論理×確率で安心・安全を極める

C-2-3

頑固なバグも楽々発見

― 暗号理論からフォーマルメソッドへ ―

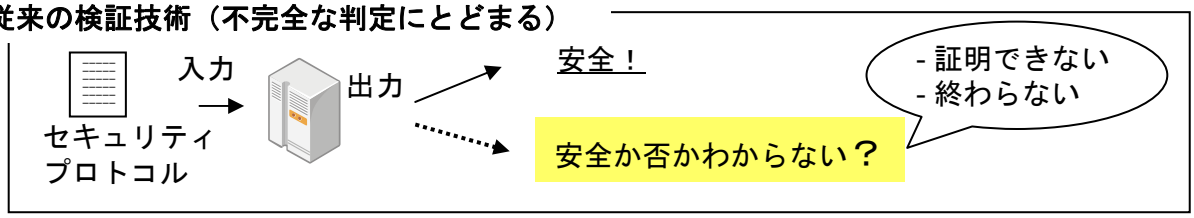
どんな研究？

- 秘密の漏洩，データの改ざんを防ぐセキュリティプロトコルの安全性を保証します．
- 何年も安全と思われてきたセキュリティプロトコルにバグが見つかることが多い．
- 計算機を使って安全性を正確に検証します．

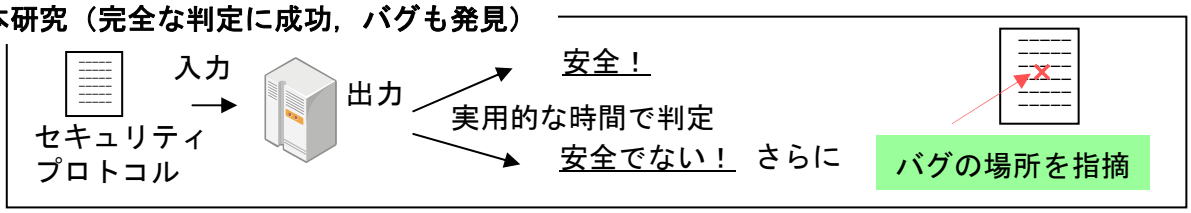
もたらされる変革

- 専門家でも苦労した安全性証明を，実用的な時間で自動検証し，バグも発見できます．
- どのような攻撃にも耐えられる頑強なセキュリティプロトコルを効率的に開発できます．
- 安心してインターネットサービスを利用できます．

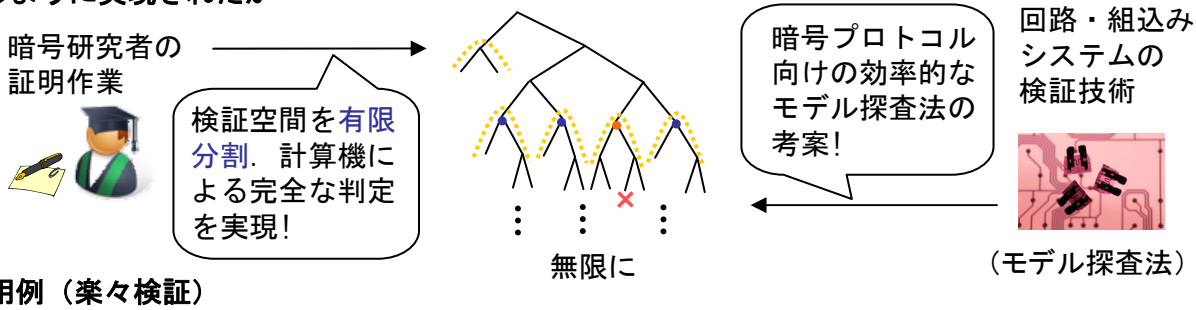
従来の検証技術（不完全な判定にとどまる）



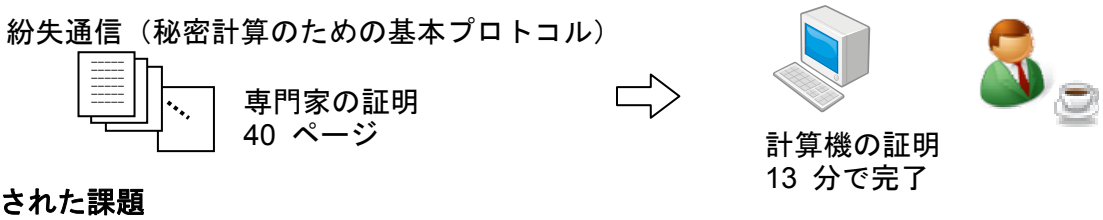
本研究（完全な判定に成功，バグも発見）



どのように実現されたか



応用例（楽々検証）



残された課題

攻撃モデルの拡張：（現状）盗聴 →（今後）データ改ざん

関連文献

T. Araragi and O. Pereira.: Automatic Verification of Simulatability in Security Protocols, the 4th International Conference on Information Assurance and Security 2008, IAS 2008, pp.275—280, 2008.

連絡先: 櫟　粛之(Tadashi Araragi)
協創情報研究部 情報基礎理論研究グループ