様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年５月１５日現在

機関番号：12102
研究種目：若手研究(B)
研究期間：2009 ～ 2011
課題番号：21700023
研究課題名（和文）　論理推論を基にした暗号プロトコルの計算論的安全性検証法の構築

研究課題名（英文）Computational Logical Verification Method for Cryptographic 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

研究成果の概要（和文）：本研究を通じ，研究代表者は先に提案された Basic Protocol Logic と呼ばれる一階述語論理を拡張し，暗号プロトコルの計算論的安全性を検証するための論理体系を構築した．これは，Basic Protocol Logic に対し，確率暗号における計算論的概念を導入したものである．また，この論理体系が健全となるような計算論的意味論を与え，Needham-Schroeder プロトコルなどの秘匿性証明に適用可能であることを示した．

研究成果の概要（英文）：We developed an extended inference system based on Based Protocol Logic (BPL), a variant of first order logic for proving correctness of cryptographic protocols. This extended system was obtained from BPL by adding some computational aspects of cryptography and sound with respect to a computational semantics. We also demonstrated the usefulness of this system by proving secrecy property of some protocols, such as Needham-Schroeder protocol.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,600,000	480,000	2,080,000
2010 年度	1,000,000	300,000	1,300,000
2011 年度	800,000	240,000	1,040,000
総　計	3,400,000	1,020,000	4,420,000

研究分野：数理的技法
科研費の分科・細目：情報学、ソフトウェア
キーワード：仕様記述・仕様検証

１．研究開始当初の背景

論理推論やモデル検査などの数理的技法による暗号プロトコルの安全性検証法は，これまで BAN 論理を端緒に，数多くの方法が提案されてきた．その中でも特に本研究と関連の深い論理推論を基にした検証法としては，BAN 論理をはじめ，John Mitchell らの研究グループによる Protocol Composition Logic（PCL），また研究代表者らによって先に提案された Basic Protocol Logic などが挙げられる．これらの論理推論を用いた検証法に共通する基本的なアイデアは，まずプロトコルに対する攻撃者の振舞いを含んだ全ての実行トレースを枚挙した通信モデルを与え，さらにこのモデル上で成り立つ種々の性質に関する推論を，論理推論体系によって定式化するというものである．これにより，暗号プロトコルの安全性は，この論理体系の形式的な証明によって示すことができる．こうした数理的技法を用いた検証法には，厳密かつ（半）自動的な安全性証明が可能になるという利点があるものの，そのほとんどが，プロトコルで使われる暗号自体が絶対に破られないことを前提としたモデルを基にしてい

るため，暗号の特徴を利用した攻撃を発見できないという欠点がある．一方，暗号理論の研究分野では，数理的技法による検証法とは独立に，計算論的アプローチによる暗号プロトコルの安全性証明手法が確立されてきた．こうした計算論的手法は，暗号の脆弱性を考慮に入れた解析ができるため，現実的な実装に即したプロトコルの安全性検証が行えるという利点があるものの，安全性証明の議論が非常に煩雑になるという欠点もあった．

以上を背景に，これら二つの安全性証明法の各々の利点を活かしながら両者を融合する試みが，Abadi-Rogaway の研究を端緒に，近年非常に盛んに行われてきた．その代表的なものの一つに，従来の論理推論による検証法で使われてきた暗号の絶対安全性を仮定したモデルを，暗号の脆弱性を考慮に入れた計算論的なモデルに拡張するという研究が行われていた．これにより，従来の数理的技法による検証法の利点を活かしながら，暗号の脆弱性を仮定しても成り立つ安全性を形式的に証明することができるようになった．本研究の直接の先行研究でもあるこのような研究としては，先の PCL によるものや，Micciancio-Warinschi による研究などが挙げられる．しかしながら，これらはいずれも明確な論理推論体系を示しておらず，また暗号プロトコルで用いられる確率暗号の特徴を十分に捉えていないという欠点があった．また特に PCL に関しては，その論理体系の複雑さから，証明が煩雑になるという問題も残されていた．そのため研究代表者らは，Basic Protocol Logic のモデルを確率過程の概念による計算論的モデルへと拡張することにより，確率暗号の脆弱性を踏まえた検証をより単純な論理体系で行えることを示した．しかしながらこの検証法では，暗号プロトコルの安全性として認証（authentication）のみしか扱えないという制約など，多くの課題を残していた．

２．研究の目的

本研究は，前述の Basic Protocol Logic の研究成果をより発展させ，暗号の脆弱性に起因する攻撃を十分に扱いうる新しい検証法の構築を目的とした．また特に，直接の先行研究である PCL に比べ，その証明能力に遜色が無く，なおかつより簡潔な証明が行えるような検証法の構築を目指した．そのために，まず理論的方面から，以下で述べるような方針で論理体系の拡張を行い，さらにその成果をコンピュータ上で試作実装することにより，暗号プロトコルの設計・検証ツール開発の足がかりとなるところまで発展させることを目標とした．より具体的には，以下の課題の達成を目標とした．

第一の目標は，これまで研究代表者らによって得られた Basic Protocol Logic を，暗号の脆弱性を考慮に入れた計算論的モデルの下で認証成立以外の安全性に関わる性質を扱えるよう拡張するというものである．特にここでは，通信メッセージの秘匿性（secrecy）を対象とした．これにより，Basic Protocol Logic でこれまで扱えなかった暗号プロトコルの安全性を，暗号の脆弱性に起因する攻撃まで想定した上で検証するための論理推論体系の構築を目指した．ただしこの拡張を行う際に重要となるのは，Basic Protocol Logic の持つ利点である論理体系の単純さを損なわない範囲で（より具体的には，本質的に一階述語論理の範囲を超えないように）行うということである．

第二の目標は， Basic Protocol Logic の枠組みを用いて，プロトコルの拡張や合成に沿った安全性証明手法を確立するというものである．暗号プロトコルの設計ではしばしば，コンポーネントとなる単純なプロトコルを拡張・合成することによって，より複雑なプロトコルを生成することが行われる．そこで，このプロトコルの生成過程にうまく対応させながら，コンポーネントの性質に関する形式証明（証明図）を拡張・合成することによってプロトコルの安全性証明を行うというのが，この拡張・合成による証明手法のアイデアである．

第三の目標は，以上で得られた理論的成果を，Isabelle/HOL などの定理証明支援系を援用することによって試作実装することである．

３．研究の方法

前述の目的を達成するための方法としては，まず，これまで研究代表者らの研究によって得られた Basic Protocol Logic に対して，暗号プロトコルの安全性に関する種々の性質を扱うための拡張を行い，かつその拡張体系の公理系が妥当となるような計算論的モデル（すなわち暗号の脆弱性を考慮したモデル）の構築を目指した．この拡張は，比較的容易であると考えられるものから難易度の高いものへと，段階的に進めた．ここで扱う性質としては，認証成立以外の重要な性質である秘匿性（secrecy）を対象とした．これを実現するための方法として，Basic Protocol Logic の言語に対してメッセージの識別不可能性（indistinguishability）を表す述語の導入を試みた．ここで識別不可能性とは，「与えられた二つの暗号化された通信メッセージについて，攻撃者には元の平文が同一であるか否かを区別できない」ことを意味する概念である．これは，暗号化されたメッセージの秘匿性を，暗号の脆弱性まで考慮

して言明する上で中心となる概念である．このアイデア自身はPCLで既に提案されているものであるが，本研究ではこの拡張を，Basic Protocol Logicが基にしている一階述語論理の枠組みを変えることなく，述語記号のみを導入することにより実現することを目指した．

次に，上記の方法によって得られた論理体系に関する定理として，暗号プロトコルの拡張・合成に沿った安全性証明が，証明図の拡張・合成によって実現可能であることを示すことを試みた．拡張・合成による安全性証明は，PCLの最大の利点であるとともに，Basic Protocol LogicがPCLを簡略化したために犠牲にした最大の課題でもあった．このような安全性証明をBasic Protocol Logic上で実現するための基本的なアイデアは，ある与えられた暗号プロトコルについて，その安全性が常に保存されるようなプロトコルの拡張・合成の一般的な諸規則を定式化することである．すなわち，暗号プロトコルをある規則に従って拡張・合成し，さらにそれに対応するように証明図を拡張・合成すると，そこで得られた証明図が拡張・合成によって得られた暗号プロトコルに関する証明図になるようにするのである．このような暗号プロトコルの合成規則を，論理体系に関するメタ定理として求めるのがここでの課題である．こうした諸規則が得られれば，あとは暗号プロトコルの安全性証明を，その証明図自体の拡張・合成を意識することなく行うことができる．以上のようなアプローチにより，PCLで実現された拡張・合成による安全性証明法が，Basic Protocol Logicにおいても論理体系の簡潔さを失うことなく同様に実現できると考えた．

さらに，以上で得られた理論的成果を基に，前述の理論的な研究を完遂させる一方で，暗号プロトコルの設計・検証のためのツールの実現に向けた試作実装として，Isabelleを使った安全性証明を試みた．

４．研究成果

平成21年度は，研究代表者によって提案された論理推論体系であるBasic Protocol Logicに対し，暗号プロトコルの安全性に関する種々の性質を扱うための拡張を行い，かつその拡張体系の公理が妥当となるような（すなわち推論体系に対して健全である）計算論的モデルを与えた．特に安全性に関する性質として，本年度は特にプロトコルのメッセージに含まれるデータの秘匿性（secrecy）を対象とした．以上の研究によって得られた具体的な成果は以下の通りである．

まず論理推論体系の言語として，プロトコルのメッセージの記号論的表現と計算論的表現の両方を，1階述語論理の項として統一的に与えうる言語を考案した．またこの言語を基に，秘匿性に関連するいくつかの概念を定式化した．さらに，この言語に対する公理系を与え，その中で秘匿性の証明が行えることを，Needham-Schroederプロトコルなどの具体的な暗号プロトコルを例に示すことができた．また，この秘匿性の証明を補題として利用することにより，合意性（agreement property）を示す方法も考案した．また一方で，以上のことが行いうる公理系に対し，健全な計算論的モデルを与えた．以上の結果は，特に秘匿性を基に合意性を証明しなければならない暗号プロトコルの証明に対しても有効であるという利点を持つ．また，この推論体系が，公開鍵暗号と対称鍵暗号のいずれを基にしたプロトコルに対しても適用可能であることが，先行研究に対する利点であると言える．

一方，ここで得られた推論体系は，上記のような証明が行える一方で，言語の表現力の高さから証明が複雑になるという欠点を持っていたため，次年度以降で，この欠点を改善するために，安全性証明を行う上で有用でかつ汎用性の高い補題を見出すことを課題とした．

平成22年度は，前年度に引き続き，暗号プロトコルの安全性に関する種々の性質を扱うための拡張を行い，かつその拡張体系の公理が妥当となるような（すなわち推論体系に対して健全である）計算論的モデルの構築を行った．特に前半では，Gergely Bana氏らの協力のもとで，国際会議での発表を目指し，前年度までに得られた論理推論体系とそのモデルを論文として取りまとめを行った．その論文は，Computer Security Foundations Symposium 2010への投稿を行ったものの，不採録となった．その際に査読者に指摘された問題点は，研究代表者らの提案する推論体系が十分簡略化されておらず，実際のプロトコル証明への適用が難しいということであった．

以上をふまえ，平成22年度の後半は，再度国際会議への投稿を目指し，それまでに得られた論理推論体系の簡略化の作業をBana氏らと共同で行った．また，Bana氏の日本滞在期間中に，プロトコル合成による検証法の構築や，定理証明支援系Isabelleを用いた推論体系のプロトタイプ実装の作業にも着手した．これらの成果を論文としてまとめ，European Symposium on Programming 2011に投稿したものの，不採録となった．この結果から，推論体系の簡略化をより一層進める必要のあることを認識し，これまで採用してきた安全性に関わる述語記号に新たな種類のものを加える検討を進めた．

平成23年度は，引き続き，これまでに得

られていた論理体系の簡略化を目指して研究を行った．そのための方針として，前年度までに得られた論理体系において使われていた原子述語の改良と，それによる公理と計算論的モデルの構築を進めた．また一方で，改良された体系を定理証明支援ツールのひとつである Isabelle を用いた証明の半自動化を試みた．以上の成果は，主に Bana 氏らの協力の下で進められ，再度国際会議への論文投稿を行ったものの，不採録となった．その理由としては，改良された論理体系は，計算論的安全性証明の手法としては意義のあるものであるが，実際の安全性証明への適用のためには，さらに簡略化が必要であるというものであった．平成 23 年度の後半では，簡略化のために，これまで採用してきた一階述語論理を基にするアプローチの他に，新たに動的論理（Dynamic Logic）などの枠組みを用いた公理化なども試みてみたが，十分な簡略化された体系を得ることができなかった．そのため，一階述語論理の枠組みを維持しながら，安全性証明の対象として，プロトコルの認証に関する性質のみに焦点を絞り，プロトコルで扱われる情報の秘匿性については，論理体系の仮定として扱うという方針で研究を進めており，その成果を論文としてまとめる作業を行った．

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）

〔学会発表〕（計 3 件）

① Gergely Bana, 長谷部浩二, 岡田光弘. 計算論的に健全な一階述語論理による暗号プロトコルの分析. 推理的技法による情報セキュリティ, 九州大学（福岡県）, 2012 年 3 月 8 日.
② Gergely Bana, Koji Hasebe, Mitsuhiro Okada. Secrecy-Oriented Computationally Sound First-Order Logical Aanlysis of Cryptographic Protocols. 6th Workshop on Formal and Computational Cryptography. Edinburgh, UK, July 20, 2010.
③ Gergely Bana, Koji Hasebe, Mitsuhiro Okada. Recent approaches to computational semantics for first-order logical analysis of cryptographic protocols. Computational and Symbolic Proofs of Security, 熱川ハイツ（静岡県）, 2009 年 4 月 9 日.

〔図書〕（計１件）

① 長谷部浩二, 岡田光弘, バナ・ゲルゲイ. セキュリティ・プロトコルの論理的検証法, 萩谷・塚田共編『数理的技法による情報セキュリティ』第 9 章, 185-203 ページ, 2010 年.

〔その他〕
ホームページ等
http://www.cs.tsukuba.ac.jp/~hasebe/

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