National Institute of Advanced Industrial Science and Technology
AIST

Research Center for Information Security

実用的な暗号の形式的証明に向けて: アセンブリでの多倍長整数アルゴリズムの形式的検証

アフェルト レナルド

情報セキュリティ研究センター（RCIS）
ソフトウェアセキュリティ研究チーム

National Institute of Advanced Industrial Science and Technology
AIST

実用的な暗号の実装の形式的証明

Research Center for Information Security

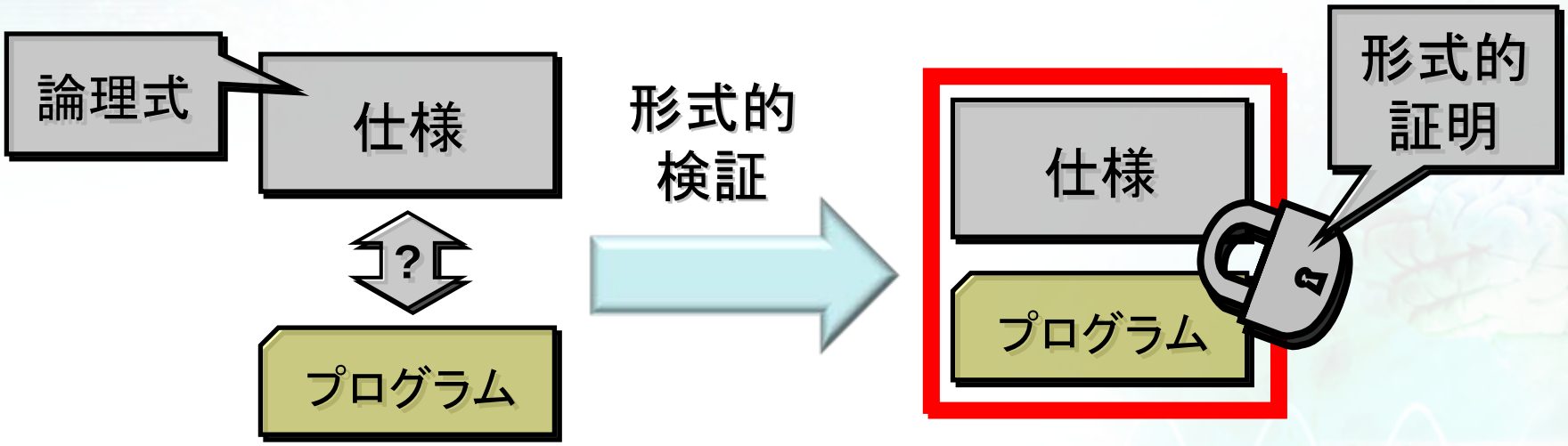
- 最終目的: 高信頼な安全性の証明
  - 暗号はセキュリティプロトコルの基本的な部分
    ⇒ 暗号の実装の誤りで安全性が破れる
- しかし, 実用的な暗号の実装の検証は困難
  - 整数論による情報処理, 高い効率を要求
    ⇒ 先端アルゴリズム, 低レベル実装
    特に, 組込みシステム(Smartcardなど)

National Institute of Advanced Industrial Science and Technology
AIST

形式的検証とは?

Research Center for Information Security

- 国際規格(コモンクライテリアなど)における最も厳密なセキュリティレベル:
  1. ソフトウェアの実装の正しさの機械検証
  2. 第三者による全自動検査可能な証明の発行



National Institute of Advanced Industrial Science and Technology
AIST

我々の貢献

Research Center for Information Security

- アセンブリ言語での整数論アルゴリズムの形式的検証を提供する
  - Coq定理証明器の上でのライブラリの開発
    - 低レベルデータ構造の扱いや
    - ホーア論理による証明の構成などの形式化
  - 実用的な暗号関数の実装とその形式的証明
    - 例: 多倍長足し算など, Montgomery掛算, 疑似乱数生成器
    - 本ポスターではMontgomery冪剰余を細かく取り上げる
  - インターネット上で公開: http://staff.aist.go.jp/reynald.affeldt/coqdev/