★情報理論研究会（IT）

専門委員長　大橋正良　副委員長　村松　純
幹事　葛岡成晃・吉田隆弘　幹事補佐　岩本　貢

★情報セキュリティ研究会（ISEC）

専門委員長　満保雅浩　副委員長　小川一人・藤岡　淳
幹事　駒野雄一・水木敬明　幹事補佐　大東俊博・須賀祐治・猪俣敦夫

★ワイドバンドシステム研究会（WBS）

専門委員長　前原文明　副委員長　浜村昌則・小野文枝
幹事　佐藤正知・能田康義　幹事補佐　小澤佑介・中村　聡・中村僚兵

日時　3月 9日（木） 10：00～17：40
　　10日（金） 9：35～17：25
会場　東海大学高輪キャンパス（港区高輪 2-3-23. http://www.u-tokai.ac.jp/about/campus/takanawa/　大東俊博）
議題
9日午前　ISEC（1）（10：00～11：15）
1. ストリーム暗号 Grain v1 の出力の鍵依存度に関する考察
　○城所賢史（東海大）・五十部孝典（神戸大）・大東俊博（東海大）
2. 共通鍵暗号方式における Linear Obfuscation を用いた効果的な難読化手法
　○ステュワート ギャヴィンレン（ジャイスト）・宮地充子（ジャイスト／阪大）・布田裕一（東京工科大）
3. 3ラウンド RSA-OAEP の関連鍵攻撃に対する安全性　○伊藤玄武・森田　啓・岩田　哲（名大）
招待講演（1）（11：25～12：15）
4.〔招待講演〕 ホワイトボックス暗号化技術について―最新の攻撃と安全な構成方法―
　五十部孝典（ソニーグローバル M & O）
9日午後　ISEC（2）（13：35～14：50）
5. 多重暗号化方式への中間一致攻撃に関する考察　○前澤陽平・岩切宗利（防衛大）
6. 通常同種写像を用いた DH 鍵共有の安全性解析　○古川　悟・高安　敦・國廣　昇（東大）
7. 特殊な加算公式を持つ楕円曲線の安全性評価　○小寺健太・宮地充子・鄭　振牟（阪大）
IT（1）（13：35～14：50）
8. 符号の修正に基づく局所復号可能な符号の設計について
　○田宮寛人（神戸大）・廣友雅徳（佐賀大）・森井昌克（神戸大）
9. Sphere packing bounds and Gilbert-Varshamov bounds for b-symbol read channels
　○Seunghoan Song・Toru Fujiwara（Osaka Univ.）
10. 特性行列と符号部分系列の巡回シフトを用いた Tail-Biting 畳込み符号のトレリスの簡単化　田島正登
ISEC（3）（15：00～16：40）
11. Hessian Curve 上の ECDLP を指数計算法で解く手法について　○森島僚平・宮地充子・鄭　振牟（阪大）
12. GHS 攻撃の対象となる奇標数合成数次拡大体上の楕円曲線の分類 その2
　○小林龍平（中大）・飯島　努（光電製作所）・趙　晋輝（中大）
13. 同種条件なしの偶標数拡大体上 GHS 攻撃に対して安全な楕円曲線に関する考察
　○久木﨑聖矢（中大）・志村真帆呂（東海大）・趙　晋輝（中大）
14. 偶標数素数次拡大体上の楕円曲線に基づく射影直線上の（2, ..., 2）型被覆の構成法に関する考察
　○森下拓也（中大）・志村真帆呂（東海大）・趙　晋輝（中大）
WBS（1）（15：00～16：40）
15. MB-OFDM-UWB 信号による相互相関関数を用いた電力遅延プロファイル測定に関する研究
　○岡本拓也・井家上哲史（明大）
16. 変形擬直交 M 系列対による二乗検波型 DS-UWB-IR におけるマルチユーザ性能評価
　○松村拓真・羽渕裕真（茨城大）
17. コードシフトキーイングを用いる OFCDM における PAPR 低減法　○細川勇気・羽渕裕真（茨城大）
18. 周波数利用効率の高い異直交符号 DS/CDMA と室内電波強度分布を用いた干渉除去の性能評価
　○中條宏郁・太刀川信一（長岡高専）
招待講演（2）（16：50～17：40）
19.〔招待講演〕 副情報に遅延が生じる場合の Wyner-Ziv 符号化問題　○松田哲直・植松友彦（東工大）
10日午前　ISEC（4）（9：35～12：35）

1. ハッシュテーブルを用いた相互依存型自己インテグリティ検証によるソフトウェア保護
　○渡邉直紀・吉田直樹・松本　勉（横浜国大）
2. 複数ユーザー向けの匿名性 Oblivious RAM　○高野　悟・宮地充子・蘇　春華（阪大）
3. 多機関の安全な set union プロトコルについて　○宍戸克成・宮地充子（阪大）
4. プライバシを考慮した多機関データベースの属性別要素数の導出方式
　○吉田貴俊（北陸先端大）・宮地充子（阪大／北陸先端大／JST）
5. 対角線上証拠識別不可能な知識の証明システム　○穴田啓晃（長崎県立大）・有田正剛（情報セキュリティ大）
6. Morphism of Polynomials Revisited　Bagus Santoso（UEC）

IT（2）（10：55〜12：35）

7. q 元 r 出力通信路における q 元線形符号の性能評価システム（2）　○古屋杏志郎・山口和彦（電通大）
8. 超解像の応用による MRI の高速化に関する検討　○中島綾香・川喜田雅則・實松　豊・竹内純一（九大）
9. COFDM システムにおけるフルダイバーシチ未達領域でのビット誤り率予測
　○菅　宣理・江頭直人・矢野一人・熊谷智明（ATR）
10. 微少な誤りを許容する可変長符号化におけるオーバーフロー確率について
　○野村　亮（専修大）・八木秀樹（電通大）

10 日午後　ISEC（5）（13：45〜15：00）

11. Notes on new fundamental schemes K（AII）Scheme, K（AIII）Scheme and K（V）Scheme for constructing secure multivariate PKC, MVPKC and product-sum PKC, ΣΠ PKC　Masao Kasahara（Waseda Univ.）
12. 辞書ベースでの検索可能暗号の構成方法　○野島拓也・岩本　貢・太田和夫（電通大）
13. 検証可能な属性ベース検索可能暗号の効率化に関する検討
　○大竹　剛（NHK）・レイハネー サファヴィナイニ（カルガリー大）・リャンフェン チャン（上海科技大）

IT（3）（13：45〜15：00）

14. 意図されないメッセージに対する秘匿性を考慮したインデックス符号　○武井茉美・古賀弘樹（筑波大）
15. 複数の二次利用者によるスペクトルセンシングの検出確率の改善
　○村中勇樹・松本隆太郎・松田哲直・植松友彦（東工大）
16. Quantum Stabilizer Codes Can Realize Access Structures Impossible by Classical Secret Sharing
　Ryutaroh Matsumoto（Tokyo Tech.）

ISEC（6）（15：10〜16：25）

17. スコア分布特性を用いた Tardos 符号の閾値設定　○井上　諒・山口和彦（電通大）
18. Secret Sharing Schemes using Module-2^m Operations　Hidenori Kuwakado（Kansai Univ.）
19. SIAS におけるセキュリティインシデント兆候解析機能の開発
　○勝野満夢・坂本大樹・大川裕之・山口崇志・布広永示（東京情報大）

WBS（2）（15：10〜16：25）

20. RGB-LED 並列伝送における誤り訂正符号の効果　○孫　冉・羽渕裕真（茨城大）・小澤佑介（東京理科大）
21. 拡張プライム符号を用いる可視光可変 N パラレル符号多値変調法におけるマルチパスリフレクションの影響
　○大澤圭佑・羽渕裕真（茨城大）・小澤佑介（東京理科大）
22. バッファを伴う小型無人航空機によるデータ中継に関する一検討　○東　昂拓・落合秀樹（横浜国大）

招待講演（3）（16：35〜17：25）

23.〔招待講演〕 時間・空間・周波数領域インデックス変調の基礎と動向　杉浦慎哉（東京農工大）

◆IEEE IT Society Japan Chapter 共催
☆IT 研究会

【問合先】

情報理論研究会幹事，幹事補佐　E-mail：it-sec@mail.ieice.org

☆ISEC 研究会今後の予定 〔　〕内発表申込締切日

5 月 12 日（金） 機械振興会館〔未定〕テーマ：一般

【発表申込先】 下記研究会発表申込システムからお申込み下さい.
http://www.ieice.org/jpn/ken/kenmoushikomi.html

【問合先】

水木敬明（東北大）　E-mail：isec-sec@mail.ieice.org（幹事，幹事補佐宛）

☆WBS 研究会

【問合先】

佐藤正知（東京都市大）
TEL〔03〕5707-0104（ext. 2968），FAX〔03〕5707-2180
E-mail：tsato@tcu.ac.jp