論理×確率で安心・安全を極める

C-2-2

99.999…%安全です

－フォーマルメソッドから暗号理論へ －

どんな研究？

- 通信システムの安全性検証の２つの方法
  - ✓フォーマルメソッドを用いた検証方法
  - ✓人手による暗号学的な検証方法

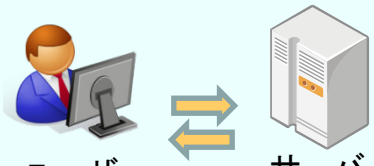
  の関係を解明
- 「前者の方法で安全なら、後者の方法でも安全である」ことを証明

もたらされる変革

- フォーマルメソッドによるセキュリティ検証方法が暗号理論的にも十分信頼性が高いことを証明
- 電子政府などのセキュリティの検証を厳密かつ簡単に行うことが可能

プロトコル

例：匿名ユーザ認証



ユーザの匿名性を保ったまま、正規ユーザであることを確認

暗号学的検証
（厳密だが大変）

暗号学的な安全性

攻撃者

任意の攻撃者がユーザの正体を暴けない

任意の攻撃者＝
- 現実的に実行できる任意の計算を行う
- ランダムな動作（推測）を行う

フォーマルメソッドによる検証
（単純化により検証が容易）

成果のポイント：
「フォーマルメソッドにおける安全性」＝「暗号学的な安全性」
を暗号（公開鍵暗号・ゼロ知識証明等）の安全性を利用して、段階的に証明

フォーマルメソッドにおける安全性

攻撃者

行儀の良い攻撃者がユーザの正体を暴けない

行儀の良い攻撃者＝
- 簡単な計算のみ行う
- ランダムな動作（推測）をしない

フォーマルメソッドにおける安全性と暗号学的な安全性をつなぐ安全性

攻撃者

プロトコル実行中は行儀よく、実行完了後は任意の計算・推測を行う攻撃者がユーザの正体を暴けない

関連文献

G. Bana, Y. Kawamoto, H. Sakurada, “Computational Soundness of (Interactive) Zero-Knowledge Proof Systems in the Presence of Active Adversaries,” Computational and Symbolic Proofs of Security, 2009.

連絡先: 櫻田英樹 (Hideki Sakurada)
協創情報研究部 情報基礎理論研究グループ