第14回

- 講演者：秋山 浩一郎 氏（東芝研究開発センター）
  - 題目：代数曲面を利用した新しい公開鍵暗号
  - 日時：平成20年2月1日（金）16:30-17:30

インターネットで商品を購入する際のクレジットカード番号送付など、 情報システムにおける機密情報を守る目的で、 整数論を応用した公開鍵 暗号が広く利用されています。 代表的な公開鍵暗号であるRSA暗号もこ の１つで、大きな整数の素因数分解が難しいことを安全性（解読の難しさ）の根拠としています。 しかし、量子計算機というこれまでとは違っ た原理で動作する計算機が出現すると、この素因数分解が容易となることが知られており、 将来に向けて別の安全性の根拠を持つ公開鍵暗号が 必要となっています。 本講演では、このような観点から量子計算機でも解読が困難となると期待できる代数曲面の求セクション問題に安全性の根拠をおく新しい公開鍵暗号を紹介します。（本研究は北海道教育大学　後藤泰宏氏との共同研究です。）

Warning, the folder related to namespace **seminar:2008:0201** does not exist.

From:
https://wiki.ma.noda.tus.ac.jp/ - **(旧)理工学部 数学科**

Permanent link:
https://wiki.ma.noda.tus.ac.jp/seminar/2007/014

Last update: **2017/11/17 15:19**