平成１４年度　情報工学専攻修士論文要旨

坂部 研究室	氏　　名	佐野 嘉則
論 文 題 目	項書換え系と木オートマトンを用いたセキュリティプロトコルの検証法における近似関数に関する研究	

近年、インターネットが普及し通信と処理を保護するためにセキュリティプロトコルの重要性が増大している。このような背景から侵入者の攻撃や不正行為に対して安全であることを検証する研究がさまざまなアプローチで行われている。その方法の一つとして項書換え系と木オートマトンを利用した方法が Thomas Genet,Francis Klay らによって提案された。この方法では、項でネットワークの状況を表現し、プロトコルや侵入者を項書換え系で表す。そして項書換え系で到達可能な項の集合で通信でのおこりうる状況を表し、その中に安全でない項が含まれるかどうかを調べることによりプロトコルの検証を行っている。その中で到達可能な項の集合を求める際、近似オートマトンを求めることにより近似を行う。その過程で使用される関数が近似関数であり、近似の精度は近似関数に依存している。また、近似オートマトンを求めるアルゴリズムの停止性は保証されておらず、使用される近似関数に依存している。現状では近似関数の生成法を定式化したものはなく、プロトコル検証の目的に適し、うまく止まるように手動で近似関数を与える方法がとられている。

本研究では、プロトコルの検証という条件下での、近似関数を生成するアルゴリズムを提案する。まず、プロトコルのモデル化に関して、項書換え系 $\mathcal{R}$、木オートマトン A_0 について条件を定義し、その条件を満たす場合での近似関数 γ の生成アルゴリズムを与える。そして、得られた近似関数での近似オートマトン生成アルゴリズムは停止し、近似オートマトン A_k が得られることの証明を行う。γ 生成アルゴリズムと近似オートマトン生成アルゴリズムを用いた近似オートマトン生成手順の全体像を下図で示す。また、Needham-Schroeder Public Key プロトコル、AKA プロトコルを例として取り上げ、それらが本論文で定義した条件を満たす項書換え系、木オートマトンで表せることを示し、生成される近似関数やそれを用いて得られる近似オートマトンについて考察する。