★情報理論研究会（IT）
専門委員長　和田山　正　副委員長　小嶋徹也
幹事　松田哲直・野崎隆之　幹事補佐　廣友雅徳

★情報セキュリティ研究会（ISEC）
専門委員長　伊豆哲也　副委員長　國廣　昇・花岡悟一郎
幹事　山本　大・米山一樹　幹事補佐　松田隆宏

★ワイドバンドシステム研究会（WBS）
専門委員長　浜村昌則　副委員長　庄納　崇・藤井雅弘
幹事　中村僚兵・小室信喜　幹事補佐　木下雅之・孫　冉

★高信頼制御通信研究会（RCC）
専門委員長　李　還幇　副委員長　東　俊一・石井光治
幹事　加川敏規・林　直樹　幹事補佐　単　麟・小蔵正輝

日時　3月10日（木）　9：40～17：40
　　11日（金）　9：40～17：30
会場　オンライン開催
議題　ISEC・IT・RCC・WBS 合同研究会
10日午前　IT 1（04 会議室）（9：40～10：55）
1. 1ビットの秘密情報に対する秘密分散法に同値な条件とその拡張　○岡村　亮・古賀弘樹（筑波大）
2. 複数のアクセス構造をもつ最適な視覚暗号の構成について　○五百木来樹・古賀弘樹（筑波大）
3. 1符号語の伝送時間及びエネルギーに制限を付した通信路におけるランダム符号と Polar 符号の性能評価
　○横澤一晟・植松友彦（東工大）
IT 2（04 会議室）（11：10～12：25）
4. BICM に適したポーラ符号における polarization 重みを用いた情報ビット選択の検討
　○黒須礼尚・ヤチョンカ ワムア・八木秀樹（電通大）
5. 組織型 Polarization-Adjusted Convolutional 符号を用いた Hybrid-ARQ 方式
　○旭　瑞歩・ヤチョンカ ワムア・八木秀樹（電通大）
6. 時間的に変化する通信路におけるレートレス PAC 符号の検討
　○ワムア ヤチョンカ・黒須礼尚・旭　瑞歩・八木秀樹（電通大）
ISEC 1（03 会議室）（9：40～10：55）
7. 算術回路に対する GKW 変換の構成　○知念広太郎・穴田啓晃（長崎県立大）
8. 分散型追跡可能属性ベース証明書スキームの一般的構成とその安全性　○安在恭弥・穴田啓晃（長崎県立大）
9. 短いメッセージに適した閾値署名の提案　○猪本卓也（阪大）・宮地充子（阪大／北陸先端大）
ISEC 2（03 会議室）（11：10～12：25）
10. 同種写像問題に基づく耐量子決定的ウォレット　○ムハマド ウスマーン・米山一樹（茨城大）
11. An extension of the CRS scheme using descending chains
　○Jiawei Chen・Hyungrok Jo・Junji Shikata（Yokohama National Univ.）
12. 準同型暗号上の CNN における活性化関数の最適化による分類精度向上
　○柳生航平・竹内　簾・ヴォ ゴック コイ グエン・西垣正勝・大木哲史（静岡大）
WBS 1（05 会議室）（9：40～10：55）
13. 流星バースト通信のための Polar 符号化再送制御パケットの提案　○小林　暁・椋本介士・和田忠浩（静岡大）
14. ミリ波高速チャープ変調レーダを用いた複数のドローンの検知に関する基礎的検討
　○黒崎将史・中村僚兵・葉玉寿弥（防衛大）
15. 動画像への情報埋め込みによる並列伝送型可視光通信システムの一提案
　○伊藤諒祐・和田忠浩・椋本介士（静岡大）・岡田　啓（名大）
WBS 2（05 会議室）（11：10～12：50）
16. ロールオフ波形整形を行う WHCDM の初期捕捉方式に関する一検討　○小松央次郎・小島年春（電通大）
17. キャリア周波数オフセット耐性を改善した MWHCDM 初期捕捉方式　○山村洋太・小島年春（電通大）
18. ガウス盗聴通信路に適した BICM のビットラベリング最適化に関する検討
　○松峯利樹・落合秀樹・四方順司（横浜国大）
19. 不完全ブロック対角化法を用いた MU-MIMO マルチストリーム伝送に関する研究

○佐藤正知・大迫智之・井手輝二（鹿児島高専）

10 日午後　IT3（04 会議室）（13：50〜15：05）

20. Reed-Muller Code Lattice Decoding with Weighted BP Decoder　○Ryoji Shimizu・Brian M. Kurkoski（JAIST）
21. LDGM 符号化器の学習に基づく有歪み情報源符号化　○小川一樹・井坂元彦（関西学院大）
22. 機械学習に基づく情報源符号化の一検討　○松浦　駿・井坂元彦（関西学院大）

IT 招待講演（04 会議室）（15：45〜16：35）

23.〔招待講演〕 ビザンチンエージェントが混在する環境におけるモバイルエージェントの集合問題
首藤裕一（法政大）

IT 特別招待講演（04 会議室）（16：50〜17：40）

24.〔特別招待講演〕 情報理論研究の広がりと面白さ　山本博資（東大）

ISEC 3（03 会議室）（13：50〜15：05）

25. アーベル曲面上の同種写像計算の explicit formulae に関する一考察
○林田大輝（三菱電機）・石井将大（東工大）
26. 有限体上のトレース写像を利用した Search Ring-LWE 問題への攻撃について
○高橋朋伽・奥村伸也・宮地充子（阪大）
27. Ring-LWE の定義体と Progressive-BKZ アルゴリズムを用いた格子攻撃
○上杉慧至・奥村伸也・宮地充子（阪大）

RCC 1（05 会議室）（13：50〜15：05）

28. センサアクチュエータネットワークの分散イベント駆動型出力フィードバック制御
○北村洸一・小林孝一・山下　裕（北大）
29. オープンな有向グラフにおける不等式制約付き分散オンライン最適化
○澤村吏貴・林　直樹・乾口雅弘（阪大）
30. ネットワーク中心性を用いたデータ駆動型合意制御におけるクラスタリング手法の最適化に関する検討
○小川翔也・石井光治（香川大）

11 日午前　RCC 招待講演（04 会議室）（9：40〜10：30）

1.〔招待講演〕 暗号化制御システムの基礎とその安全性について　○小木曽公尚・寺西　郁（電通大）

IT 4（04 会議室）（11：10〜12：25）

2. 整数 m の仲上 m フェージング環境下での重畳符号化協調通信の有限長伝送における平均ブロック誤り率の理論解析　○酒井陽平・神原征弥・木村共孝・程　俊（同志社大）
3. 部分アクセス IDMA システムにおける電力制御及び SNR 発展法による性能評価
○山岸雅弥・木村共孝・程　俊（同志社大）
4. 深層展開に基づく分散型 MIMO 信号検出法に関する検討　○熊谷雅也・中井彩乃・和田山　正（名工大）

ISEC 4（03 会議室）（11：10〜12：25）

5. 改竄を修復可能なメッセージ認証コード　○古谷　勇・井上明子・峯松一彦（NEC）
6. AES instruction を用いたラージブロック置換の改良とその応用
○中橋元輝・芝　廉太朗・阪本光星・Liu Fukang（兵庫県立大）・伊藤竜馬（NICT）・峯松一彦（NEC）・五十部孝典（兵庫県立大/NICT/JST）
7. Reduced SHA-256 と SHA-512 に対する量子衝突攻撃における量子ビット数の削減
○福村春樹・米山一樹（茨城大）

WBS 3（05 会議室）（11：10〜12：25）

8. 時間分割型 USLIPT における最適 CSK 信号点空間拡張に関する検討
○向後拓磨・小澤佑介・羽渕裕真（茨城大）
9. 低輝度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）
10. VN-CSK 型 RGB 並列伝送における光フィンガープリント法
○垂石興起・小川大輔・小澤佑介・羽渕裕真（茨城大）

11 日午後　IT 5（04 会議室）（14：05〜15：20）

11. マルチレター Ahlswede-Han スキームによる排他的論理和計算の達成可能レート
○柿島拓斗・渡辺　峻（東京農工大）
12. 分散仮説検定におけるランダムビン符号化について　渡辺　峻（東京農工大）
13. On Strong Converse Theorem for Distributed Hypothesis Testing Problem　Yasutada Oohama（UEC）

11 日午後　IT 6（04 会議室）（15：35〜16：50）

14. The explicit formula for the distributions of the nonoverlapping words　Hayato Takahashi（Random Data Lab.）
15. 量子スピンチェイン上のダイバージェンスレートと状態の漸近変換　○土谷知靖・小川朋宏（電通大）

16. マッハ 10 を超える飛翔体に対応する量子レーダの基礎研究　　廣田　修（中大）

ISEC 5（03 会議室）（14：05〜15：20）

17. 共通鍵暗号方式 Rocca の設計と安全性評価　　○阪本光星・劉　富康（兵庫県立大）・仲野有登・清本晋作（KDDI 総合研究所）・五十部孝典（兵庫県立大／NICT）
18. 共通鍵暗号方式 Rocca の実装評価　　○仲野有登（KDDI 総合研究所）・阪本光星・劉　富康（兵庫県立大）・清本晋作（KDDI 総合研究所）・五十部孝典（兵庫県立大／NICT）
19. ストリーム暗号 ChaCha における線形バイアスの理論的解析　　○和泉　海・宮地充子（阪大）

ISEC 6（03 会議室）（15：35〜17：15）

20. Transformation Protocol における Unable Combine Portion に対する評価関数の改善
    ○滝田隆之介・小泉康一・大槻正伸（福島高専）
21. 改良した Key Set Protocol で得られる秘密鍵の平均ビット長解析
    ○雲藤剛志・小泉康一・大槻正伸（福島高専）
22. Garbled Circuit の効率的な構成法　　○劉　広健・森田　光（神奈川大）
23. Improvement of Extended-NBC and its Approximate Numerical Calculation Method
    ○Tanziah Khanam・Hikaru Morita（Graduate School of Kanagawa Univ.）

WBS 4（05 会議室）（14：05〜15：20）

24. 擬直交 M 系列対による 2 乗検波型 M-ary 変調方式の特性　　○梁　勲・李　根・羽渕裕真（茨城大）
25. 視覚情報の劣化をデータの高速切替によって軽減するディスプレイ-カメラ可視光通信システム―視覚品質と通信品質による評価―
    ○林　大雅・岡田　啓（名大）・小林健太郎（名城大）・和田忠浩（静岡大）・ベンナイラ シャドリア・片山正昭（名大）
26. 水中可視光通信のための角度ダイバーシティ受信機を用いた背景光雑音軽減法に関する検討
    ○松永彗吾・小澤佑介・羽渕裕真（茨城大）

WBS 5（05 会議室）（15：35〜16：25）

27. 揺動を伴う対船舶水中光無線通信の複数送受光器と空間次元符号化による特性改善手法
    ○安藤仁志・ベンナイラ シャドリア・岡田　啓・片山正昭（名大）
28. 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シンボル同期の一検討
    ○中山晃典・荒井伸太郎（岡山理科大）

RCC 2（05 会議室）（16：40〜17：30）

29. Polar 符号の逐次除去復号における SNR ミスマッチに関する検討　　○池谷恒亮・落合秀樹（横浜国大）
30. パイロット狭帯域無線センシングを用いた UWB チャネルアクセス制御の提案
    ○李　還幇・松村　武（NICT）

◆IEEE IT Society Japan Chapter 共催

☆IT 研究会

【問合先】

IT 研究会幹事団
松田哲直（埼玉大）・野崎隆之（山口大）・廣友雅徳（佐賀大）
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】

荒井伸太郎（岡山理科大）
E-mail：arai@ee.ous.ac.jp

☆RCC 研究会

【問合先】

E-mail：rcc-sec@mail.ieice.org

◎http://www.ieice.org/~rcc/