★情報理論研究会（IT）

専門委員長　大濱靖匡　副委員長　和田山　正
幹事　日下卓也・岩本　貢　幹事補佐　野村　亮

★情報セキュリティ研究会（ISEC）

専門委員長　櫻井幸一　副委員長　角尾幸保・満保雅浩
幹事　岩田　哲・花岡悟一郎　幹事補佐　伊豆哲也・川本淳平・駒野雄一・島　成佳・水木敬明

★ワイドバンドシステム研究会（WBS）

専門委員長　羽渕裕真　副委員長　前原文明・岡田　実
幹事　松波　勲・佐藤正知　幹事補佐　小澤佑介・中村　聡

日時　3月2日（月）　10：30～17：30
　　3日（火）　10：30～15：55

会場　北九州市立大学国際環境工学部ひびきのキャンパス（北九州市若松区ひびきの1-1．折尾駅から：「折尾駅西口」バス停乗車（33番・35番・63番・64番），「学研都市ひびきの」下車（約20分）後徒歩2分，黒崎駅から：「西鉄黒崎バスセンター」バス停乗車（急行鶴松団地行き），「学研都市ひびきの」下車（約25分）後徒歩2分．http://www.kitakyu-u.ac.jp/env/access.html　TEL〔093〕695-3269　松波　勲）

議題

2日午前　ISEC（10：30～11：45）

1. Accelerating QUAD Stream Cipher using Optimal Extension Field on GPU
　○Satoshi Tanaka（ISIT/Kyushu Univ.）・Chen-Mou Cheng（Kyushu Univ.）・Takanori Yasuda（ISIT）・Kouichi Sakurai（ISIT/Kyushu Univ.）
2. NTRUにAll One Polynomialを用いた方式の検討　○三隅晃輝・野上保之（岡山大）
3. 2次拡大体上の超特異楕円曲線を用いたペアリングの効率化
　○熊野晶斗・野上保之（岡山大）・白勢政明（公立はこだて未来大）

2日午後　ISEC（13：15～14：55）

4. 非線形関数ベースのストリーム暗号の構成に関する一考察　○反町　亨・内藤祐介（三菱電機）
5. 属性ベース集約署名の一構成　○高橋　遼・長谷川真吾・磯辺秀司・小泉英介・静谷啓樹（東北大）
6. 準同型暗号の安全性証明の限界について　○高橋大樹・長谷川真吾・磯辺秀司・小泉英介・静谷啓樹（東北大）
7. 多項式環に基づく完全準同型暗号のマルチキーへの拡張　○早藤智暉・満保雅浩（金沢大）

IT（13：40～14：55）

8. 軟判定復調における q 元線形符号の復号誤り率　○川島拓也・山口和彦（電通大）
9. 2種の振幅モーメントを用いたQAM識別における誤り率解析　○大野倫明・岡　育生・阿多信吾（阪市大）
10. 尤度を用いたQAMにおけるSN比推定　○西島慎二・岡　育生・阿多信吾（阪市大）

WBS（13：40～14：55）

11. UWBレーダによる複数移動目標検知識別法の高速化に関する実験的検討
　○大石庸平・井上昌信・自見圭司・松波　勲（北九州市大）
12. UWBレーダによる2次元環境マッピング法に関する実験的検討
　○自見圭司・井上昌信・大石庸平・松波　勲（北九州市大）
13. シミュレーションによるステップドFMセンサの相互干渉回避に関する検討
　○畑田翔一・松波　勲（北九州市大）

ISEC（15：10～16：25）

14. 動的信頼グラフを用いた匿名通信路の選択手法の提案　○篠原祐真・金子直史・斉藤友彦・鷲見和彦（青学大）
15. GHS攻撃の対象となる被覆曲線を持つ楕円曲線の同型類に関する考察
　○細萱隆之（中大）・飯島　努（光電製作所）・志村真帆呂（東海大）・趙　晋輝（中大）
16. 素体上ロジスティック写像による生成系列の自己相関と演算精度に近い周期を持つループについて
　○宮崎　武（北九州市大）・荒木俊輔（九工大）・上原　聡（北九州市大）・野上保之（岡山大）

IT（15：10～16：25）

17. オートマトンを用いた2次元の反辞書符号化法　○太田隆博（長野県工科短大）・森田啓義（電通大）
18. 改ざん攻撃を検出できる（k，n）しきい値秘密分散法　○中村　渉・山本博資（東大）
19. 情報とエネルギーの同時伝送を行う2ユーザ干渉通信路におけるアウテージ容量
　○大澤　豊・松本隆太郎・松田哲直・植松友彦（東工大）

WBS（15：10～16：25）

20. UWB レーダにおける位相モノパルス方式を用いた高精度形状推定に関する実験的検討
〇井上昌信・大石庸平・自見圭司・松波　勲（北九州市大）
21. 無人航空機を利用したユーザ位置検出手法における測位精度の特性評価　〇石川博康・小暮翔太（日大）
22. Towards Tokyo Olympics : 5G/P2P Hybrid Designs for Streaming to Massive Wireless Crowds
Marat Zhanikeev（Kyushu Inst. of Tech.）

ISEC（16：40〜17：30）

23. A rapid filtering rule management plane implementation using distributed in-memory caching system
Ruo Ando（NICT）
24. Arithmetic in a Prime Field of SWIFFT/SWIFFTX　Hidenori Kuwakado（Kansai Univ.）

IT（16：40〜17：30）

25. 離散無記憶通信路に対して許容できる相互情報量の条件下で出力記号数を削減するアルゴリズム
〇永原拓実・阪井祐太・岩田賢一（福井大）
26. 一般情報源に対する Slepian-Wolf 符号化問題の 2 次の ε-達成可能レート領域の別表現
〇齋藤翔太・宮　希望・松嶋敏泰（早大）

WBS（16：40〜17：30）

27. ノード飛び越しするマルチホップ通信における経路形状を考慮したスループット解析
〇三村昂平・大内浩司（静岡大）
28. 高速伝送のためのブロック拡散 ZCZ-CDMA について
〇黒田　翔（エフエクスシステムズ）・小林一宏・井田悠太・松元隆博・松藤信哉（山口大）

3 日午前　ISEC（10：30〜11：45）

1. 市販トランプカードを用いた安全な計算について　水木敬明（東北大）
2. 秘密鍵に三系列の乱数を用いるナップザック暗号
〇村上恭通（阪電通大／中大）・濱正真佑（阪電通大）・笠原正雄（早大／中大）
3. スパース構造学習を用いた異常検知によるボットネット検出実験
〇向井　脩・川村勇気・川喜田雅則・竹内純一（九大）

IT（10：30〜11：45）

4. L1 罰則付き線形回帰の MDL による推定誤差上界について　〇豊暉原侑心・川喜田雅則・竹内純一（九大）
5. 拡大体上の定重み系列における線形複雑度について
〇戒田高康（近畿大）・鄭　俊如（九州女子大）・高橋圭一（近畿大）
6. Toward Implementation of Algebraic Coding for Wiretap Channels　Mitsuru Hamada（Tamagawa Univ.）

WBS（10：30〜11：45）

7. 音響電子機器を活用した音響通信用のチャネルサウンダに関する検討
〇市川貴英・清水崇司・相澤　大・久保博嗣（立命館大）
8. ネットワーク符号化位相変調とその Per-Survivor Processing によるブラインドスタートアップが可能な復調方式
〇道尾　涼・久保博嗣（立命館大）
9. 高速時変伝送路に適した差動時空符号化とその無線通信システムへの応用
〇中村洸貴・宮崎律子・久保博嗣（立命館大）

3 日午後　IT/ISEC/WBS 招待講演（13：15〜14：05）

10.〔招待講演〕 暗号方式の高速で安全な実装と実用化　川村信一（東芝）

IT/ISEC/WBS 招待講演（14：10〜15：00）

11.〔招待講演〕 線形符号の相対パラメータによって表される秘密分散法の安全性
〇栗原　淳（KDDI 研）・松本隆太郎・植松友彦（東工大）

IT/ISEC/WBS 招待講演（15：05〜15：55）

12.〔招待講演〕 生体情報センシングのための UWB 電波センサの開発試作　梶原昭博（北九州市大）

◆IEEE IT Society Japan Chapter 共催
☆IT 研究会

【問合先】

IT 研究会幹事，幹事補佐
E-mail：it-sec@mail.ieice.org

☆ISEC 研究会

【問合先】

岩田　哲（名大）
TEL〔052〕789-5722，FAX〔052〕789-5723
E-mail：isec-sec@mail.ieice.org（幹事，幹事補佐宛）

☆WBS 研究会

【問合先】

松波　勲

TEL & FAX〔093〕695-3269

E-mail：i-matsunami@kitakyu-u.ac.jp