情報通信

ビッグデータの有効活用とプライバシー保護を実現する個人制御可能な秘匿計算システム

An individual controllable secrecy computation system realizing effective use and privacy protection of big data

岩村　恵市　Keiichi IWAMURA　（東京理科大学　工学部第一部　電気工学科　教授）

研究の目的

現在の技術におけるキーワードの一つにビッグデータの有効活用があります。しかし、ビッグデータの中には個人情報や機密情報を含むため、プライバシー保護と両立できる必要があります。それを実現する技術の一つが秘匿計算ですが、データを秘匿したままで処理を行うため一般に処理が重く、かつデータが膨大であるため容易に利用できません。そこで、スマートフォンなどでも制御可能な手法を研究しています。

研究の概要

クラウドにデータを預ける利用者はデータ保護のため暗号化などを行いますが、それを利用するときはデータを自ら復号して元に戻す必要があり、クラウドに処理を任せることはできませんでした。近年、秘密分散法を用いてデータを秘匿しながら、その秘匿データを使ってクラウドに各種処理を実行させる秘匿計算に関する研究が盛んに行われています。しかし、1つの事業者にクラウドの管理を委託する場合、秘密分散された分散情報を集められ、秘匿したデータが復元されるかもしれないという不安から利用者は逃れられません。よって、利用者が管理する情報がなければ秘密分散法を用いた秘匿計算できないシステムを提案します。利用者はデータが膨大であっても鍵を1つ管理するだけで、システムは高速な秘匿計算を実現します。

スマートフォンを用いたライフログシステム

軽量&小容量なのでスマートフォンで自分の記録（ライフログ）を秘匿管理するアプリケーションが可能

POINT

- 膨大なデータを記憶することなく秘密鍵から生成
- 加減算のみで実現可能な高速な秘密分散処理
- 秘密情報のオーナが秘匿計算を制御可能

従来・競合との比較

- サーバが管理するはずの膨大なデータを鍵情報1つに集約でき、利用者が管理できます
- 加減算のみで分散・復元処理が可能な高速な秘密分散法を提案しています
- 利用者は鍵を1つ管理するだけなので、スマートフォンなどによる秘匿計算が可能です

想定される用途

- 家計簿のネット管理（個人情報である金額を秘匿したまま平均や合計等の処理可能）
- ライフログアプリケーション（スマートフォンによりデータが発生する毎に分散・秘匿演算・復元処理可能）
- 医療分野などで個人情報を秘匿したまま統計処理（記憶容量削減と統計処理の両立）

実用化に向けた課題

四則演算に関する基本演算は実現できていますが、具体的な演算等（演算の連続や特殊な演算など）に対する実用性の検討が必要です。

企業へ期待すること

本研究を具体的なアプリケーションに適用したいと思う企業の方はお声をかけてください。

今後の展開

2015年10月	ｺﾝﾋﾟｭｰﾀｾｷｭﾘﾃｨｼﾝﾎﾟｼﾞｳﾑ2015でデモ展示
2016～2017年	秘匿計算に関する研究
2018年～	秘密分散と秘匿計算の実用化に向けた検討

■ 関連制度：科学研究費助成事業　基盤研究（C）
■ 知的財産権：特願2018-175393「生成装置、復元装置、送信装置、受信装置、生成プログラム、復元プログラム、送信プログラム、及び受信プログラム」
特願2018-185931「分散装置、秘匿演算装置、検証復元装置、分散システム、秘匿演算検証復元システム、及びプログラム」
■ 受賞歴：情報処理学会フェロー

東京理科大学 研究戦略・産学連携センター

〒162-8601　東京都新宿区神楽坂一丁目3番地　TEL：03-5228-7440　E-MAIL：ura@admin.tus.ac.jp

2015.08
（2018.11）