【 81 】

氏名	渡邊 創（わたなべ はじめ）
博士の専攻分野の名称	博士（工学）
学位記番号	第 12829 号
学位授与年月日	平成 9 年 2 月 20 日
学位授与の要件	学位規則第 4 条第 2 項該当
学位論文名	Polynomial Time Verification Methods for the Security of Cryptographic Protocols （暗号を用いたプロトコルに対する多項式時間安全性検証法）
論文審査委員	（主査） 教授 谷口 健一 （副査） 教授 都倉 信樹　教授 藤井 護

論文内容の要旨

コンピュータネットワークにおける電子投票や電子商取引などのサービスでは，不正行為防止やプライバシ保護のため，通信において暗号が用いられる。このようなサービスの通信手順は暗号を用いたプロトコルと呼ばれ，そのプロトコルの安全性を保証することは重要である。

暗号を用いたプロトコルでは，プロトコルで使用する暗号が安全であってもプロトコルに不備があるため，全体として安全でない場合が存在する。そこでプロトコル自体の安全性の議論では，使用される暗号は安全であると仮定する。この仮定の下でプロトコルが安全であるとは，敵対者が盗聴やプロトコルで提供される操作の不正使用を行なっても，秘密情報を手に入れることやデータの改竄を行なうこと等，プロトコルの目的に反する行為ができないことをいう。既に提案されている暗号を用いたプロトコルについて，このような意味での安全性は直観的に明らかでない場合が多い。またほとんどの場合安全であることの証明はなされていない。

これまでに安全性を判定する問題は，項書換え系における二つの項の単一化不可能性の判定問題として定式化され，判定問題は一般に判定不能であることが示されている。安全なプロトルコに対してその安全性を保証することが実用上重要であるが，安全なプロトコルに対し常に安全性を保証できる半判定手続き（以下，安全性検証手続きと呼ぶ）も存在しない。このような理由から，問題が判定可能となるための十分条件，およびその条件の下で安全性判定問題を解く多項式時間安全性判定アルゴリズムが提案されてきた。しかし最悪時間計算量が $O(n^8)$ と大きいため，現実的な時間で安全性を判定できるかどうか明らかではなかった。

本論文の 2 章では，この安全性判定アルゴリズムの計算機上での実現方法，およびアルゴリズムの評価実験について述べる。アルゴリズムは最悪計算量だけに注目し，抽象的な形で提案されていたため，平均時間計算量および平均空間計算量の削減に留意し，アルゴリズムの改良，詳細設計を行なった。この設計に基づいて実現したシステムの有用性を評価するため，現実に提案されているさまざまなプロトコルに対し，安全性の問題を記述し，十分条件を満たすものについてその安全性をシステムを用いて判定した。その結果，単純なプロトコルの場合は数分以下で，比較的複雑なプロトコルの場合でも，約二日で安全性を判定できた。

現実に提案されているプロトコルの安全性の問題では，上述の十分条件を満たさない場合が存在する。特に現実のプロトコルの安全性の問題では，十分条件のうち公理の右線形性のみを満たさない場合が多く存在する。公理の右線形性以外の条件だけでは安全性検証手続きは存在しない。そこで，本論文の3章では公理の右線形性のみを満たしていないプロトコルの安全性の問題について，多項式時間でその安全性を検証する手法について述べる。まず，変数への代入が制限される場合を自然に表現できるように，安全性判定問題に項の型の概念を導入した。この安全性判定問題のもとで，安全性の問題の形式的記述を構文的に十分条件を満たす形に変形するための三つの変形法と，その変形前後の記述間の安全性に関する関係を明らかにした。そしてこれらを用いて安全性を多項式時間で検証する手法を構築した。右線形性以外の十分条件を満たし，かつ，安全なプロトコルであっても，本手法によって検証に成功するとは限らないが，多項式時間で停止するように構成した。本手法で新たに検証可能となった安全性の問題の中には，インターネット上で用いられるネットワーク認証プロトコルである「ケルベロス」のように実用的なプロトコルに対する安全性の問題が含まれており，本手法を用いて「ケルベロス」はこの問題について安全であることを検証することができた。

論文審査の結果の要旨

本論文では，暗号を用いたプロトコルの安全性を形式的に検証する方法について述べている。

2章では，これまでに提案されていた多項式時間安全性判定アルゴリズムについて，平均時間計算量，平均空間計算量の削減に留意し，アルゴリズムの改良，詳細部分の設計を行い，システムを実現している。プロトコルが安全でないときにそのことを検出するのは比較的容易であり，そのためのシステムはこれまでいくつか提案されていたが，ここで構築したシステムのようにプロトコルが安全であることを検証できるシステムは例がない。実現したシステムを用いて，比較的複雑なプロトコルの例についても，約二日という現実的な時間で安全性を判定できた。これにより，最悪時間計算量が $O(n^8)$ であるため実用の問題に適用可能かどうか明らかでなかったその判定法が実際に適用できること，また，その方法に基づいてプロトコルの安全性を検証する有用なシステムが構築できることがわかった。

3章では，これまでに示されていた安全性判定問題が判定可能となるための十分条件のうち，公理の右線形性のみを満たしていないプロトコルに対しても，多項式時間でその安全性を検証する手法を述べている。ここでは，安全性の問題の形式的記述を構文上十分条件のすべてを満たす形に変形するための変形法を三つ提案し，その変形前述の記述間の安全性の保存に関する性質を明らかにしている。そしてこれらを用いて安全性を検証する手法を構築している。本手法を用いて安全性検証に成功するとは限らないが，手続きは多項式時間で停止するように構成されている。現実のプロトコルでは，「ユーザIDを引数の一つとしてそれに依存する複数個の情報を同時に生成する」ような操作が提供されていることがよく見られるが，この操作を定義する公理は右線形性を満たさない。しかしこの問題は，ユーザIDが有限個である場合，本手法で提案した変形法の一つを用いることにより解決できる。本手法で新たに安全性を検証できるようになった問題の一つに，現実に使用されている認証プロトコルである「ケルベロス」があり，本手法を適用して安全であることが確認できた。

以上のように，本論文で述べられている検証手法およびシステムを用いることにより，現実に提案されている多くの暗号を用いたプロトコルに対する安全性保証を形式的に行なうことが可能となる。これはネットワークサービスの安全性保証技術の向上に寄与しており，本論文は博士（工学）論文として価値あるものと認められる。