プレスリリース

ISM2026-08

2026 年 8 月 20 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

TEE (Trusted Execution Environment)を用いた プライバシー保護データ解析に向けた安全性指標の導入と アルゴリズムの開発

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、「TEE（Trusted Execution Environment）」[※1]と呼ばれる高信頼実行環境を用いて、パーソナルデータの漏洩を防ぐデータ解析アルゴリズムを開発しました。開発したアルゴリズムは、近年プライバシー保護分野で研究されている「拡張型シャッフルモデル」[※2]を、TEE を搭載した 1 台のサーバを用いて実現します。拡張型シャッフルモデルは一部の悪意を持ったユーザが不正を試みてもデータの漏洩を防ぐことを可能とするもので、TEE はサーバ管理者でさえも内部のデータを閲覧・改ざんできないことを保証します。これらにより、悪意のあるユーザやサーバ管理者に対してもデータの漏洩を防ぐことが可能となります。

このようなアルゴリズムを開発するにあたり、TEE に対するサイドチャネル攻撃まで考慮した安全性指標を導入しました。具体的には、TEE は内部のデータを保護するものとして注目されていますが、メモリアクセスパターンや制御フローに基づくサイドチャネル攻撃によって、内部のデータが漏洩するリスクがあることが近年の研究で明らかになっています。この問題を解決するため、本研究では、攻撃者がアルゴリズムの出力・メモリアクセスパターン・制御フローの全てを入手したとしても、内部の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「FODP（Fully Oblivious Differential Privacy）」という安全性指標を新たに導入し、FODP を満たすようにアルゴリズムを設計しました。これにより、サイドチャネル攻撃に対しても高い安全性を保証することが可能となります。また、開発したアルゴリズムが高い精度と効率性（短い実行時間）を達成できることを、他の既存のアルゴリズムやモデルとの比較を通して明らかにしています。

本成果は、情報セキュリティ分野のトップ国際会議 The 35th USENIX Security Symposium（USENIX Security 2026、採択率：12.0%）に採択されました。

【研究の背景】

近年、スマートフォン・ウェアラブル端末・AI（Artificial Intelligence）などの普及に伴い、サービス事業者がユーザから様々なパーソナルデータ（購買履歴、位置情報、身体活動データなど）を収集して、データ解析や機械学習などの用途に利活用できるようになりました。一方で、個人のデータが用いられることから、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保護したままデータ解析や機械学習を行うため、「差分プライバシー（DP: Differential Privacy）」[※3]と呼ばれる安全性指標が広く用いられています。差分プライバシーは、データ解析結果や機械学習モデルに十分なノイズを加えることで、元データの漏洩を防ぐもので、それを実現するシステム・アーキテクチャという観点から幾つかのモデルに大別されます。

差分プライバシーのモデルの一つに「シャッフルモデル」[※2]と呼ばれるものがあり、高い精度と安全性を両立できるモデルとして知られています。シャッフルモデルでは、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。まず、ユーザが自身のパーソナルデータにノイズを加えた上で shuffler に送信し、shuffler が受け取ったデータのシャッフルを行った上で、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シャッフルデータを基に、データ解析や機械学習モデルの構築を行います。この shuffler によるデータのシャッフルが匿名化の効果を持っているため、その分、ユーザが加えるノイズの量は小さくてもデータの漏洩を防ぐことができます。即ち、高い精度と安全性を実現できます。

shuffler がデータのシャッフルを行う前に、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う「拡張型シャッフルモデル」[※2]というものも近年研究されています。ランダムサンプリングとダミーデータの追加は「ノイズ付与」としての役割を果たすため、このモデルではユーザがノイズを一切加えなくても高い安全性を実現できるようになります。拡張型ではないシャッフルモデルでは、一部の悪意を持ったユーザ（あるいは不正アカウント）がサービス事業者に自身のノイズ付きデータを共有することで、シャッフルによる匿名化の効果（即ち、安全性）を下げることができてしまいます。一方、拡張型シャッフルモデルでは、shuffler によるノイズ付与処理とシャッフル処理で高い安全性を担保できるため、悪意を持ったユーザが上記のような不正を試みても、データの漏洩を防ぐことが可能となります。

しかし、この拡張型シャッフルモデルにおいても大きな課題が残されていました。このモデルでは、shuffler が正確にプロトコル通りにノイズ付与処理（ランダムサンプリング、ダミーデータの追加）とシャッフル処理を行い、また秘密にすべき情報（シャッフル前のデータなど）を暴露しないことを保証する必要があります。逆に、shuffler がプロトコルを逸脱する、秘密情報を暴露するといった不正を行うと、元データが漏洩するリスクがあります。

―shuffler の信頼性をどう担保するか？―

この質問に対する根本的な解決策は、従来では提示されていませんでした。

【研究成果】

本研究では、データ解析タスクとして頻度分布[※4]の推定に焦点を当て、shuffler の信頼性を担保するために「TEE（Trusted Execution Environment）」[※1]を用いたアルゴリズムを開発しました（図 1）。開発したアルゴリズムは、拡張型シャッフルモデルを 1 台のサーバを用いて実現し、サーバの TEE 内部が shuffler、TEE 外部がサービス事業者としての役割を果たします。即ち、まず各ユーザが自身のパーソナルデータをサーバの TEE 内部に送信します。次に、サーバは TEE 内部で受け取ったデータのランダムサンプリング、ダミーデータの追加、データのシャッフルを行って、シャッフルされたデータを TEE 外部に置きます。最後に、サーバは TEE 外部にあるシャッフルデータを基に、全ユーザのデータの頻度分布を推定します。TEE は OS や管理者権限からも保護された、ハードウェアレベルの隔離された実行環境で、サーバ管理者でさえも内部のデータを閲覧・改ざんできないことを保証します。また、内部のコードが改ざんされていないことを第三者に証明する仕組みも有しています。これにより、shuffler がプロトコルに従い、秘密にすべき情報を暴露しないことを保証することが可能となります。

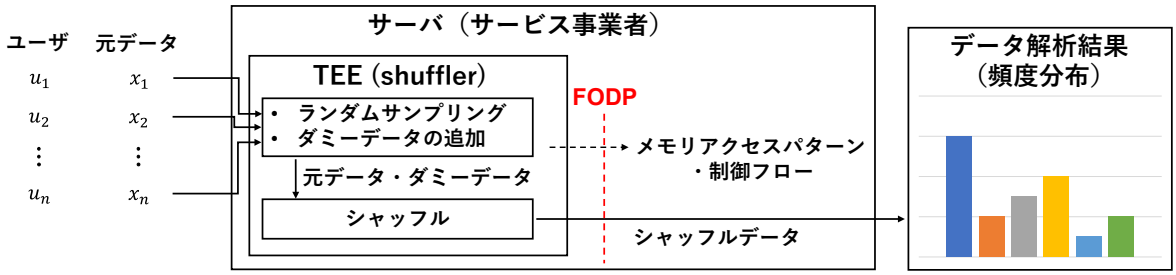

図 1: 開発したアルゴリズム。シャッフルデータとサイドチャネル情報（メモリアクセスパターン・制御フロー）から元データが漏洩しないことを FODP（Fully Oblivious Differential Privacy）によって数理的に保証する。

開発したアルゴリズムの最大の特長は、TEE に対するサイドチャネル攻撃を強固に防ぐことができる点です。TEE は内部のデータを保護するものとして近年注目を集めていますが、メモリアクセスパターンや制御フローに基づくサイドチャネル攻撃によって、内部のデータが漏洩し得ることが近年の研究で明らかになっています。この問題を解決するため、本研究では、攻撃者がアルゴリズムの出力（即ち、シャッフルデータ）・メモリアクセスパターン・制御フローの全てを入手しても、内部の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「FODP（Fully Oblivious Differential Privacy）」という安全性指標を新たに導入し、FODP を満たすようにアルゴリズムを設計しました。具体的には、開発したアルゴリズムでは、アルゴリズムの出力にノイズが加わるようにダミーデータを追加するだけでなく、メモリアクセスパターン・制御フローにノイズが加わるように「bot」（無意味なデータ）を追加します。これによって FODP を達成でき、サイドチャネル攻撃に対する安全性を保証することが可能となります。さらには、ダミー数分布／bot 数分布として、それぞれ「右／左に歪んだ非対称幾何分布」（positively/negatively skewed asymmetric geometric distribution）を導入し、その歪度（skewness）を、ランダムサンプリングの確率に応じて適切に調整する方法論も提案しています。これによって、bot の数を最小限に抑えることが可能となり、計算時間を削減できます。このような左右に歪んだ非対称幾何分布は、プライバシー保護の分野では初めて導入された新しいものです。

本研究では、他の既存のシャッフル／拡張型シャッフルアルゴリズムとの比較を通して、開発したアルゴリズムが安全性・精度・効率性において優れていることを示しています。また、開発アルゴリズムは、悪意を持ったユーザが偽データを送る「ポイズニング攻撃」に対しても、既存のアルゴリズムより高い頑健性を有しており、依然として高精度なデータ解析が可能なことも示しています。さらには、他のモデルとの比較も行うことで、開発アルゴリズムの有効性を明らかにしています。例えば、TEE を用いるのであれば、TEE 内部で直接ヒストグラムを求め、ノイズを加えた上で TEE 外部に出力することも可能です。これは、「中央集権型モデル」のアルゴリズムとして知られています。しかし、このようなアプローチは、FODP を満たそうとすると、ユーザ数・カテゴリー数が大きいときに膨大な計算時間が必要となります。一方、拡張型シャッフルモデルにおける処理は、計算時間の一番大きなシャッフル処理ですら効率的に計算できるため、遥かに短い計算時間で実行可能です。例えば、ユーザ数・カテゴリー数がともに 1 億という大規模データにおいて、中央集権型モデルのアルゴリズムでは 270 日程度の実行時間がかかるのに対し、開発したアルゴリズムでは 16 時間以下で済むことを、評価実験を通して示しています。また、中央集権型モデルは精度が非常に高いことで知られていますが、開発したアルゴリズムは上述の非対称幾何分布の導入により、このモデルと同等の精度を達成することも可能です。

以上をまとめると、本研究では、TEE を用いた拡張型シャッフルモデルの実現に向けて、サイドチャネル攻撃に対する安全性を保証する FODP という新たな安全性指標を導入し、これを満たすようにアルゴリズムを開発しました。開発したアルゴリズムは、悪意のあるユーザや、サイドチャネル攻撃を試みるサーバ管理者に対してもデータの漏洩を防ぐことができ、高い精度・効率性も達成できます。

【今後の展望】

本研究で開発したアルゴリズムは、TEE を搭載した 1 台のサーバを用いて、プライバシーを保護したまま最も基本的なデータ解析タスクの一つである頻度分布の推定を可能にします。今後、本研究で確立した安全性指標（FODP）やアルゴリズムを、頻度分布の推定以外のデータ解析や、機械学習などのタスクに応用していくことを予定しています。

【用語解説】

１）TEE（Trusted Execution Environment）：OS や管理者権限からも保護された、ハードウェアレベルの隔離された実行環境。内部のデータの漏洩や改ざんを防ぐものとして近年注目を集めている。

２）シャッフルモデル（Shuffle Model）／拡張型シャッフルモデル（Augmented Shuffle Model）：差分プライバシーにおいて近年研究されているモデル。シャッフルモデルでは、ユーザが自身のパーソナルデータにノイズを加えた上で shuffler に送信し、shuffler が受け取ったデータのシャッフルを行った上で、サービス事業者に送信する。拡張型シャッフルモデルでは、shuffler がデータのシャッフルを行う前に、受け取ったデータのランダムサンプリング、ダミーデータの追加を行う。拡張型シャッフルモデルについては**【関連情報】**も参照されたい。

３）差分プライバシー（DP: Differential Privacy）：データ解析結果から、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。

４）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（あるいは区間）ごとの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。頻度分布の推定は、データ解析における最も基本的なタスクの一つとして広く研究されている。

【関連情報】

［プレスリリース］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～: https://www.ism.ac.jp/ura/press/ISM2024-05.html

【発表論文】

学会名：The 35th USENIX Security Symposium (USENIX Security 2026)

タイトル：Fully Oblivious Differential Privacy for Frequency Estimation in the Augmented Shuffle Model with Trusted Processors

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／情報・システム研究機構 データサイエンス共同利用基盤施設 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部門 客員研究員／理化学研究所 革新知能統合研究センター 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部門研究員）

URL：https://www.usenix.org/conference/usenixsecurity26/presentation/murakami

論文公開日：2026 年 8 月 12 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 経済安全保障重要技術育成プログラム（JPMJKP24U5）、科学技術振興機構 日 ASEAN 科

学技術・イノベーション協働連携事業（JPMJNX25C2）、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 広報室
TEL：050-5533-8500（代表） E-mail：kouhou@ml1.ism.ac.jp
〒190-8562 東京都立川市緑町 10-3