論理×確率で安心・安全を極める

C-2-1

フォーマルメソッドと暗号理論をつなぐ鍵

―論理学と確率論をつなぐ―

どんな研究？

- 2つの研究分野を融合して，情報セキュリティ分野の革新的新領域を創出
  - ✓厳密な検証を目的とするフォーマルメソッド
  - ✓安全な仕組みを提供するために発展した暗号理論

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，フォーマルメソッドによって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

フォーマルメソッド

数理論理学に基づく

$encrypt(key, data)$

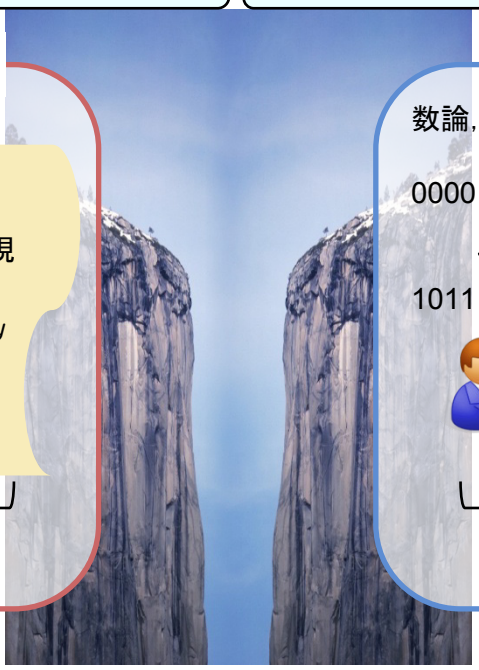
記号的表現

$decrypt(x, encrypt(x, y)) = y$

$$\frac{A,\ A \rightarrow B}{B}$$ 推論

安全 or 危険（真偽）

理想化・抽象化



暗号理論

数論，計算量理論，確率論に基づく

0000 ・・・・001　データのビット列

↓ 暗号・署名計算

1011 ・・・・010

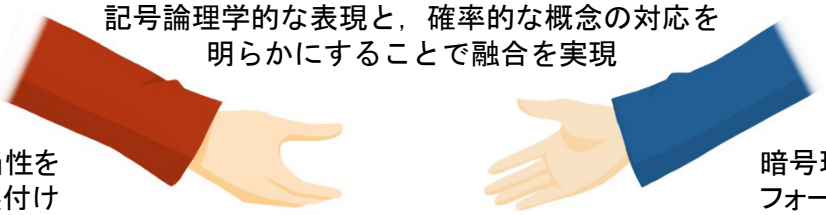
1011 ・・・・010

送受信

安全・危険の確率

現実

記号論理学的な表現と，確率的な概念の対応を明らかにすることで融合を実現



理想化の妥当性を暗号理論で裏付け（第1のアプローチ）

暗号理論のフォーマルな表現方法（第2のアプローチ）

融合によって可能になること

- フォーマルメソッドによる暗号の安全性証明
- 暗号理論による検証方法論の正当化

関連文献

真野，櫻田，河辺，塚田，“ゲーム列による安全性証明の形式化と自動化”，応用数理，vol. 17，no. 4，pp. 38-46，2007.

萩谷，塚田（編），数理的技法による情報セキュリティ，日本応用数理学会監修，シリーズ・応用数理，共立出版，2009 年刊行予定.

連絡先: 真野健 (Ken Mano)

協創情報研究部 情報基礎理論研究グループ