平成18年度 情報工学コース卒業研究報告要旨

酒井 研究室	氏　　名	坂 田 翼
卒業研究題目	Spi計算における機密性の自動検証に関する研究	

通信の安全性を示す重要な性質の1つとして機密性が挙げられる．機密性とは，どのような状況で通信を行っても秘密情報は外部に漏れることはないという性質である．情報漏洩が多発し通信の安全性が求められる昨今では，通信の機密性検証は重要な課題である．機密性の検証方法については様々な研究がなされているが，本論文ではSpi計算を用いた機密性の検証手法について考察する．Spi計算はπ計算を拡張した並列計算モデルであり，π計算に暗号化機能を表す構文が追加されている．従って，Spi計算は暗号化と復号化の手順の詳細に立ち入らず，それぞれを一つの演算として抽象した形で暗号通信プロトコルを記述することができる．このため，Spi計算では通信プロトコルを詳細かつ簡潔に表す事ができ，セキュリティ通信の安全性検証に適している．

本論文では，機密性の問題を次のように定式化する．通信プロトコルを記述したSpi計算のプログラム，外部の第三者が知っている情報の集合，および，秘密にしたい情報の3項組に対して，第三者が知っている情報を駆使してどのような行動をとっても，第三者が秘密情報を得られないとき “YES”，そうでないとき “NO” を答える問題である．もう少し詳しく言うと，第三者の知り得る情報の集合は，知っている情報とプロトコルが進行中に得られる情報に対して暗号化と復号化を任意に適用して得られる情報の集合であり，機密性の問題はこの集合に対する秘密情報のメンバーシップ問題であるとみなす．この問題は決定不能であると予想される．

本論文では，木正規表現に基づいて機密性の問題を近似的に解く手法を提案する．通信プロトコルが実行される前に外部が知っている情報を木正規表現Eで与えるものとする．通信プロトコルを記述したSpi計算のプログラムPから木正規表現$\mathit{inform}(P)$を構成する．$\mathit{inform}(P)$は通信を実行した際に漏洩する情報をすべて含む集合を表現する．よって，$\mathit{inform}(P)+E$は外部が知り得る情報をすべて含む集合を表現する．次に，もう1つの木正規表現$\bar{C}(\mathit{inform}(P)+E)$を生成する．$\bar{C}(\mathit{inform}(P)+E)$は，$\mathit{inform}(P)+E$が表現する集合の要素に暗号化，復号化を繰り返し適用して得られる情報から，暗号化されていない情報をすべて含む集合を表現する．つまりこの$\bar{C}(\mathit{inform}(P)+E)$は第三者が知り得るすべての情報の集合を近似する集合の表現である．$\bar{C}(\mathit{inform}(P)+E)$が表現する集合の中に秘密情報がなければ “YES”，そうでなければ “UNKNOWN” を返す．この近似的検証アルゴリズムが “YES” を出力すれば機密性は保障される．出力が “UNKNOWN” の場合は機密性は不明である．つまり，機密性が保たれていないと判定されてもこの検証方法では実際に機密性が保たれていないかどうかは判断できない．現時点では，この機密性検証アルゴリズムの正当性は，Eが有限個の情報だけからなる集合を表現する場合のみ証明されている．任意の木正規表現である場合の正当性証明，また，よりよい近似方法の検討は今後の課題である．