プレスリリース

ISM2024-05

2024 年 11 月 29 日

大学共同利用機関法人 情報・システム研究機構 統計数理研究所

国立大学法人 電気通信大学

国立研究開発法人 産業技術総合研究所

報道関係各位

新しいプライバシー保護データ解析プロトコル「local-noise-free protocol」を開発 ～安全で高精度な頻度分布の推定を可能に～

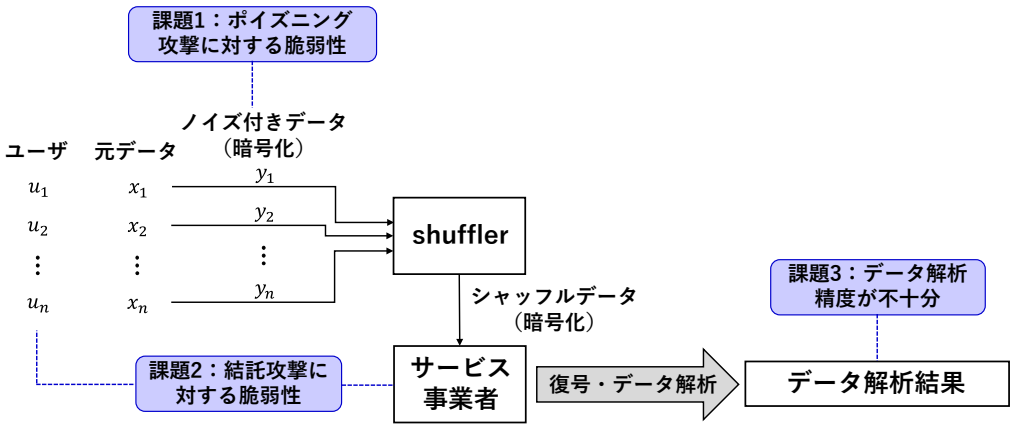

図 1：従来のシャッフルモデルのプロトコルと 3 つの課題

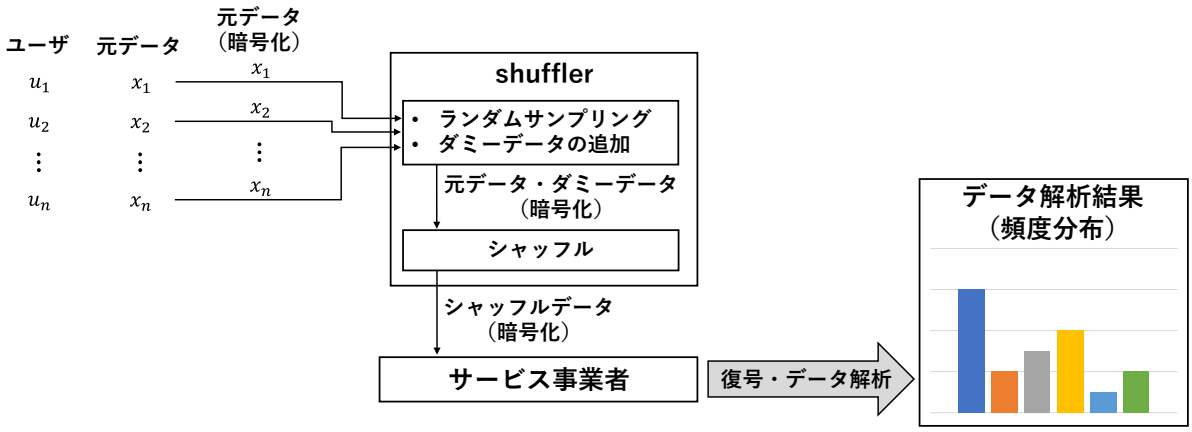

図 2：開発したプライバシー保護データ解析プロトコル「local-noise-free protocol」

プレスリリース

統計数理研究所の村上隆夫准教授、電気通信大学の清雄一教授、産業技術総合研究所の江利口礼央研究員の研究グループは、パーソナルデータの漏洩を強固に防ぐ「差分プライバシー（DP: Differential Privacy）」※1を満たす新しいプロトコル「local-noise-free protocol」を開発しました。開発したプロトコルでは、各ユーザが自身のパーソナルデータをそのまま暗号化して「shuffler」と呼ばれる中間サーバに送信します。次に、shuffler が受け取ったデータのランダムサンプリングとダミーデータの追加を行った上でデータをシャッフルし、サービス事業者に送信します。最後に、サービス事業者が受け取ったデータを復号し、全ユーザのデータの頻度分布を推定します。このプロトコルにより、サービス事業者や一部の悪意を持ったユーザが様々な不正を試みても、安全で高精度な頻度分布の推定が可能となり、それに基づく様々なデータ解析への応用が期待できます。

本成果は、情報セキュリティ分野の最難関国際会議 The 46th IEEE Symposium on Security and Privacy (S&P 2025)（過去 5 年間の採択率：14.8%）に採択されました。

【研究の背景】

スマートフォン、ウェアラブル端末、IoT（Internet of Things）などの普及に伴い、位置情報や身体活動データなどの様々なパーソナルデータを収集して、様々なデータ解析に利用できるようになりました。一方、このようなデータ解析は個人の情報を用いているため、プライバシーの問題が懸念されています。個人のプライバシーを強固に保護するために、「差分プライバシー（DP: Differential Privacy）」※1と呼ばれる安全性指標が、デファクト標準として広く用いられています。

差分プライバシーを実現するモデルとしては、中央集権型モデル、局所型モデル、シャッフルモデルなどがあります。中央集権型モデルでは、サービス事業者が全ユーザのパーソナルデータを保持しており、そこから求めたデータ解析結果に DP を満たすノイズを加えます。このモデルは、高いデータ解析結果の精度を実現できるのですが、不正アクセスなどにより、サービス事業者から全ユーザの元データが漏洩するリスクを抱えています。局所型モデルでは、ユーザが自身のデータに DP を満たすノイズを加えた上でサービス事業者に送信し、サービス事業者がノイズ付きのデータからデータ解析結果を求めます。このモデルではサービス事業者にはノイズ付きのデータしか送られないため、サービス事業者から元データが漏洩するリスクがありません。しかし、各ユーザが DP を満たすように大きなノイズを加える必要があるため、データ解析精度が低いという問題があります。

シャッフルモデルは、中央集権型モデルと局所型モデルの両方の短所を解決するためのモデルとして近年提案されたものです。具体的には、ユーザとサービス事業者の間に「shuffler」と呼ばれる中間サーバを導入します。従来のシャッフルモデルのプロトコル（図 1）では、各ユーザが自身のデータにノイズを加えて暗号化した上で shuffler に送信し、shuffler が受け取ったデータをランダムにシャッフルした上で、サービス事業者に送信します。サービス事業者は受け取ったデータを復号することで、シャッフルされたノイズ付きデータを取り出し、そこからデータ解析結果を求めます。この shuffler によるシャッフルが匿名性を高める効果を持っており、その分、ユーザが加えるノイズを少なくすることができます。また、サービス事業者には元データは送られないため、局所型モデルより高いデータ解析精度を実現しつつ、中央集権型モデルと比べてサービス事業者からの元データの漏洩リスクを低減できます。

しかし、従来のシャッフルモデルは大きな課題を 3 つ抱えていました。1 つ目の課題は、一部の悪意を持ったユーザが自身のデータと異なる偽のデータを送ることで、データ解析の精度を下げる「ポイズニング攻撃」に対する脆弱性です。特に、プライバシーを高めようとするほど、本来ユーザが加えるべきノイズ量が増加する一方、攻撃者は偽データにノイズを加えなくて良いため、データ解析の精度劣化の度合いが大きくなります。2 つ目の課題は、

プレスリリース

サービス事業者が一部のユーザと結託する「結託攻撃」に対する脆弱性です。具体的には、サービス事業者が、結託したユーザ達のノイズ付きデータを入手することで、シャッフルによる匿名化の効果を下げることができ、その分、他のユーザ達の元データを推定する（即ち、プライバシー情報を暴露する）ことが可能となります。3 つ目の課題は、データ解析精度です。具体的には、局所型モデルよりはユーザが加えるノイズを少なくできるものの、依然としてユーザのノイズ量がまだ大きいという問題を抱えています。例えば、全ユーザのデータの頻度分布（Frequency Distribution）※2 を推定するタスクにおいては、頻度の小さいカテゴリー（あるいは区間）がノイズに埋もれてしまって高精度な解析ができなくなります。従来では、このような課題に対して、根本的な解決策は提示されていませんでした。

【研究成果】

本研究では、データ解析のタスクとして頻度分布の推定に着眼し、従来のシャッフルモデルが抱えていた「ポイズニング攻撃」と「結託攻撃」に対する脆弱性を根本的に解決する新しいプロトコル「local-noise-free protocol」を開発しました（図 2）。開発したプロトコルでは、ユーザは自身のデータにノイズを全く加えず、そのまま暗号化して shuffler に送ります。その後、shuffler は(1)ランダムサンプリング、(2)ダミーデータの追加、(3)シャッフルという 3 つの処理を行います。まず、各ユーザから受け取ったデータを一定の確率で削除します（ランダムサンプリング）。次に、データのとり得る値の各々に対して、「ダミー数分布」と呼ばれる分布に従ってダミーデータ数を決定し、その数だけ暗号化されたダミーデータを加えます（ダミーデータの追加）。最後に、残ったユーザのデータとダミーデータをランダムにシャッフルした上で（シャッフル）、サービス事業者に送ります。サービス事業者は、シャッフルされたデータを復号して取り出し、そこから頻度分布を求めます。本研究では、このように shuffler がデータのシャッフルに加えて、ランダムサンプリングやダミーデータの追加を行うモデルを「拡張シャッフルモデル（augmented shuffle model）」と呼んでいます。

開発したプロトコルの最大の特徴は、ユーザがノイズを一切加えない点（即ち、「local-noise-free」である点）にあります。従来のシャッフルモデルのプロトコルでは、ユーザがノイズを加えていたため、一部のユーザが偽データを送る「ポイズニング攻撃」によってデータ解析の精度が大幅に劣化する問題を抱えていました。また、サーバが一部のユーザと結託してノイズ付きデータを入手する「結託攻撃」によって、他のユーザの元データが推定されるリスクもありました。これらの脆弱性は、どちらもユーザがノイズを加えることに原因がありました。一方、開発したプロトコルでは、ユーザではなく、shuffler がランダムサンプリング・ダミーデータの追加というノイズ付与処理を行うため、「ポイズニング攻撃」と「結託攻撃」の両方に対する頑健性を実現できます。その結果、サービス事業者や一部のユーザが不正を試みても、安全で高精度な頻度分布の推定が可能となります。また、shuffler には暗号化されたデータしか送られないため、shuffler からの元データの漏洩リスクも回避できます。尚、shuffler のランダムサンプリング・ダミーデータの追加・シャッフルという 3 つの処理は、ユーザから受け取った暗号化データを復号することなく実行でき、開発したプロトコルは任意の公開鍵暗号方式を用いて簡単に実現できます。

さらに、本研究では、ダミー数分布として、「非対称幾何分布（Asymmetric Geometric Distribution）」という新しい分布を導入することにより、従来のシャッフルモデルのプロトコルより遥かに高精度な頻度分布の推定を実現しました。DP を満たすための分布として「非対称幾何分布」を用いるのは、本研究が初です。この分布を導入することで、7 つの state-of-the-art の従来プロトコルと比べて、全ユーザのデータの頻度分布とその推定値との平均二乗誤差（MSE: Mean Squared Error）を 2-4 桁減らすことに成功し、頻度の高いところから低いところまで、高精度な頻度の推定ができることを示しています。

プレスリリース

【今後の展望】

本研究で開発したプロトコルは、プライバシーを強固に保護したまま、高精度な頻度分布の推定を行うことを可能にしています。頻度分布の推定は、最も基本的なデータ解析タスクの一つで、位置情報から人気のある観光地を解析する、あるいはウェアラブル端末から全ユーザの身体活動データの大まかな傾向を解析する、といったユースケースに応用することが期待できます。

【用語解説】

1）差分プライバシー（DP: Differential Privacy）：データ解析結果にノイズを加えることで、どのような攻撃者がデータ解析結果を入手しても、元のパーソナルデータに関する情報をほとんど得ることができないことを数理的に保証する安全性指標。プライバシー保護データ解析における安全性指標のデファクト標準として知られ、米国の企業や政府などで導入が進められている。

2）頻度分布（Frequency Distribution）：データを特定のカテゴリー（あるいは区間）に分類し、カテゴリーごと（あるいは区間ごと）の頻度、すなわちデータ数をカウントすることで求めた分布。度数分布とも言う。

【発表論文】

学会名：The 46th IEEE Symposium on Security and Privacy (S&P 2025)

タイトル：Augmented Shuffle Protocols for Accurate and Robust Frequency Estimation under Differential Privacy

著者：村上隆夫（統計数理研究所 学際統計数理研究系 准教授／産業技術総合研究所 サイバーフィジカルセキュリティ研究センター 客員研究員）、清雄一（電気通信大学 大学院情報理工学研究科 情報学専攻 教授）、江利口礼央（産業技術総合研究所 サイバーフィジカルセキュリティ研究センター 研究員）

DOI：10.1109/SP61157.2025.00019

論文公開日：2024 年 11 月 16 日

【謝辞】

本研究の一部は、日本学術振興会科学研究費（22H00521、24H00714、24K20775）、科学技術振興機構 AIP 加速研究（JPMJCR22U5）、科学技術振興機構 CREST（JPMJCR22M1）の助成を受けて実施されました。

本件に関するお問い合わせ先

【研究内容について】

大学共同利用機関法人 情報・システム研究機構 統計数理研究所

学際統計数理研究系 准教授

村上 隆夫

E-mail：tmura@ism.ac.jp

【報道・広報について】

大学共同利用機関法人 情報・システム研究機構 統計数理研究所

運営企画本部 企画室 URA ステーション

TEL：050-5533-8500（代表） E-mail：ask-ura@ism.ac.jp

〒190-8562 東京都立川市緑町 10-3