第11回

- 講演者 : **岡野 恵司** 氏 (都留文科大学)
  - 題目 : **ペアリング暗号に適した楕円曲線族の構成に関する報告**
  - 日時 : 平成28年10月5日（水）16:30 – 17:30

ペアリングに基づいた暗号方式は，適した楕円曲線(ペアリングフレンドリー 楕円曲線)が必要になる．その楕円曲線の族はある条件を満たす多項式たちか ら CM-法によって生成されるのであるが，そのような多項式の組としてさらに 「曲線の位数と暗号に使う部分群の位数がほぼ一致する」という理想的条件を もつものを探すことが，この分野の研究の一つとなっている．様々な構成法に よってより理想に近い族を探す試みがなされているが，現在までに知られてい る理想的条件をもつ曲線の完全族は唯一つである．実装に際しては様々な曲線 が必要であり，さらなる理想的曲線族の存在の有無について調べることが望ま れている．本講演ではこれまでの研究成果として，多くの場合に理想的曲線族 は存在せず，このような族で実用性あるものを見つけることはなかなか厳しい ということを報告する．

.lg-outer.lg-pull-caption-up.lg-thumb-open .lg-sub-html {bottom:80px;}

5 images