第 4 回 ワ ー ク シ ョ ッ プ 開 催 案 内

ZeroBIO プロジェクト最終成果報告会

■日　時：　2010 年 3 月 11 日（木） ～ 12 日（金）13:30～

■場　所：　リゾーピア熱海 （〒413-0012 静岡県熱海市東海岸町 13-93, TEL 0557-83-5959）
http://reserve.resort.co.jp/hotels/smc/atami/index.html

■主　催：　ZeroBIO 研究プロジェクト　http://zerobio.cs.dm.u-tokai.ac.jp

（平成２１年度科学研究費補助金（基盤研究（B）「ゼロ知識証明を用いた非対称なリモートバイオメトリクス利用者認証」）

■開催趣旨

2007 年度より始まった本プロジェクトでは，生体認証における生体情報の漏洩を防止するためにゼロ知識証明などの暗号技術の適用を検討してまいりました．認証のたびごとに振舞いを変える生体の奥は深く，一ビットの誤りも許さない暗号理論との相性は悪く，他分野の融合は困難を極めることが分かってきました．ここまでの研究成果を振り返り，生体認証プロトコルにおけるオープン問題を整理することを目的として，次のような非公式な報告会を開催いたします．是非忌憚のないご意見をお聞かせいただけましたら幸いです．

■　プログラム

（11 日（木）13:30-17:00）

1. Zerobio プロジェクトの４年間　生体情報の曖昧さに対する取り組み　菊池　浩明（東海大学 教授）
2. 曖昧性を含んだ多項式を利用した非対称生体認証　　渡邊 幸聖 （静岡大学）
3. 特別講演　テンプレート保護型生体認証技術の安全性モデルに関する検討　高橋健太（日立製作所）
4. ゼロ知識証明を用いた生体認証プロトコルの安全性と秘密関数計算の可能性　佐瀬大治郎（東京工業大学大学院）

（夕飯）

5. 安全性証明に関するチュートリアル（仮題）　尾形　わかは（東京工業大学大学院 准教授）
6. HB-Familiry の構成と安全性の歴史　川合 豊（東京大学大学院）
7. エンターテイメント認証　　西垣　正勝（静岡大学 准教授）

（12 日（金） 9:00-12:00）

8. Fairplay によるマッチングアルゴリズムの実装　山本匠（静岡大学創造科学技術大学院）
9. 特別講演　秘密回路計算のパフォーマンスと今後の展望　千田浩司（NTT 情報流通プラットフォーム研究所）
10. NP 完全問題の応用，グラフ３彩色問題による試み　小田　雅洋（静岡大学情報学部）
11. 照合タグを用いた生体認証プロトコルの提案　青木良樹　（東海大学）
12. 非対称生体認証の今後の課題　（自由討論）

問い合わせ先：
菊池　浩明 東海大学情報通信学部通信ネットワーク工学科
Email: kikn@tokai.ac.jp