をまとめたものである。(1) 位置情報サービスにおける位置情報の利活用におけるサービスの質の低下。(2) 統計値の公開における情報の不確実性。(3) 分散的なデータの分析におけるフィルタリング操作の不能性。(4) 軌跡データの合成の困難性。具体的には、これら四つの課題について以下の成果を上げている。

第一に、既存の差分プライバシ機構では、道路ネットワークを考慮することができないことに着目し、それを可能にする差分プライバシ機構を考案した。それにより、既存手法と比べて、同等のプライバシ保護レベルを与える際の位置情報サービスにおけるデータの有用性を向上させた。

第二に、差分プライバシでは情報の正確性を保証することが不可能であることを証明し、差分プライバシの緩和手法を考案した。その際のプライバシ保護を証明可能な形で定式化することで、合理的なプライバシ保護緩和と正確性の保証を両立させることに成功した。

第三に、既存の差分プライバシ機構ではフィルタリング操作により、プライバシ漏洩を起こすことを発見し、その脆弱性の解決手法を考案した。その解決によるデータの有用性への影響を分析し、最適な設定により、データの有用性への影響が大きくないことを示した。

第四に、まず、深層学習を用いた差分プライバシ機構における軌跡データの合成の難しさの原因を明らかにした。この原因を緩和するネットワーク構造・訓練手法を考案し、既存の手法と比べて質の高い軌跡データを合成できることを示した。

以上、本論文は、現実のアプリケーションに適用する際の利用性とプライバシ保護の間のトレードオフを改善する独自の手法を提案している。新規性が高く学術上、及びデータの利用性を高めるという点で実際の応用において大きな寄与を果たしている。よって、本論文は博士（情報学）の学位論文として価値あるものと認める。また、令和６年２月１９日、論文内容とそれに関連した事項について試問を行った結果、合格と認めた。なお、本論文の令和７年３月２４日以降のインターネットでの全文公表についても支障が無いことを確認した。

要旨公開可能日：　令和６年　　６月　２４日以降