研究スタッフ

教　授：　曽根　秀昭

准教授：　水木　敬明

准教授：　林　　優一（東北学院大学）

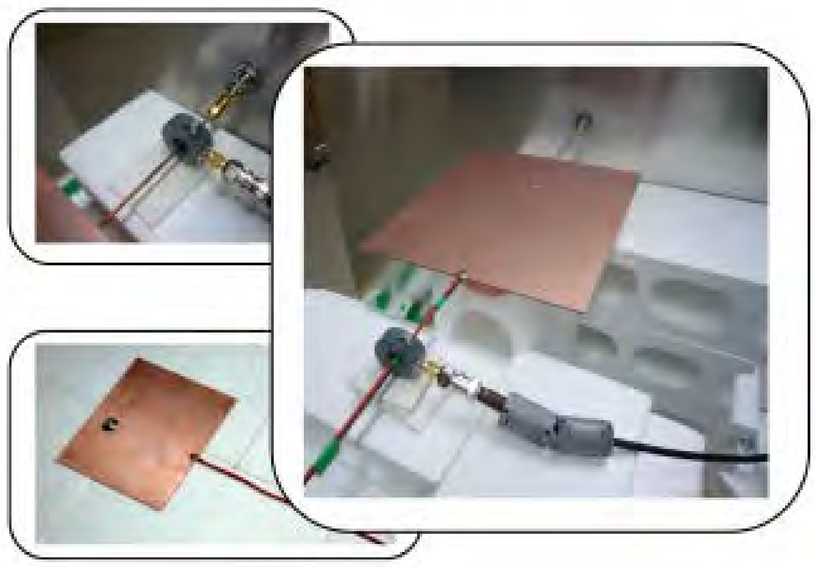
研究目的

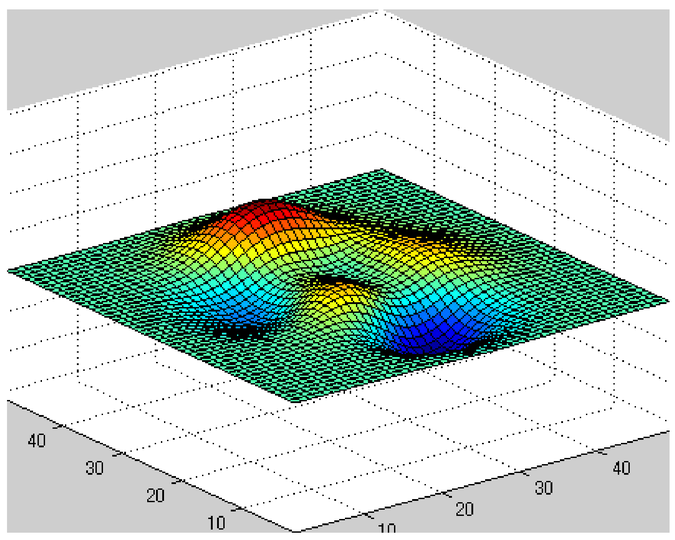
情報ネットワーク技術は情報化社会の基盤であり，本学でもキャンパスネットワークTAINSが全学の研究教育活動を支えている。本研究室の教員はTAINSを整備・運用管理し活用を図るサイバーサイエンスセンターに所属し，これに関連した立場から，以下の研究などを行っている。

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

情報ネットワークのケーブルにおいて，電磁ノイズによる妨害のために情報伝送の完全性が損なわれたり、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たりすることがある。情報通信システムの電磁イミュニティの確保のために，実験と数値計算により電磁的情報漏洩の評価を研究している。また，暗号ハードウェア等の情報システムにおける秘密情報の電磁的漏洩の抑止のために，そのメカニズムの解明と，対策技術の提案を研究課題としている。



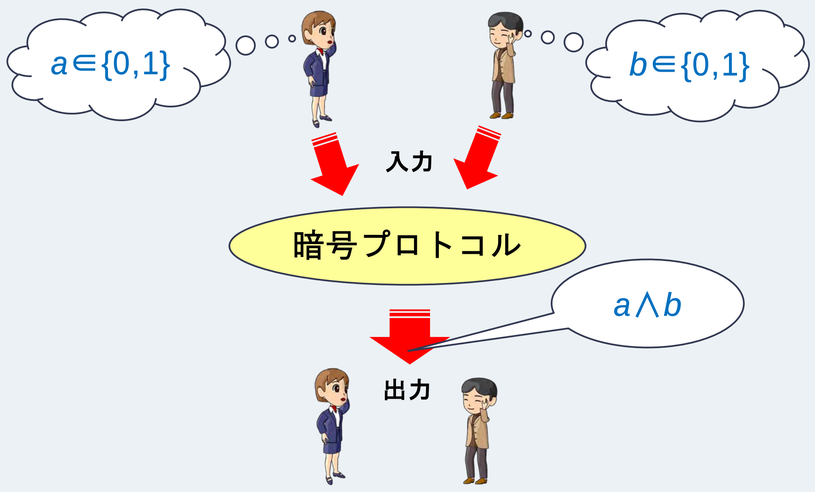


2. 情報セキュリティに関する基礎理論研究

情報ネットワークシステムにおいて，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。無制限の計算能力をもつ盗聴者に対しても安全な暗号系の構築や，秘密計算のためのプロトコルの設計などが検討課題である。

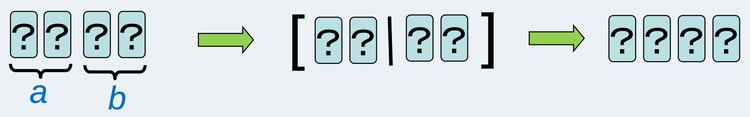
秘密計算とは，各プレイヤーの入力は秘密にしたまま，関数の出力だけを得る**暗号プロトコル**のこと

＜例＞二人で論理積 $a \wedge b$ を秘密計算する

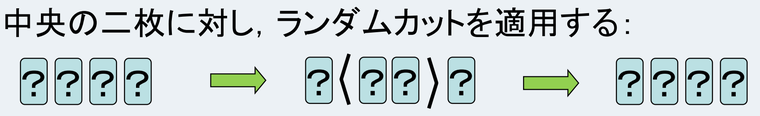


4枚のカードを用いたAND秘密計算　♣♥ = 0　♥♣ = 1

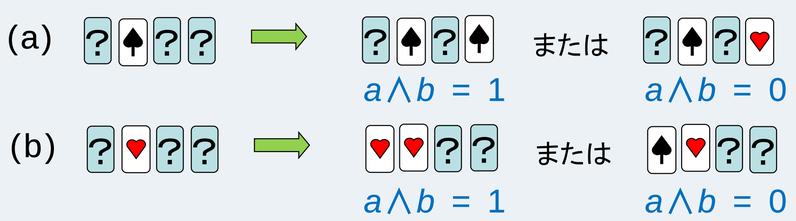
1. 二人のカードを置き，二等分割ランダムカットを適用する：



2. 中央の二枚に対し，ランダムカットを適用する：



3. 2枚目を開け，(a)黒なら4枚目，(b)赤なら1枚目を開ける：

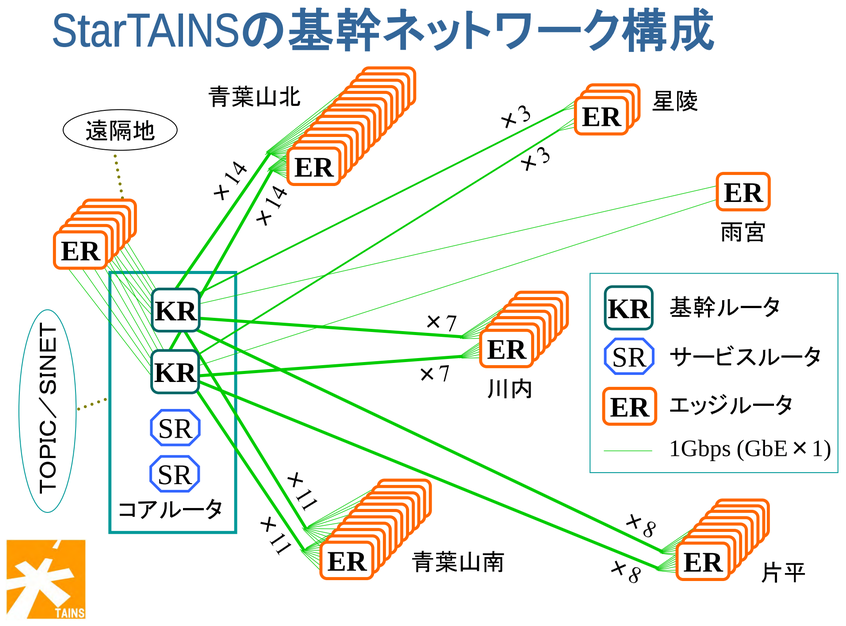


T. Mizuki, M. Kumamoto, and H. Sone, “The five-card trick can be done with four cards,” ASIACRYPT 2012, Lecture Notes in Computer Science, Springer-Verlag, vol. 7658, pp. 598-606, 2012.

	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と応用における基盤技術

長距離の超高速ネットワークにおける柔軟で効率的な運用技術の実証的研究をしている。また，ネットワークの運用管理と情報倫理の問題について，運用支援技術に関する研究を行っている。



曽根・水木研究室　　http://www.tains.tohoku.ac.jp/netlab/