平成１５年度　情報工学コース卒業研究報告要旨

坂部・酒井 研究室	氏　　名	奥谷大介
卒業研究題目	項書換え系と木オートマトンに基づく 暗号プロトコル検証法の共通鍵方式への応用	

現在，インターネットの普及に伴い，ネットワークの処理を保護するためのセキュリティプロトコルが重要になってきている．プロトコルの方式は使用する鍵の種類により，共通鍵方式と公開鍵方式に大別されるが，前者は通信相手のなりすましに弱く，後者は鍵の生成に複雑な計算を必要とするという欠点がある．そこで現在用いられているプロトコルの多くは，共通鍵方式と公開鍵方式を組み合わせたハイブリッド方式が用いられている．

一方，通信への侵入者の攻撃や不正行為に対してプロトコルが安全であることを検証する研究がさまざまな方法で行われている．公開鍵方式プロトコルの検証方法の一つとして，項書換え系と木オートマトンを利用する方法がある．この方法では，項でネットワークの状況を表現し，項書換え系でプロトコルや侵入者を表す．そして通信で起こりうる状況，つまり項書換え系で到達可能な項の集合を近似オートマトンを利用して求め，その中に安全でない状態を表す項が含まれるかどうかでプロトコルの安全性の検証を行う．ここでプロトコルが安全であるということは，そのプロトコルが機密性と認証性をもっていることを意味する．機密性とは通信するメッセージが侵入者に知られないことであり，認証性とは実際の通信相手が想定した通信相手と相違ないこと，つまりなりすましが行われていないことである．

本研究では，上記の検証方法を共通鍵方式へ適用できるように形式化の変更を行う．そのため，公開鍵方式の検証のために用意されたいくつかの関数記号を修正，追加し，機密性と認証性の検証方法も変更する．そして認証性をもたないことが知られている共通鍵方式の，Diffie-Hellman 鍵交換プロトコルに適用し，プロトコルの検証を行った．その結果，このプロトコルが機密性はもつが認証性をもたないことがという検証結果を得た．次に Diffie-Hellman 鍵交換プロトコルをハイブリッド方式に改めて，認証性をもつようにした Hybrid DH プロトコルを作成し，その機密性と認証性を本研究の検証法で検証した．複数間の通信の検証，キーサーバを介したプロトコルの検証にも適用できるように検証法を拡張することは今後の課題である．