★情報理論研究会（IT）
専門委員長　小嶋徹也　副委員長　野上保之
幹事　松田哲直・眞田亜紀子　幹事補佐　野崎隆之

★情報セキュリティ研究会（ISEC）
専門委員長　國廣　昇　副委員長　四方順司・花岡悟一郎
幹事　松田隆宏・米山一樹　幹事補佐　花谷嘉一

★ワイドバンドシステム研究会（WBS）
専門委員長　庄納　崇　副委員長　石川博康・落合秀樹
幹事　荒井　剛・木下雅之　幹事補佐　孫　冉・陳　娜

★高信頼制御通信研究会（RCC）
専門委員長　東　俊一　副委員長　小林孝一・石井光治
幹事　加川敏規・岡野訓尚　幹事補佐　単　麟・足立亮介

日時　3月14日（火）　9：00～18：05
　　15日（水）　9：30～16：35
会場　山口大・常盤キャンパスD講義棟1，2階（宇部市常盤台2丁目16-1　JR宇部線宇部新川駅→宇部市営バス開線・萩原（開）循環線，ひらき台行き→工学部前バス停→徒歩3分→常盤キャンパス（工学部）．https://www.yamaguchi-u.ac.jp/info/campus_map/access_ubechiku/index.html　電気電子工学科　足立亮介）
議題　RCC・ISEC・IT・WBS合同研究会
14日午前　WBS1（D21）（9：00～10：15）
1. 流星バースト通信における伝送路モデルの改良とインドネシア実証実験結果の比較
　○岩崎寛人・椋本介士・和田忠浩（静岡大）
2. 流星バースト通信へのマルチレシーバシステムの適用に関する一考察
　○加山　巧・椋本介士・和田忠浩（静岡大）
3. 仮想画像に基づく画像分類器を用いる可視光通信システムの提案
　○内藤正崇・和田忠浩・椋本介士（静岡大）・岡田　啓（名大）
IT2（D21）（10：30～11：20）
4.〔招待講演〕 セキュリティを考慮した2つの問題に対する情報理論的解析について―Local Differential Privacyの下でのパラメータ推定問題と，プライバシーと有用性のトレードオフ問題―　齋藤翔太（群馬大）
ISEC1（D22）（9：00～10：15）
5. 第2-Meスカラー倍と相性の良い正の有理数上の演算oplusの提案―第2-Meスカラー倍による楕円曲線署名の類似の構成―　白勢政明（公立はこだて未来大）
6. Security Anslysis of binary elliptic curve GLS254
　○Yue Gao（Osaka Univ.）・ShuFan Wu（Taiwan Univ.）・Atsuko Miyaji（Osaka Univ.）
7. エラー付きbinary GCD演算系列を用いたRSA秘密鍵の完全復元　○谷　健太・國廣　昇（筑波大）
ISEC2（D22）（10：30～12：10）
8. 部分体上のRing-LWE問題に対する安全性解析　○上杉慧至・奥村伸也・宮地充子（阪大）
9. 円分体の部分体における耐量子安全なModule-LWEに対する安全性解析　田村昂輔（阪大）
10. 同種写像暗号における超楕円曲線間の同型写像計算コストについて
　林田大輝（三菱電機）・○石井将大（東工大）
11. Analysis of（U, U＋V）-code Problem with Gramian over Binary and Ternary Fields
　○Ichiro Iwata・Yusuke Yoshida・Keisuke Tanaka（Tokyo Inst. of Tech）
IT1（D12）（9：00～10：15）
12. A Study on Secure Coded Communications Using Two-Dimensional Discrete Fourier Transform
　○Shoichiro Yamasaki（Hiroshima City Univ.）・Tomoko K. Matsushima（Yokohama College of Commerce）・Hirokazu Tanaka（Hiroshima City Univ.）
13. 複数回のハッシュ化双方向通信を用いた鍵共有プロトコルの鍵レートについて
　○和田康宏・渡辺　峻（東京農工大）
14. エンタングルメント純粋化・蒸留に関する情報スペクトル的研究　○阿知波宗輝・小川朋宏（電通大）
14日午後　RCC1（D21）（13：00～14：15）
15. 時相論理仕様を満足するマルチエージェント監視システムの強化学習における報酬分配について

○寺嶋啓太・小林孝一・山下　裕（北大）
16. GPS 及び QZSS のスプーフィング信号生成　○河崎雄太・石井光治（香川大）
17. 高精度時空間同期技術を活用した秘匿通信　○世永公輝・志賀信泰・安田　哲・滝沢賢一・吉田真紀（NICT）

WBS2（D21）（14：55〜16：35）

18. セキュリティギャップに基づく Polar 符号の設計に関する検討　○松井秀赳・松峯利樹・落合秀樹（横浜国大）
19. High Speed Optical Wireless Uplink using MU-MIMO with Angle Diversity
○Xuejuan Zhu・Chedlia Ben Naila・Hiraku Okada・Masaaki Katayama（Nagoya Univ.）
20. 4PPM 空間分割多重スクリーンによるアップリンク可視光通信の物理層セキュリティ強化
○川出有紗・中條　渉・小林健太郎（名城大）
21. LED 設置位置の異なるプロペラ型回転式 LED 送信機を用いたイメージセンサ通信の性能評価
○尺田一輝・荒井伸太郎（岡山理科大）

RCC2（D21）（16：50〜17：40）

22.〔招待講演〕 高周波数帯端末連携によって実現する新たな無線通信システム　村田英一（山口大）

ISEC3（D22）（13：00〜14：40）

23. 格子に基づく多権限属性ベース署名　○金子悠人・冨田斗威・四方順司（横浜国大）
24. 同種写像暗号 OSIDH に基づく署名方式
○青柳光太郎（豊橋技科大）・南出大樹（東京高専）・鈴木幸太郎（豊橋技科大）
25. トレース写像を用いた効率的な Ring-LWE ベース暗号の構成手法について
○大久保佑弥（阪大）・宮地充子（阪大／北陸先端大）・奥村伸也（阪大）
26. PQC 署名アルゴリズム QR-UOV の高位合成による FPGA 実装と性能評価
○山越公洋・清村優太郎・齋藤恆和（NTT）

ISEC4（D22）（14：55〜16：35）

27. web3.0 上での利用に適した主張機能と否認機能をもつリング署名の構築
○上原真悟・宮地充子（阪大）・デン ヨウコウ（サリー大）
28. 属性ベース検索可能暗号について　○雨宮幸太郎・冨田斗威・四方順司（横浜国大）
29. 署名した事実を開示可能な検証者指定署名方式
○山下恭佑（阪大）・原　啓祐（産総研／横浜国大）・渡邉洋平（電通大／ジャパンデータコム）・矢内直人（阪大／ジャパンデータコム）・四方順司（横浜国大）
30. 鍵生成センタに対して安全な ID ベースマッチメイキング暗号
○知久奏斗（横浜国大）・原　啓祐（産総研／横浜国大）・四方順司（横浜国大）

ISEC5（D22）（16：50〜18：05）

31. DIP 法における適切なホールドアウトサンプルの割合の推定法　○川原尚己・宮地充子（阪大）
32. 非線形な機械学習手法に適した局所差分プライバシーメカニズムの評価
○山月達太・ハー ビンチャン・山下慎太郎（阪大）・宮地充子（阪大／北陸先端大）・三本知明（ATR）
33. GAN を用いた個人情報レコードの多様化　○蒋　程曦・王　天澄・森田　光（神奈川大）

IT3（D12）（13：00〜14：40）

34. Exponential Strong Converse for Source Coding with Encoded Side Information—Comparison with Source Coding with Non-encoded Side Information—
○Daisuke Takeuchi・Shun Watanabe（Tokyo Univ. of Agriculture and Technology）
35. Minimum-Entropy Coupling 問題に対する貪欲アルゴリズム　柴田泰成・○岩田賢一・橋本健吾（福井大）
36. N ビットの復号遅延を許容するアルファベティック符号の構成法
植田大智・○岩田賢一（福井大）・山本博資（東大）
37. LZ78 符号とそのバリエーションを用いた文法圧縮の構成　有村光晴（湘南工科大）

IT4（D12）（14：55〜16：10）

38. 強化学習を用いた LoRaWAN の衝突回避ためのユーザ待機時間の制御
○大津佳都・路　姗・鎌部　浩（岐阜大）
39. t-分布を用いたスパース Bayes 線形回帰モデルに関する推定性能　村山一明（電通大）
40. 最適な量子測定に基づく量子ニューラルネットワーク分類器の性能特性　○山田優作・鈴木　淳（電通大）

15 日午前　RCC3（D12）（9：30〜10：45）

1. スパース最適化による高次元マルチエージェントシステムの合意ダイナミクス設計
○足立亮介・若佐裕治（山口大）
2. 未来地図を用いた搬送ロボットの制御　○松高亜樹（名大）・東　俊一（京大）・有泉　亮・浅井　徹（名大）
3. 産業用ロボットの無線操作における不完全な通信の補完を用いた作業品質改善手法
○高城洋介・ベン ナイラ シャドリア・岡田　啓・片山正昭（名大）

WBS3（D12）（11：00～11：50）

4.〔招待講演〕 Beyond 5G/6G 時代の大容量通信を実現するテラヘルツ帯を活用した仮想化端末技術
　○林　高弘・國澤良雄・長尾竜也・竹澤和輝・伊藤智史・松野宏己・山崎浩輔・岸　洋司（KDDI 総合研究所）

ISEC6（D22）（9：30～10：45）

5. CNN で抽出した特徴量に基づく VAE によるネットワークの異常検出
　○東畑和希（阪府大）・青木茂樹・宮本貴朗（阪公立大）

6. 機械学習を用いたデジタルフォレンジックのためのログ自動判別システムの検討
　○岩崎晃大・岸本頼紀（東京情報大）

7. Designing for Supply Chain Network Model with Disruption Risk by Hybrid GA and Enhanced Jaya Algorithm
　○Mitsuo Gen（Fuzzy Logic Systems Inst.）・YoungSu Yun・Tserendulam Erdenebaatar（Chosun Univ.）

ISEC7（D22）（11：00～12：15）

8. ハッシュ関数の連結リストを用いる Garbled Circuit の構成法　○劉　広健・王　天澄・森田　光（神奈川大）

9. カード入力を制限することで段階をダウングレードするリッカート尺度入力カードベースプロトコルの構成
　須賀祐治（IIJ）

10. グラフスペクトルを用いたグラフに対するステガノグラフィ
　○川口和久・豊永憲治（豊橋技科大）・高橋茶子（山形大）・中井雄士・鈴木幸太郎（豊橋技科大）

IT5（D12）（9：30～10：45）

11. BICM システムにおける組織的構成法に基づく幾何学シェイピングの検討　○栗原英人・落合秀樹（横浜国大）

12. PAC 符号の SCF-Fano 復号を用いた性能改善　○小川響生・鎌部　浩・路　サン（岐阜大）

13. Efficient composition of encoding polynomial in distributed coded computing scheme
　○Daisuke Hibino・Tomoharu Shibuya（Sophia Univ.）

15 日午後　WBS4（D12）（13：00～14：40）

14.（k, n）視覚復号型秘密分散法によるデータ分散照明光通信システム
　○幡豆亮平・小澤佑介・羽渕裕真（茨城大）

15. 角度ダイバーシティ受信機を用いた海中可視光通信のための FOV 最適化に関する検討
　○松永彗吾・小澤佑介・羽渕裕真（茨城大）

16. RGB-LED アレイを用いた海中光カメラ通信の平均ビット誤り率解析に関する一検討
　○横尾和音・小澤佑介（茨城大）・澤　隆雄（海洋研究開発機構）

17. RGB-LED 並列伝送法における変形 MPPM フレーム同期法　○羽渕裕真・松島　丈（茨城大）

WBS5（D12）（14：55～16：35）

18.〔招待講演〕テラヘルツ帯表面電磁波共振器とその機能デバイス応用
　○四方潤一・岩川優也（日大）・大野誠吾（東北大）

19. 予測型ドローン配置による効果的なトラフィックオフロードの特性評価　○市川壮太郎・田久　修（信州大）

20. 無人航空機を用いたユーザ位置検出システムにおけるドップラーシフト多重観測手法の測位精度改善効果
　出口泰河・○石川博康（日大）

ISEC8（D22）（13：00～14：40）

21. 共用端末を用いた自己主権型アイデンティティシステムにおける属性情報保護方法の提案
　○中村　渉・高橋健太（日立）

22. 一般化 Unicity Distance とその Y-00 量子暗号への応用　相馬正宜（玉川大）・○廣田　修（中大）

23. 耐量子計算機暗号と量子鍵配送を利用したハイブリッド鍵共有に関する一考察
　○知加良　盛・齋藤恆和・清村優太郎（NTT）

24. NFT の一意存在性実現のための暗号証明系の応用に関する考察　櫻井幸一（九大）

ISEC9（D22）（14：55～16：35）

25. Keccak〔r＝40, c＝160, nr＝2〕における原像計算時間に関する実験
　○戚　莘鈺・藤岡　淳（神奈川大）・青木和麻呂（文教大）

26. ブロック暗号 Midori の関連鍵差分攻撃評価とその対策
　○平尾星音・堀部佳吾・阪本光星・五十部孝典（兵庫県立大）

27. Salsa における線形差分攻撃　○李　君如・宮地充子（阪大）

28. Sub-Block Dividing を用いた Type-2 一般化 Feistel 構造に対する MILP による Active S-box 数解析
　○岡崎雅哉・岩田　哲（名大）

IT6（D12）（13：00～14：40）

29. 共有乱数を利用した分散情報消去における達成可能コスト領域　松田哲直（埼玉大）

30. 一般のアクセス構造に対するランプ型秘密分散法の最適な構成について　黒川周吾・○古賀弘樹（筑波大）

31.（t, n）しきい値型の視覚暗号における n 枚重ねたときの相対差の最適値について　古賀弘樹（筑波大）

32. 背景色によって復号の可否が変わる視覚復号型秘密分散法の設計について
〇丸井惇司・廣友雅徳（佐賀大）・白石善明（神戸大）

◆IEEE IT Society Japan Chapter 共催

◎D12，D22 教室のプロジェクターは 4：3 です．D21 教室のプロジェクターは 16：9 にも対応します．

☆IT 研究会

【問合先】

IT 研究会幹事

眞田亜紀子（長岡技科大）・松田哲直（埼玉大）・野崎隆之（山口大）

E-mail：it-sec@mail.ieice.org

☆ISEC 研究会

【問合先】

松田隆宏（産総研）

E-mail：isec-sec@mail.ieice.org

☆WBS 研究会

【問合先】

WBS 研幹事団

E-mail：wbs-kanjidan@mail.ieice.org

☆RCC 研究会

【問合先】

RCC 研究会幹事団

E-mail：rcc-sec@mail.ieice.org

◎http://www.ieice.org/~rcc/