氏　　名	Md. Nurul Huda
学位（専攻分野）	博士（情報学）
学位記番号	総研大甲第1054号
学位授与の日付	平成１９年３月２３日
学位授与の要件	複合科学研究科　情報学専攻 学位規則第６条第１項該当
学位論文題目	A Mobile Agent-based Privacy Protection Mechanism in Solving Multi-party Computation Problems
論文審査委員	主　査　教授　山田　茂樹 教授　曽根原　登 助教授　計　宇生 助教授　岡田　仁志 教授　川原崎　雅敏（筑波大学）

論文内容の要旨

The proliferation of the Internet has opened the opportunities for automated cooperative computation, where people are cooperating with each other to conduct computation tasks based on the inputs they each supplies. These computations could occur between trusted parties, between partially trusted parties, or even between untrusted parties. Usually, to conduct these computations, one must know inputs from all the parties; however if nobody can be trusted enough to know all the inputs, privacy will become a primary concern. The primary goal of this research work is to find a mechanism for protecting private (input) data while solving multi-party computation problems (MPCPs) without having too much complexity. The mechanism should not be application-specific so that it can be applied for many applications. In addition, it should not incur very high performance penalties in other important considerable factors (e.g., computational time), which might make it impractical.

A multi-party computation (MPC) allows n parties to compute an agreed-upon function of their inputs and every party learns the correct function output. To solve an MPCP, the participants may need to share their private data (inputs) between one another, resulting in data privacy loss. The key research issue that has been addressed in this thesis is - how to solve multi-party computation problems without disclosing anyone's private data to others.

Firstly, by studying and analyzing the traditional computational models, we have devised a privacy loss model for multi-party computation problems and proposed a novel metric, called the Min privacy metric, for quantitatively measuring the amount of data privacy loss in solving the MPCPs. Then, we have presented a mobile agent-based scheduling algorithm that applies pseudonymization technique to reduce data privacy loss. Finally, we have proposed the security system design, including security policies and security architecture, of an agent server platform for enhancing data privacy protection while solving the MPCPs.

The privacy loss model has identified three factors affecting the amount of privacy loss in solving the MPCPs:

(1) the fraction of private data which is shared with others,

(2) the probability of associating the shared private data with the data subject, and

(3) the probability of disclosing the shared private data to unauthorized parties.

Privacy loss can be reduced by any mechanisms which reduces the values of any of the three factors. The proposed Min privacy metric accounts for the number of participants that lose their private data and the amount of private data disclosed to unauthorized parties, regardless of how many parties they are revealed to.

Existing scheduling algorithms aim for a global objective function. As a result, they incur performance penalties in computational complexity and data privacy. This thesis describes a mobile agent-based scheduling scheme called Efficient and Privacy-aware Meeting Scheduling (EPMS), which results in a tradeoff among complexity, privacy, and global utility for scheduling multiple events concurrently. We have introduced multiple criteria for evaluating privacy in the meeting scheduling problem. A common computational space has been utilized in EPMS for reducing the complexity and the privacy loss in the scheduling problem. The analytical results show that EPMS has a polynomial time computational complexity. In addition, simulation results show that the obtained global utility for scheduling multiple meetings with EPMS is close to the optimal level and the resulting privacy loss is less than for those in existing algorithms.

Cryptography-based algorithms for MPCPs are either too complex to be used practically or applicable only to the specific applications for which they have been developed. In addition, traditional (non-cryptography-based) algorithms do not provide good privacy protection for MPCPs. We have proposed a novel privacy protection mechanism in which MPCPs are solved by

mobile agents using traditional algorithms at an agent server platform, called isolated Closed-door One-way Platform (iCOP). The participating mobile agents are trapped into iCOP where they are allowed to share their private information to solve the problem using traditional algorithms. However, they are protected from disclosing the shared private information to the outside world. The enforcement of the security policies protects the participating agents from sending anything other than the computational result to the users. The security and privacy analysis illustrates that the proposed mechanism provides very good privacy protection if the participants solve the problem with distributed algorithms and can provide complete privacy protection if the participants exchange inputs within the iCOP and each of them solve the problem with centralized algorithms. Finally, experimental evaluation shows that the proposed agent platform security system significantly enhances privacy protection while solving many MPCPs with traditional algorithms.

論文の審査結果の要旨

本博士論文は、複数人が存在する環境下で各人の個人データを入力として一つの問題を解く「複数者計算問題(MPCP: Multi-party Computation Problem)」に関して、各人の個人データを互いになるべく見せずに処理を実現するプライバシー保護アルゴリズムとプライバシー保護アーキテクチャに関する研究成果をまとめたものである。本論文による技術的な貢献内容は(1)MPCP 用プライバシー流出モデルの提案、(2)プライバシー流出の新しい評価尺度 Min Metric の提案、(3) MPCP の典型である会議スケジューリング問題に対するプライバシー流出の少ないスケジューリングアルゴリズム EPMS(Efficient and Privacy-aware Meeting Scheduling Scheme)の提案、(4) モバイルエージェント用サーバ支援型プライバシー保護機構 iCOP (isolated Closed-door One-way Platform) の提案である。本論文は 7 章より構成されている。

本論文の第 1 章では MPCP におけるプライバシー問題を分析している。MPCP は各人の個人データを入力として解を求めていく問題なので、データプライバシーの保護が求められる環境でどのようにして他人に個人データを見せずに処理をいくかが重要な課題である。

第 2 章では関連する従来技術とそれらの問題点を述べている。従来技術として暗号化したまま処理をする方法(cryptographic approach)は汎用性に欠け、それ以外の方式 (non-cryptographic approach : 集中型、分散型) でも個人データの共用使用を減らす試みが種々行われているが、有効なものが少ない。

第 3 章ではプライバシー流出への影響要因を整理した新しいプライバシー流出モデルとプライバシー流出評価尺度 Min Metric を提案している。本プライバシー流出モデルの特徴は個人データの所有者、データ使用者、第 3 者に分けてプライバシー流出要因を明確にした点にある。Min Metric は流出した個人データの取りうる状態の数には依存するが、従来と異なり、流出データの受信者の数には依存しない流出評価尺度である。

第 4 章では会議スケジューリング問題を定式化した後、スケジューリングアルゴリズム EPMS を提案し、そのプライバシー流出度、計算の複雑度と計算コスト等を理論計算とシミュレーションによって求め、分析、評価している。EPMS は共通の計算空間上で個人データを集めて計算する際に処理順序にランダム性を導入して一種の匿名化を施したアルゴリズムなので、プライバシー流出量が一般的に少ないことが定量的に示されている。

第 5 章ではモバイルエージェント用サーバ支援型プライバシー保護機構 iCOP を提案し、その詳細を述べるとともにセキュリティとプライバシー面の分析を行っている。また、シミュレーションとプロトタイプシステムによる実測を通してそのプライバシー流出度を従来型機構のものと比較し、iCOP の有効性を定量的に示している。iCOP では各人が自分の個人データを含んだモバイルエージェントを、アクセス権に基づきコントロールされる共通エージェントプラットフォーム(iCOP)に送り込む。iCOP 内でモバイルエージェントはローカルな通信で個人データを交換ながら処理を進める。共通エージェントプラットフォームは各エージェントの計算結果を比較することで秘匿

チャネル経由でデータ流出するのを防ぐとともに、エージェントがモバイルエージェントの代わりに計算結果を個人に返すことで強固なプライバシー保護を実現している。

第6章ではEPMSとiCOPのアプリケーションについて議論している。特にiCOPはプライバシー保護を必要とするデーマイニングやデータベース検索等の分野でも適用可能である。

第7章で結論と将来課題をまとめている。

出願者は、本研究に関わる査読付きジャーナル論文と国際会議論文にそれぞれ1件と5件の発表を行っており、さらに査読付きジャーナル論文1件を投稿中である。

試験は、出願者に提出博士論文の内容の発表をしてもらい、論文内容を中心に、これに関連した分野ならびに基礎知識の内容も含め、審査委員全員からの口頭試問で行った。これらの質疑応答を通して、出願者から納得できる回答を得ることができた。

本論文の提案内容は、新規性、有効性、信頼性が十分に備わっており、また学術的価値も十分に認められる。さらに最近はプライバシー保護が社会や産業界における大きな関心事となり、法制度面の整備だけでなく、有効なプライバシー保護技術の研究開発が強く求められていることから、産業界や社会への貢献も十分に期待できる。

以上により、本学位請求論文が複合科学研究科における博士授与の基準に達していると判断し、合格とした。