秘密計算による秘密データ利活用の社会応用にむけて

筑波大学 大学院システム情報工学研究科, JST CREST 佐久間 淳

複数の異なるエンティティがそれぞれ他のエンティティに明かすことができない秘密情報を保持しているとしよう. 秘密計算とは, これらの秘密情報をどれか一つのエンティティに集約させて初めて可能となる計算を, これらを集約・共有せずに実現する暗号理論を利用した計算技術である. 秘密計算とは暗号理論分野において長い歴史を持ち 精緻に理論化された研究分野であるが, 実際の社会における応用例はこれまでのところさほど多くない. 私たちの研究グループは, 2009 年度-2012 年度において JST さきがけの「知の創成と情報社会」領域において秘密計算に関するアルゴリズム開発や開発環境の整備を行った. またその発展として, 2013 年度から開始された JST 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」領域において, 高機能暗号を用いた秘密計算における自己情報コントロール機構の構築を行うとともに, その応用領域を個人ゲノムに定め, 秘密計算を活用したプライバシ保護個別化医療とゲノム疫学におけるフィージビリティスタディを目指している. 本講演では, これまでに共同研究者[1]とともに研究開発した以下の 3 つの成果について紹介する. まず, さきがけ研究における理論的成果としてグラフのプライバシを保護した PageRank 計算法である PrivateRank を, 開発上の成果として Android 端末上で秘密計算を行うための開発環境 FairyRing を紹介する. また CREST 研究において目指している個人ゲノムを用いた秘密計算の基礎技術の一つとして, 秘密パターン照合法を紹介する.

ユビキタス秘密計算環境 Fairy Ring. 個人がカジュアルな用途に手軽に秘密計算を利用できるように, Android 端末などスマートフォンをインターフェースとした, 秘密情報を含む多人数間の意思決定を実現するためのフレームワークを紹介する. このフレームワークは, 加法準同型暗号をビルディングブロックに用いたマルチパーティ秘密計算を提供する. 高い性能を持たない計算機でも秘密計算が利用できるように, 攻撃者は semi-honest に振る舞うなどの強い仮定を置き, この状況の下で加法準同型暗号を用いた秘密計算をスマートフォン上で提供する. このフレームワークでは, 統計計算や投票などいくつかの秘密計算の実装例を持つ. 講演では秘密安定結婚問題の実装とその結果について述べる.

秘密グラフにおけるリンク解析法 PrivateRank. リンク解析とは互いにリンクされたエンティティのリンク構造から有用情報の抽出を目指すアルゴリズムである. 特に PageRank はハイパーリンクを持つ Web 文書のランキングに実際に利用され, 有用性が知られる. PrivateRank とは, 各ノードが秘密情報をもつエンティティからなるグラフ (秘密グラフ) において, その秘密を互いに明かさずにリンク解析を行うアルゴリズムである. 秘密グラフの例として, 企業間の取引関係 (取引=リンク, 取引額=重みが秘密) や電話やメールによる通信関係 (通信=リンク, 通信頻度=重みが秘密) や評価する人・評価される人を匿名化するダブルブラインドレビュー (評価関係=リンク, 評価値=重みが秘密) などが挙げられる. 講演では, PrivateRank の概念を紹介し, これを物理侵入者検出や性病感染可能性検出に応用した結果について述べる.

秘密パターン照合 SPM. パターン照合とは, 正規表現など特定の規則に従って記述された文字列のパターンが, 与えられた文字列中に存在するかどうかを判定する問題である. この研究では, あるパーティーが秘密の文字列を持ち, 別のパーティーが秘密のパターンを持つときに, 秘密文字列と秘密パターンを互いに明かすことなく, パターンの存在性のみを判定する秘密パターン照合を紹介する. 応用例の一つとして, DNA による疾患判定が挙げられる. 特定の疾患と関連のある塩基配列パターンを保持するサービス提供者が, 個人が持つ DNA を用いて疾患の事前診断を行う例を考える. この場合, サービス提供者にとって塩基配列パターンを公開することはサービスの運営上好ましくなく, また個人が持つ DNA をサービス提供者に公開することはプライバシ保護の観点で問題がある. 秘密パターン照合は, 互いの持つデータを互いに秘匿しつつ, DNA 所有者は自身の DNA に, サービス提供者が持つパターンが含まれるかを照合することができる. 講演では, 秘密パターン照合法のアルゴリズムを紹介し, テスト実装の結果および既存研究との比較について述べる.

[1] 青木良樹, 照屋唯紀, 荒井ひろみ, 小林重信, 原田弘毅, 笹川裕人, 有村博紀 (順不同, 敬称略)