科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　　５　日現在

機関番号：　１２１０２
研究種目：　若手研究(B)
研究期間：　2012～2013
課題番号：　２４７０００２２

研究課題名（和文）論理推論を基にした合理的秘密分散プロトコルの安全性検証法の構築

研究課題名（英文）Logical verification method for rational secret sharing protocols

研究代表者
長谷部　浩二（Hasebe, Koji）

筑波大学・システム情報系・助教

研究者番号：８０４７００４５

交付決定額（研究期間全体）：（直接経費）　　3,400,000円、（間接経費）　　1,020,000円

研究成果の概要（和文）：本研究課題は，合理的秘密分散プロトコルの安全性を検証するための論理推論体系の構築を目的として遂行された．この目的を実現するためのアプローチとして，ネットワーク参加者らの知識に関する推論やプロトコルの実行過程を，一階述語論理や知識論理をもとにした論理言語によって表現する方法が採用された．また，プロトコルの実行過程を対象とするモデルを与え，先に与えた論理体系に対する健全性が検討された．

研究成果の概要（英文）：We developed logical inference systems for rational secret sharing protocols. The key idea behind our systems was to use the first order logic and modal epistemic logic to describe inferences of each participant and execution processes of a protocol. We also considered a model as the set of traces of a protocol and showed soundness with respect to our systems.

研究分野：　形式手法

科研費の分科・細目：　情報学・ソフトウェア

キーワード：　数理的技法　安全性検証　秘密分散プロトコル　論理推論体系

１．研究開始当初の背景

本研究の対象とする秘密分散プロトコルは，暗号プロトコルの一種であり，ある秘密情報を複数人で共有するためのものとして知られている．こうした暗号プロトコルの安全性に関するこれまでの研究の中心的課題は，悪意ある攻撃者がネットワークに存在することを仮定し，その中で情報漏洩や成りすましなどが不可能であることを示すというものであった．しかしながら近年，秘密分散プロトコルの安全性に対する新しい考え方が Halpern らによって提起され，盛んに議論されるようになった．すなわち，秘密分散プロトコルにおいて，参加者が正直に自分のシェアを申告することで利得が最大になるようにし，利得を最大化しようとする利己的な参加者に自主的に申告させるというものである．Halpern らによって，こうした意味での安全性を考慮した秘密分散プロトコルとして，合理的秘密分散プロトコルが提案され，その後，ゲーム理論においてメカニズムデザインとして知られる研究分野の成果をもとに，さまざまな観点からの改良や拡張が試みられてきた．

一方，ゲーム理論の分野では，利得を最大化するための合理的な意思決定過程を分析するための方法として，数理論理学を用いる研究が数多くなされてきた．こうした分析手法の目的は，プレイヤーがゲームを遂行する際にどのような知識を持ち，またその知識から，どのような推論を経て意思決定を行うのかを，論理推論によって定式化することにある．代表者らも，これまでに public announcement logic と呼ばれる体系を基にした分析手法や，belief revision と呼ばれる論理的枠組みを用いた分析手法を提案していた．しかしながら，こうした分析手法の研究は，経済学や数理論理学の範囲に比較的限定されており，情報科学のとりわけ暗号プロトコルの分野への応用は，未だ十分になされていなかった．

２．研究の目的

本研究課題は，合理的秘密分散プロトコルを検証するための数理的技法（フォーマルメソッド，形式手法）の構築を目的とするものである．

特に，プロトコル参加者の利己的な振る舞いを仮定した上での安全性を，論理体系によって証明する方法の提案を目指して遂行された．そのための方法として，本研究では，これまでゲーム理論の分野で研究されてきたプレイヤーの合理性に関する論理的分析手法を応用するというアプローチが採用された．また，本研究によって考案された検証法に関し，他のプロトコルへの適用可能性や，安全なプロトコルの設計への応用について検討することも目指した．より具体的には，以下で挙げる三つの課題の達成を目標とした．

第一の目標は，合理的秘密分散プロトコルにおける各参加者の推論を論理体系によって定式化し，さらにその体系を用いて「各参加者が自らの利益を最大化するように振る舞うと，必然的にプロトコルに従った行動を取る」という安全性命題の証明法を構築することである．また第二の目標は，以上で得られた安全性証明の手法を，秘密分散プロトコルと密接に関連するマルチパーティプロトコルなどの検証に対しても適用し，その有効性を示すことである．さらに第三の目標は，上記で得られた検証法を利用して，安全なプロトコルの設計を行うことである．これは，従来想定されていたよりも攻撃的な振る舞いをする参加者の存在を仮定し，その下で安全であるようなプロトコルの設計を行い，その安全性を示すというものである．

３．研究の方法

プロトコルの実行過程は，典型的なゲーム論的状況である．すなわち，他の参加者がシェア（分割された秘密情報）を送るか否かに応じて自らの利得が変化し，また自らの行動が他の参加者のそれぞれの利得に影響する状況となっている．こうした状況を論理体系で定式化するには，他の参加者の行動を推測して自らの利益を最大化させるような意思決定過程を論理言語によって記述することが必要となる．そのために，まず各参加者の持つ利得関数（プロトコルを実行し終わった時に得られる利得を定める関数）や，コイン投げの結果や，シェアの送付の有無を論理式として表現することが必要である．また，これらの事実に関して各参加者がどのような知識を持っているのかといった情報や，さらには「他の参加者が知っていることを別の参加者が知っている」といった知識に関する表現も必要となる．これらの事柄を論理式として表現できる体系として，知識論理が知られている．知識論理は，こうした知識に関する命題を，必然性を表す様相概念によって表現することができる．また一方で，このプロトコルの実行過程においては，シェアの送付や各自のコイン投げの結果を他の参加者に伝えるといった情報交換があるため，これを論理言語で表現することも必要となる．以上で述べた要請を満たすものとして，本研究課題では，代表者らによって提案された public announcement logic をもとにした体系を採用するという方針がとられた．Public announcement logic は知識論理に情報伝達を表す様相を加えた論理体系である．これにより，上述の事柄が論理式で記述され，また各参加者の行う推論が証明図として表現され，最終的にプロトコルのルールを表す論理式の集合から安全性を表す命題である「各参加者が自らの利益を最大化するならば，プロトコルに従った行動を取る」ことが証明される．以上が最も自然と考えられる定式化の方法である．しかしながら，ここでは検証に向い

たより簡潔な体系を得るために，知識の概念を用いない通常の一階述語論理による定式化なども併せて試みることが計画された．

以上で得られた論理体系を基にして，初年度の後半では，Halpern らのプロトコルの後継となる種々の合理的秘密分散プロトコルに対する安全性検証法の構築を目指した．その対象として，本研究では特に，非同期的な通信を考慮したものや，プロトコルの繰り返し実行を考えたもの，あるいは非同期通信を配慮した上で送信メッセージ数の削減を行ったものなどを対象として考えている．当年度は，これまでに得られた合理的秘密分散プロトコルの検証手法を，合理的マルチパーティプロトコルに対して適用することが計画された．先述のように，このプロトコルは合理的秘密分散プロトコルと密接に関連したものである．ここではまず，参加者の利己的な振る舞いに関して比較的単純な仮定を置いた合理的マルチパーティプロトコルを対象として，さらに複雑なものへと発展させる方針によって研究が行われる．マルチパーティプロトコルにおける安全性についての最近の研究を対象とすることが計画された．特に，必ずしも自らの利得を最大化するとは限らない，完全に自由に振る舞う悪意ある攻撃者の存在を仮定した上での安全性が議論された研究があり，こうした参加者の振る舞いが他の参加者に及ぼす影響を，各参加者の知識を分析することにより明らかにすることを目標とした．

４．研究成果

平成 24 年度は，Halpern らによって最初に提案された最も基本的な合理的秘密分散プロトコルを対象に，その分析を行うための論理推論体系の構築を行った．そのためにまず，ネットワークにおける他の参加者の行動を推測して自らの利益を最大化させるような意思決定過程を，論理言語によって記述することを目標とした．より具体的には，各参加者の持つ利得関数やコイン投げの結果，さらにはシェアの送付の有無を論理式として表現し，また，これらの事実に関して各参加者が持つ知識や，さらに他の参加者の知識に関する表現を行いうる論理体系の構築を行った．平成 24 年度は，主に知識論理を用いて研究が遂行された．また一方で，このプロトコルの実行過程においては，シェアの送付や各自のコイン投げの結果を他の参加者に伝えるといった情報交換があるため，これを論理言語で表現することも必要となる．以上で述べた要請を満たすためのものとして，本研究課題では，代表者らによって提案された public announcement logic の派生体系を基に行った．また，プロトコルの実行過程のモデルを定式化し，先に与えた論理推論体系に対する健全性を検討した．

続く平成 25 年度は，先述の代表者らによる public announcement logic の派生体系を用いた論理体系の構築を目指し，研究が遂行された．特に，合理的秘密分散プロトコルにおけるコイン投げの結果などの確率論的概念の表現などを対象に研究を進めた．そのためのアプローチとして，平成 25 年度は動的様相を用いない代わりに一階述語論理を用いた言語による定式化を試みた．本研究中心課題である合理的秘密分散プロトコルの安全性検証法については，研究課題期間中にその成果を査読付き媒体にて発表するまでには至らず，現在，国際会議論文としてまとめ，投稿の準備をしている段階である．しかしながら，先述の確率論的概念の定式化の研究を通じて，本研究課題に関連する暗号プロトコルの確率論的・計算論的な安全性証明を行うための論理体系を考える上でも有用であることが分かり，その研究成果を国際会議や国内の研究集会などで発表した．また，それまでに得られた論理体系は，合理的秘密分散プロトコルの安全性証明のみならず，1980 年代後半に暗号プロトコルの安全性証明手法として考案された BAN 論理の元々の意図を，public announcement logic や dynamic epistemic logic などを用いて再構成するというアイデアを得ることができた．今後の研究の展開として，こうしたアイデアをもとに，合理的秘密分散プロトコルを含めたより一般的な暗号プロトコルを対象に，ネットワーク参加者らの知識の形成過程と安全性との関係を論理推論体系によって明らかにすることを計画している．また，当初計画されたマルチパーティプロトコルの安全性検証法については，研究課題期間中に十分検討することができなかった．今後は，こうした合理的秘密分散プロトコル以外の種々のプロトコルに対する安全性検証法についても研究を継続する予定である．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計１件）

① Gergely Bana, Koji Hasebe, and Mitsuhiro Okada. Computationally Complete Symbolic Attacker and Key Exchange. Proceedings of the 20th ACM Conference on Computer and Communications Security (ACM CCS 2013), 査読有. 2013. pp. 1231-1246. DOI: 10.1145/2508859.2516710.

〔学会発表〕（計２件）

① バナ・ゲルゲイ, 長谷部浩二, 岡田光弘. 計算論的に完全な記号的攻撃者と鍵交換に関する分析手法. 暗号と情報セキュリティシンポジウム. 2014 年 1 月 21 日～24 日. 鹿児島.

② Gergely Bana, Koji Hasebe, and Mitsuhiro Okada. Computationally

Complete Symbolic Attacker and Key Exchange. 20th ACM Conference on Computer and Communications Security (ACM CCS 2013). November 4-8, 2013. Berlin, Germany.

６．研究組織

(1)研究代表者

長谷部　浩二（HASEBE, Koji）
筑波大学・システム情報系・助教
研究者番号：８０４７００４５