氏　　名	閻　靖晨
博士の専攻分野の名称	博士（学術）
学位記号番号	博理工甲第 1129 号
学位授与年月日	平成 31 年 3 月 20 日
学位授与の条件	学位規則第 4 条第 1 項該当
学位論文題目	Improving Formal Analysis Method with Reasoning for Cryptographic Protocols （暗号プロトコルのための推論を用いた形式分析手法の改善）
論文審査委員	委員長　准教授　後藤　祐一 委　員　教　授　吉田　紀彦 委　員　教　授　吉浦　紀晃 委　員　准教授　大久保　潤

論文の内容の要旨

Cryptographic protocols are protocols which perform some security-related functions using cryptography. Flaws of cryptographic protocols will bring serious security problems to the cyberspace application, and even cause the immeasurable loss. Therefore, security analysis of the cryptographic protocols become an indispensable process.

Formal analysis method is used to security analysis for cryptographic protocols. Until now, theorem proving method and model checking method is widely used for formal analysis of cryptographic protocols. These methods can be regarded as proving methods because analysts should enumerate the security properties that a protocol should satisfy and accurately describe these properties as formulas in advance, then prove or check whether the target cryptographic protocol satisfies the formulas or not, thereby verifying whether flaws exist or not. Theoretical limitation of such proving methods is that analysts should enumerate all formulas accurately describe the security properties before they start to verify target cryptographic protocols with the methods and the methods only can verify the security through the enumerated formulas. If the enumeration is not enough, some flaws cannot be detected. However, it is generally difficult for analysts to enumerate the formulas completely.

As an alternative way, a concept of formal analysis method with reasoning has been proposed by Cheng. Analysts do not need to enumerate all the formulas that accurately describe the properties in advance but take the behaviors explicitly and implicitly included in the specifications of cryptographic protocols as premises to perform forward reasoning. By forward reasoning, formulas related to flaws can be deduced and it is possible to deduce the formulas that point to some unknown flaws in principle. Wagatsuma et. al proposed the concrete procedures of formal analysis method with reasoning for key exchange protocols. In the method, analysts formalize the participant's behaviors and an intruder's behaviors to perform forward reasoning, and then analysts analyze the deduced formulas whether successful attacks exist. However, there are still some limitations and problems in the method. First, it cannot analyze the cryptographic protocols except key exchange protocols. Second, there are no clear flaw analysis criteria to accurately analyze whether the deduced formulas are related to flaws of the target protocol. Third, due to the limitations of the intruder's behaviors,

some flaws cannot be detected. Fourth, many tasks in the method need to perform manually that lead to time-consuming and error-prone problems.

This thesis proposes the improving formal analysis method with reasoning for cryptographic protocols and the supporting environment for formal analysis to solve the above limitations and problems. First, we extended the formal analysis method with reasoning to apply to various cryptographic protocols. Second, we proposed the fine-grained flaw analysis criteria to analyze the deduced formulas. Third, we extended the formalization tasks and forward reasoning tasks to detect more types of flaws. Fourth, we proposed the supporting environment for formal analysis. This thesis describes the findings and results obtained through our research on demonstrating the effectiveness of the extended method and the support environment.

The extended formal analysis method can deal with 19 representative cryptographic protocols. As the first step of expansion, we compared 19 representative cryptographic protocols based on participants' number and behaviors and summarized five features of these protocols. Then, we extended the participants' behaviors by adding new rules corresponding to the summarized features. We also proposed a specific procedure to decided how falsified data that an intruder would send. After extending, we performed case studies to verify whether the extended method can be used to detect flaws of various cryptographic protocols. By succeeding in detecting the known flaws of secret splitting protocols, it can be said that the extended method can deal with various cryptographic protocols.

Fine-grained flaw analysis criteria have been proposed to analyze the deduced formulas. First, we defined what is a flaw in a cryptographic protocol and considered the security properties of cryptographic protocols can be used as criteria for testing the security of cryptographic protocols. We have organized six fine-grained security properties of confidentiality, authentication, fairness, non-repudiation, anonymity, and atomicity, and used them as flaw analysis criteria to analyze flaws in cryptographic protocols. We also verified the flaw analysis criteria are capable by analyzing Needham Schroeder protocol and anonymous atomic transaction protocols.

The extended formal analysis method can detect flaws related to not only guessing attacks and external replay attacks but also non-repudiation and fairness. To detect more types of cryptographic protocol flaws, we extended the intruder's behavior to describe guessing attacks and external replay attacks and proposed a new method to perform forward reasoning to test the flaws related to non-repudiation and fairness caused by participants' deception. We also took the Needham Schroeder protocol and ISI protocol as cases to perform security analysis. By the result of analyzing, it is proved that the improved formal analysis method with reasoning is effective to detect the flaws of guessing attacks, external replay attacks and the flaws related to non-repudiation and fairness.

The first supporting environment for formal analysis of cryptographic protocols has been proposed. To resolve the time-consuming and error-prone problems, We developed automated formalization tools and integrated other automated supporting tools so that it can support analysts to perform formal analysis of cryptographic protocols through the whole processes automatically.

論文の審査結果の要旨

暗号プロトコルとは、互いに見えない、知らない、同時に行動できないかもしれない関係者の間に、様々な目的で、情報を安全（公平の意味も含め）に交換するために、暗号を使ってデータをやりとりする規則と手順の組み合わせである。現在の高度情報化社会において、ネットワーク上で情報通信と情報共有を安全かつ公平に行うため、数多くの暗号プロトコルが提案され使用されている。暗号プロトコルの高い情報安全性は、様々な脅威から情報を守り、正当な資格を持つ利用者に対して情報を安全に利用できる「安心感」を与えるために極めて重要なことである。しかし、一部の暗号プロトコルにおいて実際に使用された後、次々と脆弱性が発見され、そのプロトコルを使用したシステムにとって情報安全性の問題になった。従って、様々な暗号プロトコルが情報通信と情報共有に必要な高度な情報安全性を確実に保証しているかどうかについて常に分析し評価しなければいけない。

従来、暗号プロトコルの情報安全性を評価するために、形式分析手法として定理証明やモデル検証がよく利用されてきた。これらの証明的形式分析手法では、攻撃者の攻撃手法や攻撃動作を予め列挙してから、列挙された動作が対象の暗号プロトコルにおいて成立し得ることを証明する。証明的形式分析手法では、原理的に、分析前に列挙されていない動作について検証できない。従って、定理証明やモデル検証のような証明的形式分析手法を用いて、対象の暗号プロトコルが安全であるかどうかを完全に評価するためには、検証すべき動作を予め全て列挙できなければならない。これは、多くの場合、非常に難しいことである。

一方、証明的形式分析手法における上記の原理的な限界と問題点を解決するために、前向き推論を用いて暗号プロトコルにおいて成立しうる動作を全て導出し、その中から、暗号プロトコルの安全性にとって脅威となるものを探し出すという推論的形式分析手法のアイデアが提案された。推論的形式分析手法では、原理的に、分析前に検証すべき動作を予め全て列挙する必要がなく、分析者自身もまだはっきり認識している攻撃手法や攻撃動作を発見することも有り得る。この考えに基づき、鍵交換プロトコルを対象とした具体的な推論的形式分析手法が提案された。しかし、提案手法は暗号プロトコルの一種である鍵交換プロトコルのみに適用可能なこと、また、機密性保持と認証に関する欠陥しか分析できないなど限定されたものであった。

本論文は、暗号プロトコルに関する推論的形式分析手法をより実用的なものとするために、より多くの種類の暗号プロトコル、および、より多くの種類の欠陥を扱える推論的形式分析手法の提案および提案手法の有用性を実証するための事例研究、そして推論的形式分析手法を支援するツールについて、著者の研究を通じて得た知見と成果を述べたものであり、８章から構成されている。

第１章では、本研究の背景、目的、および位置付けについて述べた。まず、暗号プロトコルに関する形式分析手法を概観したうえ、本研究の目的として、より多くの種類の暗号プロトコルを扱えるように従来の推論的形式分析手法を改善すること、また、より多くの欠陥を検出できるようにするため、まず、暗号プロトコルが満たすべき情報安全性特性を明らかにし、各情報安全性特性に関する欠陥を分析できるように推論的形式分析手法を改善すること、そして、事例研究を通じて改善手法の有効性を実証することを定めた。

第２章では、暗号プロトコルに関する形式分析における基本原理、基礎概念と専門用語、および、鍵交換プロトコルのための推論的形式分析手法とその限界について説明した。

第３章では、暗号プロトコルに対する推論的形式分析手法の拡張について述べた。まず、代表的な 19 種の暗号プロトコルを識別できる５つ特徴を明らかにし、それらのうち４つの特徴を記述できるように既存の推論的形式分析手法を拡張した。既存の推論的形式分析手法は大きく分けて形式化、推論、分析の３つのプロセスから成り立っている。今回の拡張では、形式化プロセスに４つの特徴を表す形式的表現を付け加えて、

それら４つの特徴を持つ暗号プロトコルを扱えるようにした。また、改善した推論的形式分析手法の有効性を実証するために４つの特徴をもつ暗号プロトコルである秘密分散プロトコルにおいて、改善した推論的形式分析手法を用いて、既知の欠陥を分析できることを示した。この結果より、従来よりも多くの暗号プロトコルを扱えるようになった。

第４章では、暗号プロトコルが満たすべき情報安全性特性について述べた。鍵交換プロトコルのための推論的形式分析手法は機密性保持と認証に関する欠陥しか分析することができなかった。また、推論によって導出した結論の中から欠陥に関連するものを見つけるための基準も明らかでなかった。そこで、既存の暗号プロトコルの形式分析に関する研究を調査し、暗号プロトコルが満たすべき６つの情報安全性特性、すなわち、機密性保持、認証、公平性保持、否認防止、匿名性保持、原子性保持を明らかにした。また、これらの情報安全性特性が実際に暗号プロトコルの欠陥に関連することを事例をもって示した。

第５章では、推論的形式分析手法で分析できる欠陥の種類を増やす第一歩として否認防止および公平性保持に関連する欠陥を分析できるように推論的形式分析手法の拡張を行い、拡張した手法の有効性を事例研究を通して示した。機密性保持や認証に関する欠陥を分析する際には攻撃者の振る舞いを考慮すれば十分であったが、否認防止に関する欠陥を分析するためには、信頼できる参与者と信頼できない参与者を考慮しなければならない。このため、信頼できる参与者と信頼できない参与者を表す記述、およびふるまいを形式化プロセスに追加した。また、公平性保持のためには、暗号プロトコルに基づく通信が任意のステップで終了したとしても各参与者は同等の秘密情報を保持していなければならない。そこで、推論および分析プロセスの手順を変更し、各ステップにおいて公平性が保持できているかを検討できるようにした。拡張した手法の有効性を確認するため否認防止および公平性保持に関連する欠陥が指摘されている ISI プロトコルおよびそれらの欠陥を含まないプロトコルである CMP1 プロトコルにおいて事例研究を行い、本手法で欠陥を検出できること、誤検出をしないことを示した。この結果より、拡張した推論的形式分析手法によって、４つの情報安全性特性（機密性保持、認証、公平性保持、否認防止）に関する欠陥を分析できることを示した。

第６章では、推論的形式的分析を行う際に分析者の手間を軽減し分析者によるミスを減らすために必要となる暗号プロトコルの形式分析支援環境の必要性とその要求および機能、そして設計を行い、想定利用法を示した。

第７章では、本研究で提案した手法とその支援環境について、健全性の観点から考察し討論した。

最後に、第８章では、本研究で得た成果と知見をまとめ、残された研究課題を示した。

なお、本論文の主な内容は、既に４編の学術論文として、国際学術論文誌（Springer Lecture Notes）（２編）、および査読付きの IEEE 学会国際会議論文集（２編）において公表され、あるいは公表が決定されている。

以上のように、本論文では、暗号プロトコルに関する推論的形式分析手法を実用化するために、適用できる暗号プロトコルの種類および分析できる欠陥の種類を増やすための推論的形式分析手法の拡張を行い、また、拡張した手法の有効性を事例研究を通して示した。これらの研究成果は、情報セキュリティ工学分野にとって新しい知見を示し貢献するものである。従って、当学位論文審査委員会は、本論文が、博士（学術）の学位を授与するに値するものと判定した。