研究室名	**岩本・渡邉研究室**	場所 東 3 号館 924 号室(岩本) 東 3 号館 928 号室(渡邉)
連絡先(email 等)	mitsugu@uec.ac.jp, watanabe@uec.ac.jp	

Ⅰ．研究概要

多くの情報セキュリティシステムは，暗号理論を安全性の基盤としています．岩本・渡邉研究室では，情報セキュリティシステムの安全性と実装方法を主たる研究テーマとして，安全性が厳密に証明でき，かつ現実的にも効率のよい暗号システムの提案を目指しています．同時に暗号システムへの攻撃手法も研究しています（敵を知り，己を知れば，百戦危うからず）．研究にあたっては，離散数学を基本的な道具として計算量的アプローチと情報理論的アプローチを駆使し，暗号実装を軸に研究を進めている崎山・李・宮原研究室，菅原研究室，王研究室と協力しつつ，情報セキュリティシステムについて多角的に考察することを目指しています．

Ⅱ．研究分野（卒研テーマ）

岩本研は暗号技術の基盤理論，渡邉研は暗号技術の高機能化を主たる研究テーマとしますが，原則として合同研究室として垣根なく活動します．具体的な卒研テーマは例えば以下の通りですが，下記以外のテーマでも相談に応じます．

- ✧ 暗号・署名などの基本的な構成要素の提案と安全性評価
- ✧ 暗号技術を面白く，分かり易く伝える技術の開発
- ✧ 秘密計算，ゼロ知識証明等の暗号プロトコルの定式化・設計手法の再考
- ✧ 先端情報技術/環境（AI, B5G等）と組み合わせ可能な高機能暗号技術の検討
- ✧ 暗号化したまま検索を可能とする暗号方式の設計と安全性解析
- ✧ モビリティ向け匿名認証技術の開発

Ⅲ．卒研生の要件

離散数学・暗号理論を履修していることが望ましいです．最低限，離散数学の履修内容がある程度理解できた上で，興味がもてる内容であったこと（知識不足はフォローしますが，論理的な話題に苦手意識があると苦労します）．
詳細は研究室WEBサイト https://iw-lab.jp/messages/ を参照してください．

Ⅳ．配属面談の申請方法

専用のスプレッドシートを用いた先着予約制です．スプレッドシートの URL や具体的な方法は暗号理論の講義で説明しています．受講していない人は友人等から情報を共有してもらうか，岩本・渡邉両名まで連絡してください．