★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　野崎隆之・廣友雅徳　幹事補佐　太田隆博

★情報セキュリティ研究会（ISEC）

専門委員長　廣瀬勝一　副委員長　伊豆哲也・國廣　昇
幹事　面　和成・山本　大　幹事補佐　米山一樹

★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　荒井伸太郎・中村僚兵　幹事補佐　Duong Quang Thang・森山雅文・木下雅之

日時　3月4日（木）　9：00～17：15
　　5日（金）　9：00～16：15
会場　オンライン開催（Zoom, Webex, EventIn）
議題　WBS・IT・ISEC 合同研究会

4日午前　オンライン会場 A : IT 1（9：25～10：40）

1. Polar 符号の逐次除去リスト復号における枝刈りのためのパリティチェックの構成
　○大木湧介・柴田　凌・八嶋弘幸（東京理科大）
2. 光符号分割多元接続のための可変拡散率符号の提案　○小野恭平・山嵜彰一郎・松嶋智子（職能開発大）
3. チップペア符号を用いた同期光符号分割多元接続方式の誤り率特性
　○松嶋智子・山嵜彰一郎・小野恭平（職能開発大）

オンライン会場 A：IT 2（10：55～12：10）

4. 区間ごとに文脈木モデルが変化する情報源における効率的ベイズ符号化アルゴリズム
　○島田航志・齋藤翔太・松嶋敏泰（早大）
5. CSE 法における再構成可能な部分文字列の十分条件に関する一考察
　○田中駿伍・鎌部　浩・路　サン（岐阜大）
6. Streaming Data Compression and Decompression by One-Way Quantum Finite State Automata, leading to Quantum Finite State Deep and Shallow Information　Tomoyuki Yamakami（Univ. of Fukui）

オンライン会場 B：ISEC 1（9：00～10：40）

7. Tweakable ブロック暗号を用いた 4 ブロックの Type-2 Feistel 暗号　○中家一輝・岩田　哲（名大）
8. 軽量ブロック暗号 MANTRA に対する Bit-Based Division Property を用いた Integral 攻撃
　○小松宏輝・五十嵐保隆・金子敏信（東京理科大）
9. M6 の線形解析における MILP 探索と計算機シミュレーションの比較
　○金川創治郎・五十嵐保隆・金子敏信（東京理科大）
10. Salsa20 の入力／出力差分の新たな線形バイアスの解析　○渡辺　暸・宮地充子（阪大）

オンライン会場 B：ISEC 2（10：55～12：35）

11. アニーリング計算を用いた最短ベクトル問題の求解―疑似マルチスピンフリップを用いたハミルトニアン生成―
　○山口純平（富士通研）・大輪拓也（九工大）・古川和快（富士通研）
12. 相対次数が偶数の場合における探索 Ring-LWE 問題への攻撃について
　○奥村泰久・奥村伸也・宮地充子（阪大）
13. No-dummy CSIDH における fault injection 攻撃について　○新井颯斗・宮地充子・小寺健太（阪大）
14. 同種写像暗号の並列計算手法の効率化　○宇谷亮太・鈴木幸太郎（豊橋技科大）

4日午後　オンラインポスターセッション：WBS，IT（13：20～14：40）

15.〔ポスター講演〕 回転式 LED 送信機を用いたイメージセンサ通信における Alamouti 型時空間符号化の実験評価
　○唐　正強・荒井伸太郎（岡山理科大）・山里敬也（名大）
16.〔ポスター講演〕 PAPR 低減を目的としたディザ信号を付加した ACO-OFDM 方式の特性評価
　原田大樹（静岡大）
17.〔ポスター講演〕 時間領域において一部欠落した OFDM 信号の復元
　○劉　承博・陳　娜・岡田　実（奈良先端大）
18.〔ポスター講演〕 OFDM と DFT-Precoded OFDM を併用した秘匿通信におけるフェーディング通信路下での受信特性評価　○金子愛理・落合秀樹・四方順司（横浜国大）
19.〔ポスター講演〕 デュアルカメラを用いた選択受信によるローリングシャッタ型可視光通信性能の改善
　○茨木大空・戸熊拓海・山口　駿・木下雅之・鎌倉浩嗣（千葉工大）・山里敬也（名大）

20.〔ポスター講演〕 Non-asymptotic converse theorem on the overflow probability of variable-to-fixed length codes
○Shota Saito・Toshiyasu Matsushima（Waseda Univ.）

オンライン会場 A：IT 3（14：55～16：10）

21. シェアの回転により秘密画像を復元できる視覚暗号の最適な構成法　○関根恭平・古賀弘樹（筑波大）
22. 線形符号を用いた evolving 型の秘密分散法に関する一検討　鳥海大希・○宮　希望・地主　創（青学大）
23. データベースごとに限度の異なる問い合わせの情報漏洩を許した秘匿情報検索における通信容量の上界と下界
○豊田修与・松田哲直・植松友彦（東工大）

オンライン会場 A：招待講演（WBS）（16：25～17：15）

24.〔招待講演〕 IOWN における 6G 時代に向けた複数無線アクセスの活用　鷹取泰司（NTT）

オンライン会場 B：ISEC 3（14：55～16：10）

25. 二面体カードを用いた覆面算に対する物理的ゼロ知識証明
○五十鈴川頼宗（東北大）・宮原大輝・水木敬明（東北大／産総研）・曽根秀昭（東北大）
26. 物理暗号通信システムに向けた安全性解析の基本諸原理について　加藤研太郎（玉川大）
27. A Real-Time Bluetooth Protocol Fuzzing System
○Bo Wang・Ako Suzuki（JVCKW）・Yuichi Kaji（Nagoya Univ.）

5 日午前　オンライン会場 A：WBS 1（9：25～10：40）

1. WFrFT を利用したキャリア周波数オフセットとシンボル時間オフセットのブラインド推定
○小島利文・大内浩司（静岡大）
2. 色間電力の異なる RGB-LED 照明を用いる VN-CSK 型並列屋内照明光通信の性能評価
○垂石興起・羽渕裕真・小澤佑介（茨城大）
3. Indoor Long Distance High Speed Imaging MIMO System With Linear Transmitting Element Array
○Chedlia Ben Naila・Hiraku Okada・Masaaki Katayama（Nagoya Univ.）

オンライン会場 A：WBS 2（10：55～11：45）

4. 障害物検知用ミリ波レーダを用いた車速及び走行距離の推定　○自見圭司・小木津武樹（群馬大）
5. FMCW レーダにおけるレプリカ信号を用いた干渉低減法に関する一検討　○田幸史也・大野光平（明大）

オンライン会場 B：ISEC 4（9：00～10：40）

6. 匿名放送型認証における安全性概念の関係性と認証子サイズの下界について
○小林大航（横浜国大）・渡邉洋平（電通大／産総研）・四方順司（横浜国大）
7. グラフ理論に基づく頑健性符号の構成　○佐竹翔平（熊本大）・顧　玉杰・櫻井幸一（九大）
8. Constant-Round Two-Party Exponentiation Based on Additive Secret Sharing　○Yi Lu・Keisuke Hara（Tokyo Inst. of Tech./AIST）・Kazuma Ohara・Jacob Schuldt（AIST）・Keisuke Tanaka（Tokyo Inst. of Tech.）
9. 主観評価を加えた統計的因果推論の方式　○池田大地・森田　光（神奈川大）

オンライン会場 B：ISEC 5（10：55～12：35）

10. ワイルドカードを利用可能なディジタル署名　○宮澤智輝・四方順司（横浜国大）
11. 参加者の動的変化に対応する非対話型マルチパーティ計算　○間澤将太・四方順司（横浜国大）
12. 分散型マルチ権限追跡可能匿名証明書スキームの一構成　穴田啓晃（長崎県立大）
13. Fast Multiparty Threshold ECDSA With Robustness　○Wang zhaobo・Atsuko Miyaji（Osaka Univ.）

5 日午後　オンライン会場 A：IT 4（14：20～15：10）

14. Minimum-Entropy Couplings 問題に対する Cicalese-Gargano-Vaccaro アルゴリズムの改善
○坂谷航平・岩田賢一（福井大）・藤崎礼志（金沢大）
15. マルコフ情報源に対する分類問題における最適な誤り指数の解析　○倉又洋人・八木秀樹・川端　勉（電通大）

オンライン会場 A：招待講演（IT）（15：25～16：15）

16.〔招待講演〕 Lee 距離に基づく 2 次元格子上の誤り訂正符号　森田啓義（電通大）

オンライン会場 B：ISEC 6（13：30～15：10）

17. 攻撃者のふるまいを利用したセキュリティ情報検索　○川口雄己・山嵜麿与（NTT）
18. Ethereum ネットワークにおけるハニーポット設置に向けた攻撃活動の分析　○陳　浩太・面　和成（筑波大）
19. Learning Contract-Wide Code Representations for Vulnerability Detection on Ethereum Smart Contracts
○Nami Ashizawa・Naoto Yanai・Jason Paul Cruz（Osaka Univ.）・Singo Okamura（NITNC）
20. Consideration of embedding methods and machine learning models for detecting malicious URLs
○Qisheng Chen・Kazumasa Omote（Univ. of Tsukuba）

◆IEEE IT Society Japan Chapter 共催
☆IT 研究会

【問合先】
IT 研究会幹事

E-mail：it-sec@mail.ieice.org（幹事，幹事補佐）

☆ISEC 研究会

【問合先】

面　和成（筑波大）

E-mail：isec-sec@mail.ieice.org（幹事，幹事補佐宛）

☆WBS 研究会

【問合先】

荒井伸太郎（岡山理科大）

E-mail：arai@ee.ous.ac.jp