平成 19 年日本応用数理学会研究部会連合発表会
「数論アルゴリズムとその応用」(JANT) セッション

3 月 3 日, 4 日に開催される日本応用数理学会研究部会連合発表会におきまして, JANT のセッションを以下のように行います. 詳しくは次のページをご覧下さい.
http://ntw.e-one.uec.ac.jp/jant/2007spring.html

世話人　後藤丈志 (東京理科大学理工学部)

記

日時：平成 19 年 3 月 3 日 (土) 14:40–18:40
会場：名古屋大学 東山キャンパス 情報科学研究科棟

プログラム

14:40–15:10 小崎 俊二 (情報セキュリティ大学院大学 M2), 松尾 和人 (情報セキュリティ大学院大学)
種数 2 の超楕円曲線の 2 冪ねじれ点の計算アルゴリズムの改良

15:10–15:30 綱 友之 (早稲田大学大学院理工学研究科 D2)
種数 2 の超楕円曲線のヤコビアンの加法アルゴリズムについて

15:40–16:05 長沼 健 (東京大学大学院数理科学研究科 M2)
Monsky-Washnitzer cohomology を使った Fermat 曲線の位数計算アルゴリズム

16:05–16:25 Janice Asuncion (首都大学東京理学研究科 M2)
Integer Factorization Using Different Parameterizations of Montgomery's Curves

16:40–17:00 齋藤 健太郎 (首都大学東京理学研究科 M2), 中村 憲 (首都大学東京理工学研究科)
虚 2 次体のイデアル類群計算の実装

17:00–17:15 安江 健 (名城大学大学院理工学研究科 M2)
実二次体における基本単数の係数についての考察

17:15–17:40 西本 啓一郎 (首都大学東京理学研究科 M2), 中村 憲 (首都大学東京理工学研究科)
量子公開鍵暗号に対する数値実験およびその考察

17:50–18:10 田中 覚 (首都大学東京理学研究科 M2), 中村 憲 (首都大学東京理工学研究科)
ペアリングベースの楕円曲線暗号に適した曲線の構成法

18:10–18:40 荒井 研一 (信州大学大学院総合工学系研究科 D1), 岡崎 裕之 (信州大学大学院工学系研究科), 不破 泰 (信州大学大学院工学系研究科)
ペアリングを用いたグループ署名方式