論文内容の要旨

博士論文題目　A Study on Security Verification of Real-time Cryptographic Protocols
(時間の概念を含む暗号プロトコルの安全性検証に関する研究)

氏　　名　　田中 猛彦

暗号プロトコルの安全性を厳密な方法で検証することを目的として，これまでさまざまな形式的検証法が提案されている．形式的検証は，まず与えられた暗号プロトコルの仕様を何らかの計算モデルに基づいて形式的に記述し，次にその記述が安全性に関する性質を満たすか否かを判定する，という手順で行われる．これにより，設計者の直観や経験を排除して，暗号プロトコルの理論的な安全性を保証することや，安全でない暗号プロトコルの欠陥を検出することが可能となる．しかし，考案されまた実用化されている暗号プロトコルではしばしば，タイムスタンプを用いて情報の新しさを判定しているが，従来の検証法では，時間の経過やタイムスタンプといった時間の概念に対してほとんど注意が払われていなかった．

本論文では，このような時間の概念を含む暗号プロトコルを対象として，その安全性の形式的検証法を提案する．ここで暗号プロトコルが安全であるとは，敵対者が，盗聴等により知り得る情報および利用可能な操作を用いたとしても，目標を達成するのに必要な情報が得られないことと定義する．提案する検証法は，形式化の枠組と判定手続きからなる．形式化のための計算モデルとして，条件付き項書換え系を用いる．時間を非負整数の集合としてモデル化し，敵対者がある情報をいつ所有するかを特別な形の項によって表現する．操作の意味および操作による時間の経過を書換え規則で記述し，タイムスタンプを用いて情報の新しさを判定する操作を条件付き書換え規則で表現する．形式化の段階で，敵対者の能力および目標についても記述する．判定手続きは，形式化の枠組に従って得られた，暗号プロトコルの形式的記述に対して，敵対者の目標となる情報に対応する項が得られるか否かを判定する．本検証法を用いることで，暗号プロトコルを現実に近い形で形式的に記述し，その安全性を議論することが可能となる．

本論文ではさらに，提案した検証法を用いて三つの暗号プロトコルの安全性を検証し，本検証法の有効性を示す．まず，認証と鍵共有を行うある暗号プロトコルについて，それが安全でない，すなわち敵対者が他者になりすまして認証を受け，鍵を共有できることを示す．このプロトコルは，BAN 論理による検証法で安全であると判定されたものである．この検証結果の違いは，時間の概念のモデル化にある．本論文で提案する検証法では，時間を定量的に取り扱っている．そのため，他者を装った通信により情報中のタイムスタンプを更新する方法を発見できた．また，実用化されている認証プロトコル Kerberos を検証し，実際的な使用環境の下で安全であることを示す．

氏　名	田 中　猛 彦

論文審査結果の要旨

近年の計算機ネットワークの発達に伴い，ネットワーク上で安全な秘密通信や認証を実現するために，これまで様々な暗号プロトコルが提案されている．暗号プロトコルを使用するに当たって，あらかじめその安全性を保証すること，あるいは欠陥があればそれを検出することが重要な課題となっている．本論文は，タイムスタンプ等の時間の概念を含む暗号プロトコルを対象として，その安全性の形式的検証法を提案するとともに，本検証法を用いて実際に安全性検証を行い，その有用性を示したものである．本論文の主な成果は次のように要約される．

(1)時間の概念を含む暗号プロトコルの安全性問題を形式的に記述するための枠組を提案している．時間を定量的に取り扱えるようモデル化し，暗号プロトコルにおいて使用される操作を条件付き項書換え系で記述することにより，時間の概念を自然な形で表現することが可能となった．

(2)提案した形式化の枠組により得られる形式的記述を入力として，その安全性を判定するための一つの手続きを提案している．この手続きは，一般には停止する保証はないが，停止すれば安全か否かが決定できる．具体例について，繰り返しが起る場合の対策を考察している．

(3)提案した形式化の枠組および安全性判定手続きを用いて，三つの暗号プロトコルの安全性を検証している．その中で，従来のBAN論理による検証法により安全であると判定されていた暗号プロトコルが安全でないことを示している．また，実用化されている認証プロトコル Kerberos については，その中核部分となるプロトコルが現実的な使用環境の下で安全であることを示している．

以上のように，本論文は，時間の概念を含む暗号プロトコルに対する安全性の形式的検証法を提案するとともに，本検証法を用いて実際に安全性検証を行い，その有用性を示したものであり，情報セキュリティの分野において，学術上，実用上寄与するところが少なくない．よって，本論文は博士（工学）の学位論文として充分に価値のあるものと判断する．