平成 29 年 3 月 1 日

報道関係者各位

国立大学法人　筑波大学
国立研究開発法人　科学技術振興機構

数値･順序･離散データを暗号化したまま統計解析する実用的秘密計算手法を開発

研究成果のポイント

1. データを暗号化したまま統計解析を行うための秘密計算手法を構築しました。
2. 完全準同型暗号における高速な行列演算と大小比較演算を開発し、統計解析の秘密計算において、計算効率性と高精度を両立できることを示しました。
3. 複数の組織に分散した個人情報を用いて、プライバシーを一切損なうことなく、組織横断的な統計解析や機械学習が実現できるようになります。

筑波大学システム情報系　佐久間淳　教授、同大学院システム情報工学研究科　陸文杰（博士後期課程1年）、川崎将平（博士前期課程2年、研究当時）および中澤貴明　技術職員（研究当時）の研究グループは、情報を暗号化したまま加算や乗算が可能である完全準同型暗号を用いて、数値属性データ、順序属性データ、離散属性データなどを暗号化したまま統計解析を実現するための秘密計算手法を構築しました。多様な種類のデータから記述統計、予測統計、統計的検定など様々な種類の統計解析の秘密計算を統一的に実現できる世界初の技術です。

完全準同型暗号とは、入力情報を暗号化したまま加算や乗算を可能にする、データ解析のセキュリティ･プライバシー保護のための理想的な性質を持つ暗号系の総称で、2009年に初めて実現可能な方式が提案されました。しかしながら、大規模データにおいて実用的な計算時間と計算精度を保証しつつ様々な統計解析を実行する手法は実現できていませんでした。

本研究グループは、多くの統計計算が行列演算と大小比較演算で記述されることに着目し、完全準同型暗号を用いた効率の良い行列演算と大小比較演算のためのアルゴリズム、および、統計解析に必要な高精度の数値演算を暗号文上で実現するための演算方法を開発しました。これらの手法を組み合わせることで、数値属性、順序属性、離散属性を含む数万レコードの暗号化データを対象として、標準的な記述統計や予測統計、統計的検定などの評価を数秒から10分程度で実現することに成功しました。

個人の医療情報や遺伝情報、行動履歴、購買履歴などは、プライバシー保護のために組織横断的な統合が困難でした。この技術を活かすことで、プライバシーを一切損なうことなく、組織の壁を超えた統計解析や機械学習が実現できるようになることが期待できます。

本研究成果は2017年2月26日から開催される米国の国際会議「The Network and Distributed System Security Symposium 2017」(NDSS)で発表される予定です。

また、開発の成果は2017年3月31日にソースコードがオープンソースとして公開される予定です。

＊本成果は、JST戦略的創造研究推進事業（CREST）「ビッグデータ統合利活用のための次世代基盤技術の創出･体系化」研究領域（研究総括：喜連川優･国立情報学研究所/東京大学）における研究課題「自己情報コントロール機構を持つプライバシー保護データ収集･解析基盤の構築と個別化医療･ゲノム疫学への展開」（研究代表者：佐久間　淳）によって得られました。また、本研究領域は平成28年度から文部科学省の人工知能/ビッグデータ/IoT/サイバーセキュリティ統合プロジェクト（AIPプロジェクト）の一環として運営しています。

研究の背景

ビッグデータとこれを用いた統計解析は、私たちの生活を支援する画期的なサービスを生み出す源泉となりますが、データが機密情報や個人から取得された情報を含む場合、慎重な取り扱いが必要になります。秘密計算とはデータを暗号化したまま別のサーバに預けてデータ解析を行い、その計算結果だけを返してもらう方法です。暗号化データを預けたサーバには暗号文を解読することができないため、サーバデータの内容を一切明かさずに、データ解析のみを委託することが可能になります。また万が一、サーバからデータが漏洩しても、データは暗号化されているため、復号のための鍵が漏洩しない限り、内容が漏洩することはありません。このような秘密計算をアウトソーシング型秘密計算と呼びます。

準同型暗号はアウトソーシング型秘密計算を実現するために必要な暗号理論における要素技術です。暗号化したまま加算ができる「加法準同型性暗号」や乗算ができる「乗法準同型性暗号」は古くから知られていましたが、暗号化したまま加算と乗算の両方ができる「完全準同型性暗号」は2009年になって初めて実現されました*（図1）。2進数においては、加算はAND演算、乗算はXOR演算に相当します。コンピュータで計算可能な計算はすべて、AND演算とXOR演算の組み合わせで表すことができますから、完全準同型性暗号の実現によって、いかなる計算もアウトソーシング型秘密計算として実現可能であることが同時に示されたと言えます。

提案当初の完全準同型性暗号は、暗号文や鍵が極めて多くの記憶容量を必要とする上に、実用的な時間で計算可能な乗算の回数は数回に限られるなど、多くの制約がありました。その後の研究開発によって、計算時間と記憶容量は飛躍的に改善されましたが、大規模データを入力とする統計解析計算を、実用的な計算時間と記憶容量において実行することは困難でした。

研究内容と成果

本研究グループは、代表的な統計解析が必要とする計算が、実数行列の加算と乗算および実数の比較演算の組み合わせに帰着できることに着目し、完全準同型性暗号においてこれらの計算を高速かつ高精度に実現する手法を開発しました。この手法を用いて、数万レコード規模の数値属性、順序属性、カテゴリ属性からなるデータについて、最頻値などの記述統計を数秒～数分程度で，線形回帰などの予測統計モデリングを10分程度で計算可能であることを示しました。例えば線形回帰では、入力次元数に対して指数的な計算時間を必要とする従来の手法に比べ、多項式時間での計算が実現し、20~数千倍以上の効率化となります。

完全準同型暗号の暗号文は多くの記憶容量を消費します。そこで、数十次元程度の実数行列を、暗号系の代数的構造を利用して一つの暗号文に詰め込むことで、1データあたりが消費する記憶容量を低減すると同時に、暗号化された行列同士の準同型加算や準同型乗算の繰り返し実行を可能にするレイアウトを考案しました（図2）。これにより、単一の暗号文から様々なアルゴリズムによって多様な統計量を計算することが可能にしました。

また従来、完全準同型暗号が計算効率的に扱うことができる数値データの精度は限定的でしたが、、同様に暗号の代数的構造を利用して一つの数値の行列を複数の暗号文を用いて表現することで、任意精度の数値の行列を表現する手法を開発しました（図3）。これにより、精度の高い数値計算を必要とする予測統計モデリングを暗号文で高速かつ並列実行することを可能にしました。

完全準同型暗号を用いた秘密計算は、すでに長年のアルゴリズムの工夫の積み重ねと高度な実装技術による高速化が実現している秘匿回路評価による計算に比べ、低速で実用性に欠けると考えられていました。今回の実験結果は、行列の乗算や数値の大小比較を含む秘密計算の場合、完全準同型暗号を用いた方法が、条件によっては秘匿回路評価と同等以下の計算時間で処理できることを示しており、これまでの常識を覆す画期的な結果です。

本研究グループは、開発した秘密計算手法の開発フレームワークを2017年3月末にオープンソースとして公開する計画です。

今後の展開

本研究では、数値·順序·離散データを暗号化したまま統計解析する、完全準同型暗号に基づく秘密計算フレームワークを開発しました。このフレームワークを用いることで、複数の組織が保持する個人情報や機密情報を、その機密性やプライバシーを損なうことなく統計解析を行い、その解析結果のみを安全に取得することが可能になります。今後は医療データや個人ゲノムデータ、金融データなど、その取り扱いに慎重さが求められるデータにおいて、プライバシーを完全に保護しつつ自由に統計解析が実行できるようになることが期待できます。

参考図

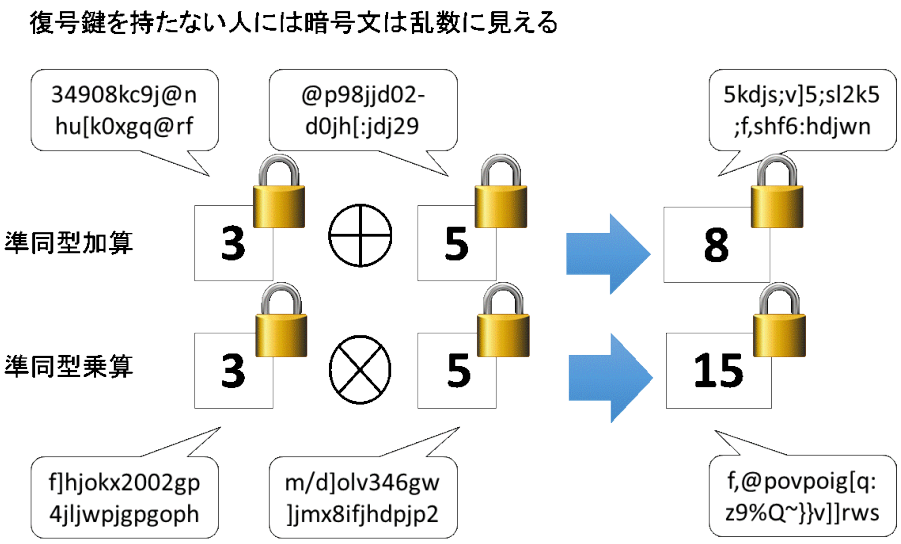

図 1　完全準同型暗号

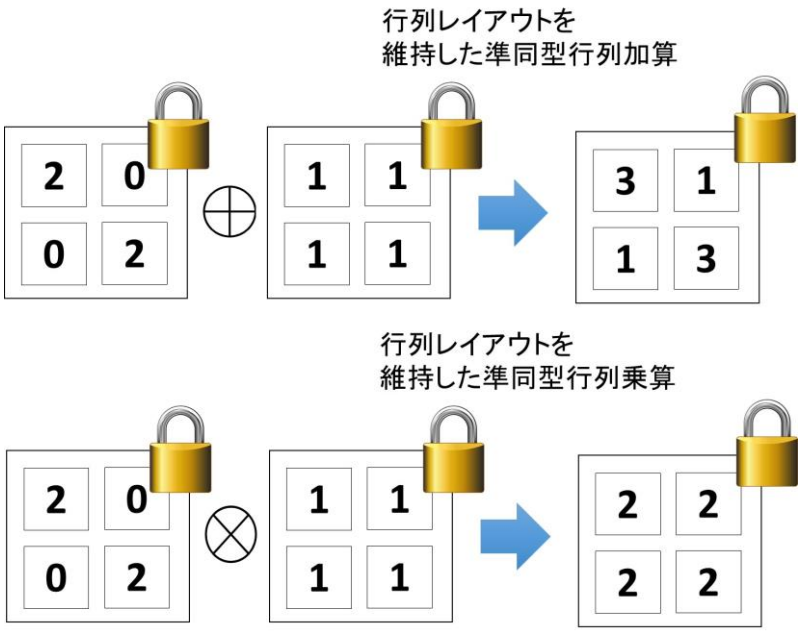

図 2　行列レイアウトを維持する行列準同型加算と行列準同型乗算

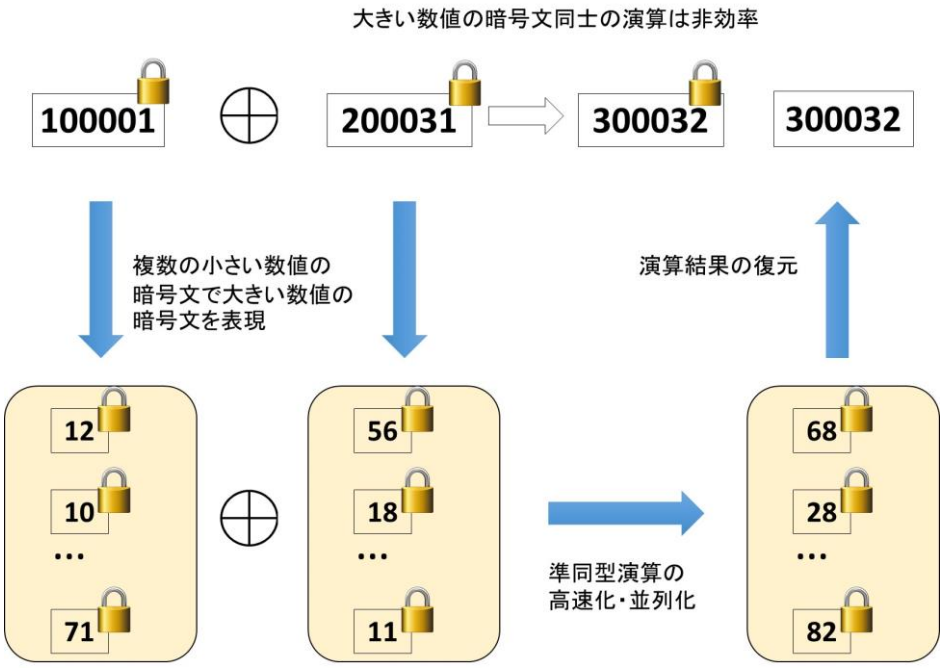

図 3　複数の準同型暗号を用いた任意精度をもつ数値行列の暗号文の実現

参考文献

＊Craig Gentry, Fully homomorphic encryption using ideal lattices. The 41st ACM Symposium on Theory of Computing（STOC 2009), pp 169-178.

掲載論文

【題　名】Using Fully Homomorphic Encryption for Statistical Analysis of Categorical, Ordinal and Numerical Data
（完全準同型暗号を用いたカテゴリカル･順序･数値属性データの統計解析）

【著者名】Wen-jie Lu, Shohei Kawasaki, Jun Sakuma

【掲載誌】Proceedings of The Network and Distributed System Security Symposium 2017

問合わせ先

【研究に関すること】

佐久間　淳（サクマ　ジュン）

筑波大学　システム情報系　教授

【報道に関すること】

筑波大学　広報室

Tel: 029-853-2039　Fax: 029-853-2014

Email: kohoshitu@un.tsukuba.ac.jp

科学技術振興機構　広報課

Tel:03-5214-8404　Fax:03-5214-8432

E-mail:jstkoho@jst.go.jp