★情報セキュリティ研究会（ISEC）

専門委員長　小川一人　副委員長　藤岡　淳・盛合志帆
幹事　水木敬明・大東俊博　幹事補佐　江村恵太・駒野雄一・須賀祐治

★コンピュテーション研究会（COMP）

専門委員長　伊藤大雄　副委員長　宇野裕之
幹事　脊戸和寿・斎藤寿樹

日時　12 月 21 日（木）　9：30～17：05
　　22 日（金）　9：50～15：30
会場　高知工科大学永国寺キャンパス教育研究棟 2F A213 教室（http://www.kochi-tech.ac.jp/kut/about_KUT/access.html　福本昌弘）
議題
21 日午前
1. 複数のハニーポットを利用した攻撃者の分類に関する基礎的研究　〇山下和也・沖野浩二（富山大）
2. ストリーム暗号のバイアス探索に関する統計的な評価手法　〇棚本清也・大東俊博（東海大）
3. Minalpher における MC が安全性に与える影響―6 ラウンドでの結果―
　〇岸　優樹・佐々木太良・藤岡　淳（神奈川大）
4. Circular Arc 上の独立集合を求める省領域アルゴリズム
　〇浦川翔平（神戸大）・トム バンデルザンデン（ユトレヒト大）・斎藤寿樹（九工大）・上原隆平（北陸先端大）
5. O（$n^{1/3}$）-space algorithm for the grid graph reachability problem
　〇Ryo Ashida・Kotaro Nakagawa（Tokyo Inst. of Tech.）
6. 部分グラフクラス上での最大 k-パス頂点被覆問題
　〇八木田　剛・宮野英次・斎藤寿樹（九工大）・上原隆平（北陸先端大）・Tom C. van der Zanden（ユトレヒト大）
7. 木における 1 ラウンドボロノイゲームの後手の最適戦略　〇杉本晃弘（神戸大）・斎藤寿樹（九工大）

21 日午後（14：10～）
8.〔招待講演〕 データを暗号化したまま分析できる秘密計算：その仕組みと実用に向けた研究　菊池　亮（NTT）
9. 公開検証可能なプライバシー保護時系列データ統計計算の実装評価
　〇鈴木達也（東海大）・江村恵太（NICT）・木村隼人・大東俊博（東海大）
10. サーバによるキーワード推測攻撃に対して安全な検索可能公開鍵暗号の安全性検討と拡張
　〇齋藤尭範・中西　透（広島大）
11. アキュームレータを用いた評価値ベースのブラックリスト型匿名認証　〇金谷健士・中西　透（広島大）
12. 動的自己書換えによる自己破壊的タンパー応答の実装性　大石和臣（静岡理工科大）

22 日午前
1. 線型準同型署名を用いた管理者に対して秘匿性を持つ評価システム　〇上野山大貴・中西　透（広島大）
2. ノンスに偏りのある Schnorr 型署名に対する Bleichenbacher 攻撃の最適化
　〇髙橋　彰（京大）・ティブシ メディ（NTT）
3. ID ベース暗号における匿名性定義―LOR 安全と SW 安全における関係―
　〇大友萌夢・佐々木太良・藤岡　淳（神奈川大）
4. カードベースプロトコルにおける並べ替え誤りに関する考察　〇水木敬明（東北大）・駒野雄一（東芝）

22 日午後
5.〔招待講演〕 半正定値緩和手法によるランダム制約充足問題の反駁の限界　森　立平（東工大）
6. 区間グラフ最大長指定分割問題の整数計画法による定式化　井上恵介（金沢高専）
7. An Efficient Enumeration Algorithm for Dominating Sets in K-Degenerate graphs
　〇Kazuhiro Kurita（Hokkaido Univ.）・Kunihiro Wasa・Takeaki Uno（NII）・Hiroki Arimura（Hokkaido Univ.）
8. pass 操作に制限のある物理的バケットソート　〇長尾篤樹・呉　偉（成蹊大）・伊藤大雄（電通大）

☆ISEC 研究会今後の予定 〔　〕内発表申込締切日
2018 年 3 月 8 日（木），9 日（金）　東京理科大葛飾キャンパス〔1 月 15 日（月）〕テーマ：IT・ISEC・WBS 合同研究会

【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）

☆COMP 研究会

【問合先】

斎藤寿樹（九工大大学院情報工学研究院）

〒820-8502　飯塚市川津 680-4

E-mail：toshikis@ces.kyutech.ac.jp