研究スタッフ

教　授：　曽根　秀昭

准教授：　水木　敬明

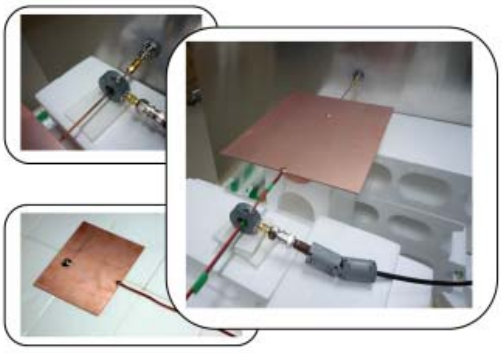
研究目的

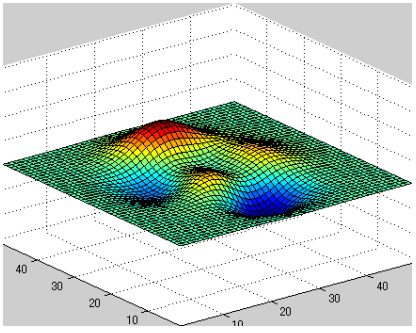
情報ネットワーク技術は情報化社会の基盤であり，本学でもキャンパスネットワークTAINSが全学の研究教育活動を支えている。本研究室の教員はTAINSを整備・運用管理し活用を図るサイバーサイエンスセンターに所属し，これに関連した立場から，以下の研究などを行っている。

主な研究テーマ

1. 環境電磁工学（ＥＭＣ）と電磁情報セキュリティ

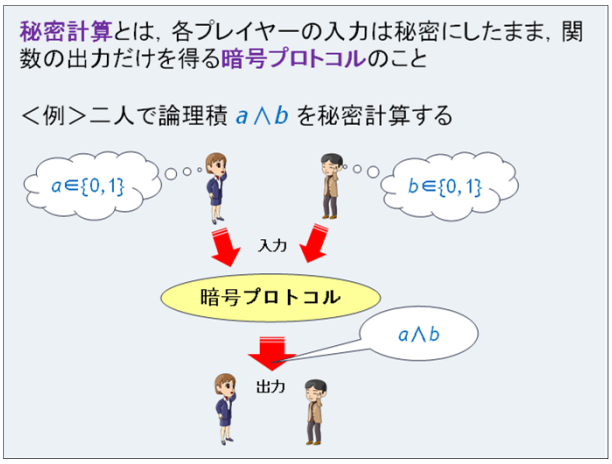
情報通信機器からの電磁放射による情報漏洩のために秘密情報の機密性が損なわれる問題がある。暗号ハードウェアやその他の情報通信システムにおける不要電磁放射の抑制と電磁的情報漏洩の抑止について実験と数値計算により研究している。また、情報ネットワークケーブルのコネクタについて、接触性能の劣化のために起こる情報伝送の完全性のき損や電磁的情報漏洩の測定評価にも取り組んでいる。

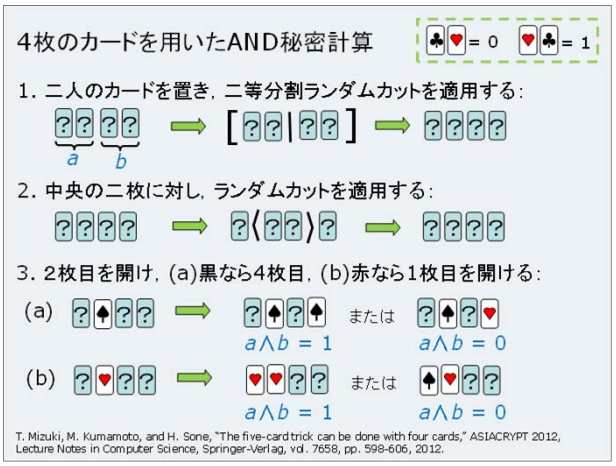


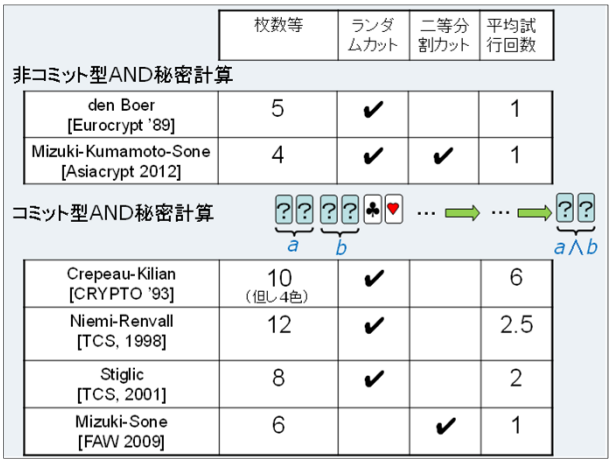


2. 情報セキュリティに関する基礎理論研究

セキュリティ確保の問題は極めて重要であり、セキュリティ確保のために広く利用されている暗号について、基礎的研究を行っている。情報理論的に安全な暗号系の構築、例えばカード組を用いた秘密計算のためのプロトコル設計や部分的漏えい秘密からの秘密鍵共有が検討課題である。







	枚数等	ランダムカット	二等分割カット	平均試行回数
非コミット型AND秘密計算				
den Boer [Eurocrypt '89]	5	✔		1
Mizuki-Kumamoto-Sone [Asiacrypt 2012]	4	✔	✔	1
コミット型AND秘密計算				
Crepeau-Kilian [CRYPTO '93]	10 (但し4色)	✔		6
Niemi-Renvall [TCS, 1998]	12	✔		2.5
Stiglic [TCS, 2001]	8	✔		2
Mizuki-Sone [FAW 2009]	6		✔	1

3. ネットワークの運用・管理と応用

情報ネットワークの運用・管理制度や
応用サービスの研究開発をしている。