National Institute of Advanced Industrial Science and Technology
AIST

Research Center for Information Security

Certifying Assembly with Cryptographic Proofs

〈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〉

Reynald AFFELDT, David NOWAK, and 山田 聖
レナルド アフェルト, ダヴィット ノヴァック, やまだ きよし

情報セキュリティ研究センター
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

研究の特徴

Research Center for Information Security

- **暗号アルゴリズムの安全性検証技術** と **プログラム検証技術** を **統合**
  - アセンブリ言語で記述された**暗号プログラムの暗号学的安全性検証** ができる
  - 定理証明支援ソフトウェアの利用により，**厳密な検証**ができる

National Institute of Advanced Industrial Science and Technology
AIST

研究の背景

Research Center for Information Security

暗号プログラムの安全性検証の必要性

機密情報をやりとりする
製品・サービスが普及

暗号プログラム

効率のためアセンブリ言語で記述されがち

- 暗号学的安全性の検証は行われていない
- 多くの製品で利用されているため，
  不具合が発見された場合の
  社会的・経済的影響が大きい

数理的技法(形式手法)による厳密な暗号学的安全性検証を
暗号プログラムに適用した前例がない！

National Institute of Advanced Industrial Science and Technology
AIST

研究の概要

Research Center for Information Security

暗号アルゴリズムの安全性検証とプログラム検証の統合

プログラムの正しさの検証
分離論理(ホーア論理の拡張)
検証済みプログラム変換器

＋ 統合

暗号アルゴリズムの安全性検証
ゲーム列による安全性証明

暗号プログラムの安全性検証
ゲーム列による安全性証明を拡張
- プログラムの正しさの証明に立脚したゲーム変換ステップの追加

定理証明支援ソフトウェア　Coq

National Institute of Advanced Industrial Science and Technology
AIST

事例研究

Research Center for Information Security

- 疑似乱数生成器Blum Blum Shub(BBS)の実装の安全性検証
  - 疑似乱数生成器:

    暗号システムの重要な構成要素 (鍵生成，ノンス生成等)

    安全性: 次ビット予測不能性

  - BBSの実装プログラム:

    SmartMIPSアセンブリで記述(約240行)

  - 結果:

    自動検証可能な安全性証明を得る

BBS アルゴリズム

$x_0 \leftarrow$ seed; $M \leftarrow$ modulus

$x_{i+1} = x_i^2 \bmod M$; $b_i = \text{parity}(x_i)$