どんな研究？

- 高いセキュリティを持つ情報システムを実現するための技術
- 別々に発達した2つの研究分野を融合

もたらされる変革

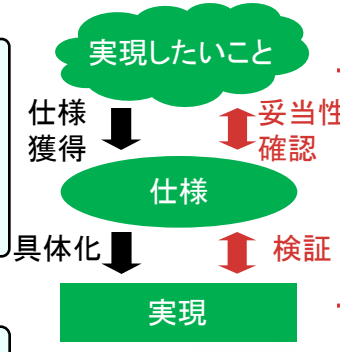
- 高度な暗号を駆使した情報システムの安全性を厳密かつ効率的に検証可能
- 特に高い安全性を求められる電子政府などのシステムを実現するための，基礎技術を提供

展示紹介

- 融合の意義，鍵となるアイデア，および融合のためのアプローチの種類について紹介
- ［第1のアプローチ，フォーマルメソッドから暗号理論へ］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
- ［第2のアプローチ，暗号理論からフォーマルメソッドへ］困難であった安全性証明を計算機に任せることが可能に

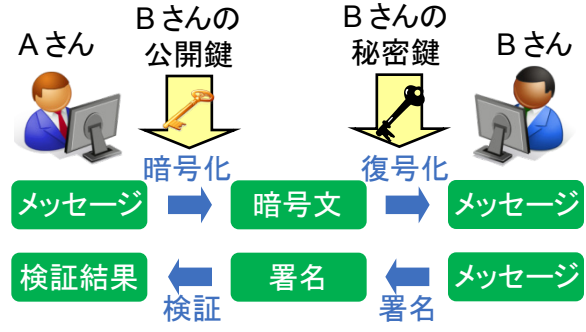
連絡先：真野健
協創情報研究部
情報基礎理論研究グループ

フォーマルメソッド



これらの過程を論理的に厳密に（フォーマルに）行う

暗号理論



高確率で安全な仕組みを提供

融合によって，システムの安全性をより確実に保証！