平成23年度 情報工学コース卒業研究報告要旨

結縁 研究室	氏　　名	杉 浦　広 基
卒業研究題目	モデル検査器と Self Composition を用いた 量的情報流の検証	

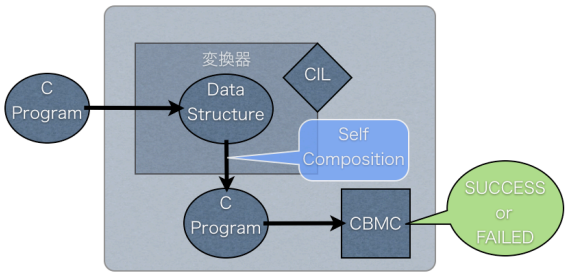
本研究は，Self Composition とモデル検査器 CBMC を用いて，C 言語プログラムの量的情報流の値を自動的に見積もる手法を提案する．

近年，個人情報を扱う企業などによる機密情報の流出が問題となっている．流出の主な原因は人為的なミスやプログラムのバグである．しかし，正常な動作をするプログラムであっても，出力を観測することで機密情報を推測することが可能であるため，情報漏洩の原因となる．出力が含む情報量を見積もることで，プログラムの情報漏洩に関する信頼性を評価できる．

プログラムの入出力間の依存関係を情報流という．量的情報流とは，情報流において情報がどの程度漏洩するかという考え方ある．量的情報流の定義の 1 つに「シャノンエントロピーをベースにした量的情報流」（以下 SE とする）がある．SE は出力の確率分布に依存し，出力の確率分布は入力の確率分布に依存する．一般に入力の確率分布は一意に定まらないため，実際に SE を計算するのは困難である．しかし，SE が最大値を取る場合を考慮することで，SE が少なくとも最大値以下であると評価できる．出力の確率分布が一様分布であるとき SE は最大値を取ることが知られている．SE の最大値を「チャネルキャパシティベースの量的情報流」（以下 CC とする）という．ある実数 q に対して $CC \leq q$ であるかを判定する問題を CC の上限問題という．CC の上限問題を真とする q は $SE \leq q$ を満たすので，SE の値を見積もることができる．

C 言語プログラムを Self Composition を用いて書き換え，モデル検査器 CBMC で解析することで，CC の上限問題を判定する手法がある．C 言語は記述の自由度が高く，意図する命令を様々な形式で記述できるため，プログラムの解析が複雑になる場合がある．OCaml のライブラリである CIL により，C 言語プログラムを構文木のデータ構造として扱うことができる．Self Composition は，プログラムを複製し，異なる入力に対する各出力を調べる手法である．データ構造化したプログラムに Self Composition を用いることで，プログラムを統一した記述に書き換えることができ，効率よく CC の上限を計算することが可能である．書き換えにより事前・事後条件を与えられたプログラムをモデル検査器 CBMC の入力とすることで，条件を満たすかどうかを判定できる．Self Composition は，判定する CC の上限の値が大きくなると，記述する命令が指数関数的に増大するため，手動で書き換えを行うことは現実的ではないという問題がある．

本研究では，Self Composition による C 言語プログラムの書き換えの負担を軽減するために，書き換えを自動的に行う変換器を実装した．右図は本研究のフローチャートである．変換器は入力として与えられた C 言語プログラムを解析し，Self Composition を用いた書き換えを行った後，書き換えられた C 言語プログラムを出力する．変換器により書き換えられたプログラムを CBMC にかけて解析したところ，プログラムの CC の上限問題を判定し，SE の値を見積もることができた．



フローチャート