広域数理科学概論 (4)

担当：内田　幸寛

講義の内容

現代の暗号理論では，楕円曲線を用いた暗号が盛んに研究され，また実際に利用されている．この講義では，楕円曲線とその一般化である超楕円曲線，それらの暗号理論への応用について講義する．具体的な内容は以下の通りである．ただし，状況に応じて変更することがある．

- 楕円曲線の群演算
- 有限体上の楕円曲線
- 楕円曲線暗号
- 超楕円曲線とそのヤコビアン
- 超楕円曲線暗号
- まとめ・レポート

テキスト・参考書等

教科書は特に指定しない．参考書として以下を挙げておく．

- 辻井重男，笠原正雄編著『暗号理論と楕円曲線』森北出版，2008.
- N. Koblitz, *Algebraic Aspects of Cryptography*, Springer, 1998（邦訳：林彬訳『暗号の代数理論』丸善出版，2012）.
- L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Chapman & Hall/CRC, 2nd ed., 2008.

成績評価方法

授業参加度 (30%)，レポート (70%) により評価する．

オフィスアワー

8 号館 6 階 667 室，水曜日 5 時限 (16:20–17:50)

ウェブページ

`http://www.comp.tmu.ac.jp/y-uchida/lectures/2016ko4/`

講義に関する情報をここに掲載する．