様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年　６月　８日現在

機関番号：８２６２６
研究種目：若手研究（Ｂ）
研究期間：2009～2011
課題番号：２１７００００８

研究課題名（和文）　分離理論による現実的なプログラムの形式的証明

研究課題名（英文）　Formal Proofs of Realistic Programs using Separation Logic

研究代表者
Affeldt Reynald　(AFFELDT Reynald)
独立行政法人産業技術総合研究所・情報セキュリティ研究センター・研究員
研究者番号：４０４１５６４１

研究成果の概要（和文）：

組込みシステムの普及に伴い，低レベルプログラムの安全性の保証に対する重要性が高まっている．国際規格において，最も厳密な評価保証レベルは形式検証である．しかし，現状では，形式検証で大規模なプログラムを扱い辛い．一方，低レベルプログラムの特徴である詳細なメモリ操作のために研究レベルでは分離論理という形式手法が提案されている．本研究では，分離論理に基づく形式検証の環境を構築し，現実的なケーススタディ（IC カード用のアセンブリ言語の疑似乱数生成器，暗号スキームの実装に欠かせない２進拡張互除法を含む符号付き多倍長整数処理の関数）でその検証環境の実用性を実証した．

研究成果の概要（英文）：

With the dissemination of embedded systems, it has become important to provide strong security guarantees for low-level programs. According to international standards, the most reliable evaluation assurance method is formal verification. Unfortunately, given the current state of the art, it is still difficult to perform formal verification of large programs. Yet, low-level programs are characterized by detailed memory manipulations, for which the formalism of Separation Logic has been proposed by researchers. In this project, we have developed an environment for formal verification based on Separation Logic, whose usefulness is demonstrated by realistic case studies (SmartMIPS implementations of a pseudorandom number generator and signed multi-precision arithmetic, including the binary extended GCD algorithm, as used in the implementation of cryptographic schemes).

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,200,000	360,000	1,560,000
2010 年度	600,000	180,000	780,000
2011 年度	700,000	210,000	910,000
総　計	2,500,000	750,000	3,250,000

研究分野：総合領域
科研費の分科・細目：情報学・ソフトウェア
キーワード：仕様技術・形式手法・形式検証・定理証明支援系・ホーア論理・分離論理・多倍長整数関数・疑似乱数生成器

１．研究開始当初の背景

(1) 組込みシステムの普及に伴い，低レベルプログラムの安全性の保証に対する重要性が高まっている．国際規格において，最も厳密な評価保証レベルは形式検証である．形式検証とはここでは，コンピュータ上で証明作業を行い，誤りのない証明を構築する手法を指す．通常は，証明する人が定理証支援系というソフトウェアで対話的に形式検証を行う．

(2) しかし，現状では，形式検証で大規模なプログラムを扱い辛い．主な理由として実用的な再利用できる基礎ライブラリが提供されていないことを挙げられる．形式的証明の構成が非常に詳細にわたるため，検証のために開発された環境の再利用が困難である．

(3) 一方，低レベルプログラムは逐次的で，ポインターを通じて詳細なメモリ操作を行う特徴がある．そのようなプログラムに対して，分離論理という形式手法が提案されている．本研究の研究代表者が以前，疑似コードとアセンブリ言語の形式検証のための分離論理の形式化を行い，低レベルのメモリ管理関数やアセンブリプログラム等でその実用性を確かめた．

２．研究の目的

本研究の目的は，低レベルプログラムの形式検証のための，定理証明支援系に基づく形式検証の環境の構築である．その検証環境の実用性を実証するために，セキュリティプロトコルの暗号の実装に使われる多倍長整数演算等の現実的なケーススタディの形式検証を行う．

３．研究の方法

(1) 今回，低レベルプログラムの形式検証のための基盤としてフランス国立情報学自動制御研究所で1985年から開発されているCoqという定理証明支援系を使う．下記で説明する形式検証環境を形式化しながら，ケーススタディの検証を行う．

(2) 形式検証環境の構成は主に２つの部分からなる．１つ目は低レベルプログラムの形式化に必要な基礎ライブラリである．２つ目は分離論理による形式検証のためのサポートである．

(3) 基礎ライブラリとは，検証対象のプログラムの意味論に依存せず，　一般的なプログラムの形式的証明に必要なデータ構造や関数等と，その性質に関する定理を含むライブラリである．これらの基礎ライブラリを予め提供することで，定理証明支援系に於いて自動化ができない場合でも，対話的な形式検証を簡単にすることができる．

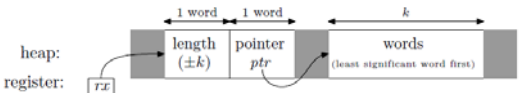

図１　符号付き多倍長

(4) 分離論の形式検証のためのサポートとは，対話的な検証作業を簡単にするための再利用可能な仕組みである．検証対象のプログラムの意味論が証明したい性質と比較して余計に複雑であるとき，形式的証明が容易になる意味論に移して証明を行うことが有用である．例えば，プログラム変換や模倣関係によって，対象の低レベルプログラムを形式検証に相応しい形に変えることができる．

４．研究成果

(1) 形式検証の基礎ライブラリの概観

① 本研究では，ケーススタディとして（４．研究成果（２）で説明する），低レベルプログラムの暗号関数の形式検証を行った．その場合，形式仕様は暗号論的な安全性の証明に基づくので，整数論や確率論等の形式検証が必要になる．例えば，下記に紹介するケーススタディでは，暗号論的疑似乱数生成器の形式仕様は数学の平方剰余問題に基づく．その形式仕様の記述ができるように，コンピュータが扱う整数等の形式化を行い，基礎ライブラリを提供してきた．特にその中で，暗号関数の仕様に欠かせない多倍長整数を，GMP という有名な多倍長整数ライブラリに沿って，分離論理を用いて形式化を行った．具体的な例として，図１と図２で符号付きの多倍長整数のイメージと形式仕様を示す．特に，図２の最終行は分離論理によるポインター構造を表している（詳細は雑誌論文(3)を参考）．また，この基礎ライブラリの応用として，確率論に対して，大数の法則を含む確率論の形式化に加えて，情報理論の基礎を形式化し，情報理論の有名なシャノン定理の形式化に

```
Definition var_signed k rx val st h : Prop :=
 u2Z ⟦rx⟧_st + 4 * 2 < β ∧
 ∃ l, ptr, A. length A = k ∧
  s2Z l = Zsgn(s2Z l) * k ∧
  val = Zsgn(s2Z l) * Sum k A ∧
  Zsgn(s2Z l) = Zsgn val ∧
  u2Z ptr + 4 * k < β ∧
  Zabs val < β^k ∧
  (rx ↦ l :: ptr :: nil * ptr ↦ A) st h.
```

図２　符号付き多倍長の分離論理による形式仕様

成功した(雑誌論文(2)に参考)． つまり，本研究で提供する形式基盤では整数論に基づく暗号関数だけでなく，情報理論に基づく次世代暗号のプログラムの形式検証にも役に立つ可能性も示すことができた．

② 低レベルプログラムは効率を考慮して開発されるので，実装は詳細的で，形式検証に相応しくないことがしばしばある．今回，小規模コンパイラの形式化で基礎ライブラリの機能を拡張した．このコンパイラは制御構造とジャンプ命令の言語の間の翻訳に於いて，意味を保つだけでなく，分離論理による性質も保つので，形式モデルから実際に実行できるプログラムの生成ができ，下記説明するケーススタディに適用ができた．そのコード生成の実験によって本研究の実用性の確認ができただけでなく，その過程で有名なデバッガ(GDB)のバグを発見した(雑誌論文(1)を参考)．

③ 本研究の目的の一つは低レベルプログラムの形式検証のスケーラビリティの問題である．今回，その問題に対して，抽象的な疑似コードからのアセンブリプログラムの構成を提案した．組込みシステム用の低レベルプログラムは効率を考慮してコンパイラで生成せず，直接手で実装することが多い．そこで，低レベル記述による複雑さを省き検証を容易にするために，疑似コードからアセンブリプログラムを構成する形式的な模倣の概念を導入し，基礎ライブラリを拡張した(雑誌論文の(3)，(6)を参考)．

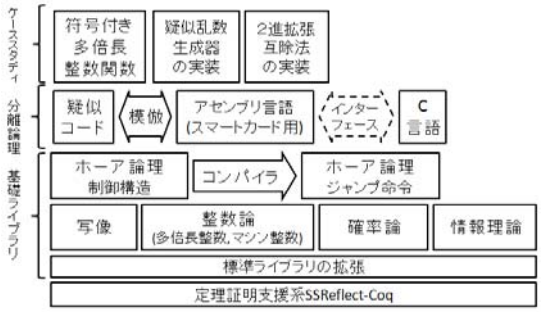

図３ 形式検証の基礎ライブラリの構造

④ 最後に，現実的なC言語のモデルの形式化を行った．その形式モデルでは，C 言語のデータ構造の特徴であるアライメントとパディングを公理化したので，再帰的データを含むデータ構造のレイアウトが明確に表現できる．更に，そのC言語のモデルに沿って，分離論理を拡張し，古典的な実例で確かめた．この形式モデルとその分離論理を用いて，暗号スキームの実装にしばしばあるC言語とアセンブリ言語の組み合わせの形式検証が可能になった(雑誌論文(4)を参考)．

⑤ 上記の数学基盤と小規模コンパイラと模倣の概念とC言語のサポートを一つの再利用の可能な基礎ライブラリで纏め，Coq 定理証明支援系で形式化した．特に，モジュールを導入したおかげで，一つの枠組みの中で，複数のプログラミング言語(疑似コード，アセンブリ言語，C言語)のサポートの提供ができた(図３ 形式検証の基礎ライブラリの構造)．

(2)形式検証済みの暗号関数のライブラリに向けて

① 疑似乱数生成器の形式検証に成功した．対象の疑似乱数生成器は Blum-Blum-Shub（BBS）によるアルゴリズムに基づくSmartMIPSというICカード用のアセンブリ言語で実装されたものである．この成果は安全性の面から重要である．まず，疑似乱数は暗号スキームの重要な要素であるので，実装のバグは安全性の問題に繋がる．また，従来，暗号研究者らによる安全性証明の対象はアルゴリズムであり，実際に動作するプログラムではなかった． 本研究ではアセンブリ言語を直接扱いながら，暗号学的・形式的安全性の同時証明に初めて成功した．その成果を国際雑誌にて発表した．図４ 暗号論的疑似乱数生成器の形式仕様に分離論理による疑似乱数生成器の形式仕様を示す(雑誌論文(1)を参考)．

図４ 暗号論的疑似乱数生成器の形式仕様

② 一般的に，暗号スキームの実装は符号付き多倍長整数の関数を必要とする．次のケーススタディに向けて，様々な符号付き多倍長整数関数の形式検証を行った．更に，基礎ライブラリに導入した形式模倣を用いて，多倍長整数の関数と疑似コードの模倣を形式検証できた．その形式検証の実験によって，初めて現実的で形式検証済みの符号付きの多倍長整数のライブラリの構築ができた(雑誌論文(6)を参考)．

③ 最後に，2進拡張互除法の実装の形式検証

に成功した．そのアルゴリズムを用いて，暗号スキームの復号に使われるモジュラ計算の逆数の計算ができるようになった．上記紹介した符号付き多倍長整数の関数の形式検証を用いて，アセンブリ言語の２進拡張互除法の実装は疑似コードから構成したため，スケーラビリティ問題を乗り越え，数百行の中規模低レベルプログラムの形式検証ができた．（図５　模倣による２進拡張互除法の形式仕様）．更に，疑似コードとアセンブリ言語の模倣から，アセンブリ実装の正しさの形式証明も得ることができる．（雑誌論文(3),(6)を参考）．

```
Lemma begcd_simu :
nodup(g, u, v, u1, u2, u3, v1, v2, v3, t1, t2, t3) →
nodup(rk, rg, ru, rv, nu1, nu2, nu3, nv1, nv2, nv3,
 rt1, rt2, rt3, a0, a1, a2, a3, a4, a5, a6, a7, a8, a9, r0)
→ 0 < vu → 0 < vv →
fwd_sim (state_mint (g ⇛ unsign rk rg ⊎
  u ⇛ unsign rk ru ⊎ v ⇛ unsign rk rv ⊎
  u1 ⇛ signed L nu1 ⊎ u2 ⇛ signed L nu2 ⊎
  u3 ⇛ signed L nu3 ⊎ v1 ⇛ signed L nv1 ⊎
  v2 ⇛ signed L nv2 ⊎ v3 ⇛ signed L nv3 ⊎
  t1 ⇛ signed L nt1 ⊎ t2 ⇛ signed L nt2 ⊎
  t3 ⇛ signed L nt3))
 (fun s st h ⇒ uv_init vu vv u v s ∧
               uv_bound rk st u v s L)
 (begcd g u v u1 u2 u3 v1 v2 v3 t1 t2 t3)
 (begcd_mips rk rg ru rv nu1 nu2 nu3 nv1 nv2 nv3
             nt1 nt2 nt3 a0 a1 a2 a3 a4 a5 a6 a7 a8 a9).
```

図５　模倣による２進拡張互除法の形式仕様

④ 以上の基礎ライブラリとケーススタディを纏めて，現時点までに，整数論に基づく暗号スキーム(例えば,ElGamal 暗号スキーム)に必要な疑似乱数生成と暗号と復号の関数の形式検証ができるようになった．今後，本研究で提案したC言語の形式モデルと分離論を用いて，形式検証済みの完全な暗号スキームの実装ができるようにする．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計８件）

① Reynald Affeldt, David Nowak, Kiyoshi Yamada, Certifying Assembly with Formal Security Proofs: the Case of BBS, Science of Computer Programming, Elsevier, 査読有, 77 巻, 10-11 号, 2012, pp. 1058-1074,
DOI: 10.1016/j.scico.2011.07.003

② Reynald Affeldt, Hagiwara Manabu, Formalization of Shannon's Theorems in SSReflect-Coq, Proc. of the 3rd Conference on Interactive Theorem Proving, Lecture Notes in Computer Science, Springer, 査読有, 7406 巻, 2012, 16 頁, 記載確定
http://staff.aist.go.jp/reynald.affeldt/bib.html

③ Reynald Affeldt, On Construction of a Library of Formally Verified Low-level Arithmetic Functions, Proc. of the 27th ACM SIGAPP Symposium On Applied Computing, 査読有, 2 巻, 2012, pp. 1326-1331,
DOI: 10.1145/2245276.2231986

④ Reynald Affeldt, Kiyoshi Yamada, Formal Verification of C Programs for Implementations of Communication Protocols, 日本ソフトウェア科学会第 28 回大会講演論文集, 査読無, 2011, 16 頁,
http://staff.aist.go.jp/reynald.affeldt/bib.html

⑤ Reynald Affeldt, David Nowak, Kiyoshi Yamada, Certifying Assembly with Formal Cryptographic Proofs: the Case of BBS, Electronic Communications of the EASST, 査読有, 23 巻, 2010, 15 頁
http://journal.ub.tu-berlin.de/index.php/eceasst/article/view/316

⑥ Reynald Affeldt, Toward Formal Construction of Assembly Arithmetic Functions from Pseudo-code, 第 12 回プログラミングおよびプログラミング言語ワークショップ論文集, 日本ソフトウェア科学会, 査読有, 2010, pp. 1-15,
http://staff.aist.go.jp/reynald.affeldt/bib.html

〔学会発表〕（計 11 件）

① Reynald Affeldt, On Construction of a Library of Formally-verified Low-level Arithmetic Functions, 27th ACM SIGAPP Symposium On Applied Computing, 2012 年 3 月 30 日, Riva del Garda, Italy

② Reynald Affeldt, Manabu Hagiwara, シャノンの定理の形式化, 日本応用数理学会 2012 年春の研究部会連合発表会, 2012 年 3 月 8 日, 福岡県福岡市, 九州大学伊都キャンパス

③ Reynald Affeldt, Kiyoshi Yamada, Formal Verification of C Programs for Implementations of Communication Protocols, 日本ソフトウェア科学会第 28 回大会, 2011 年 9 月 27 日, 沖縄県那覇市, 沖縄産業支援センター

④ Reynald Affeldt, Toward a Library of Verified Arithmetic Functions, 日本応用数理学会 2011 年度年会, 2011 年 9 月 14 日, 京都府, 同志社大学今出川キャンパス

⑤ Reynald Affeldt, Kiyoshi Yamada, 分離論理を用いた,C言語プログラムの機械的検証(ポスター), 第 13 回プログラミングおよびプログラミング言語ワークショップ, 2011 年 03 月 10 日, 北海道札幌市
⑥ Reynald Affeldt, Toward Formal Construction of Assembly Arithmetic Functions from Pseudo-code, 第 12 回プログラミングおよびプログラミン グ言語ワークショップ , 2010 年 3 月 3 日, 香川県琴平
⑦ Reynald Affeldt, David Nowak, Kiyoshi Yamada, 形式的な暗号学的安全性証明によるアセンブリプログラムの安全性検証:BBS の事例, 日本応用数理学会 2009 年度年会, 2009 年 9 月 28 日, 大阪大学豊中キャンパス
⑧ Reynald Affeldt, David Nowak, Kiyoshi Yamada, Certifying Assembly with Formal Cryptographic Proofs: the Case of BBS, 9th International Workshop on Automated Verification of Critical Systems (AVoCS 2009), 2009 年 9 月 23 日, University of Wales, Gregynog Hall, UK

〔その他〕
検証環境とケーススタディのホームページ:
http://staff.aist.go.jp/reynald.affeldt/coqdev

６．研究組織

(1)研究代表者
Affeldt Reynald (AFFELDT Reynald)
産業技術総合研究所・セキュアシステム研究部門・研究員
研究者番号：４０４１５６４１