

電気通信大学 平成21年度シラバス

授業科目名	暗号・情報セキュリティ特論		
英文授業科目名	Cryptography and Information Security		
開講年度	2009年度	開講年次	
開講学期	前学期	開講コース・課程	博士前期・後期課程
授業の方法	講義	単位数	2
科目区分	電気通信学研究科-情報通信工学専攻-専門科目		
開講学科・専攻	情報通信工学専攻		
担当教官名	太田 和夫		
居室	総合研究棟928		

公開E-Mail	授業関連Webページ
ota@ice.uec.ac.jp	http://www.oslab.ice.uec.ac.jp/class/cryptography_and_information_security/09/

<p>【主題および達成目標】</p> <p>暗号理論の代表的なトピックスについて、年毎に1つ話題を選んで、基礎から時代の先端までの話題を講義する。 過去には、証明可能安全な方式、マルチパーティプロトコル、ハッシュ関数の安全性、鍵交換プロトコルの安全性概念、Indifferentiabilityとハッシュ関数の設計論について、代表的な論文の解説から最新の結果までを紹介した。</p> <p>本年は「Side Channel 攻撃に対する証明可能安全性を目指して」という主テーマのもとで、 (1) IND - CCA安全な公開鍵暗号、メモリ漏洩攻撃に対する耐性を持つ署名法などへの応用を持つ非対話型ゼロ知識証明 (NIZK)の構成論、 (2) Side Channel攻撃の対象と考えられる Hash関数および公開鍵暗号システムの最新の研究動向、 (3) 安全な Hash関数のハードウェア実装を目指して という内容を扱う。</p> <p>いずれのテーマであっても、定式化の理念、証明方法などを理解することを目的とする。</p>

<p>【前もって履修しておくべき科目】</p> <p>離散数学第一 / 第二, アルゴリズム・データ構造, 暗号理論, 情報セキュリティシステム</p>

<p>【前もって履修しておくことが望ましい科目】</p> <p>計算科学特論, 理論計算機科学特論, 情報数理特論などを合わせて聴講すると, さらに理解が深まります。</p>
--

【教科書等】

今年の講義で使用する論文は講義のHPを参照してください。

参考書：

「現代暗号」

岡本,山本

産業図書

ISBN4-7828-5353-X

Foundations of Cryptography

Oded Goldreich

Cambridge University Press

ISBN0-521-79172-3

【授業内容とその進め方】

取り上げるテーマの、代表的な論文を精読したのち、時代の最先端の結果の意義を理解できるように解説する。論文の精読は、受講生に分担して報告してもらったり、論文中の証明の論理ギャップを補足説明してもらおう予定。

【成績評価方法及び評価基準(最低達成基準を含む)】

平常点（報告を聞きながら議論するので、積極的に議論に参加してもらいたい。）と課題に対するレポートの成績による。

【オフィスアワー：授業相談】

特に設けない。質問等があるときは事前にメールでアポイントメントを取ってから研究室を訪問すること。

【学生へのメッセージ】

論理的な思考ができていること、キッチリと論文を読む習慣が身につくように指導したい。RSA法などの公開鍵暗号の知識を前提とします。

【その他】

講義で扱うトピックスは、暗号分野でホットな話題にしたいので、8月中に確定して、9月に5日間の集中講義形式で行います。