★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

日時　5月16日（水）　9：00～17：30
会場　東京工業大学大岡山キャンパス西8号館E棟10階情報理工学院大会議室（目黒区大岡山2-12-1．https://www.titech.ac.jp/maps/　田中圭介）
議題

1. Gitの履歴を利用したソースコード内のぜい弱性検知に関する研究
   ○山本健太（北陸先端大）・面　和成（筑波大）
2. Correlation Power Analysis with Long Cable
   ○Liu Yu・Momoka Kasuya・Takeshi Sugawara・Kazuo Sakiyama（UEC）
3. 有限体上楕円曲線の新しい演算に基づく離散対数問題の困難性とディジタル署名
   白勢政明（公立はこだて未来大）
4. 計算効率の良い逐次拡大体の構成条件の下でのBLS曲線の係数決定法
   ○南條由紀・カンダカル エムディ アルアミン（岡山大）・白勢政明（公立はこだて未来大）・日下卓也・野上保之（岡山大）
5. カックロに対する物理的ゼロ知識証明の効率化　　宮原大輝・○佐々木達也・水木敬明・曽根秀昭（東北大）

招待講演：ASIACRYPT2017特集（1）

6. 〔招待講演〕 The Minimum Number of Cards in Practical Card-Based Protocols（ASIACRYPT 2017より）
   ○宮原大輝（東北大）・林　優一（奈良先端大）・水木敬明・曽根秀昭（東北大）
7. 〔招待講演〕 Quantum Multicollision Finding Algorithm—ASIACRYPT 2017より—
   ○細山田光倫・佐々木　悠・草川恵太（NTT）

午後（14：00～）

8. ダークネット観測情報を用いた仮想通貨ネットワークの分析
   ○今村光良（筑波大／野村アセット）・面　和成（筑波大）
9. コインチェック事件における流出NEMの追跡に関する実態調査
   ○佐藤哲平（筑波大）・今村光良（筑波大／野村アセット）・面　和成（筑波大）
10. 国内外の仮想通貨取引所の実態調査
    ○藤谷知季（筑波大）・今村光良（筑波大／野村アセット）・面　和成（筑波大）
11. ネットワーク符号を基盤としたセキュアクラウドストレージにおけるデータ動的処理の検討
    ○渡邊　竣（筑波大）・トラン フン タオ（KDDI総合研究所）・面　和成（筑波大）

招待講演：ASIACRYPT2017特集（2）

12. 〔招待講演〕 Blockcipher-Based MACs：Beyond the Birthday Bound Without Message Length
    Yusuke Naito（Mitsubishi Electric）
13. 〔招待講演〕 2ラウンドEven-Mansour暗号に対する新しい鍵回復攻撃
    ○五十部孝典（兵庫県立大）・渋谷香士（名大）
14. 〔招待講演〕 On the Untapped Potential of Encoding Predicates by Arithmetic Circuits and Their Applications
    Shuichi Katsumata（Univ. of Tokyo）

【問合先】

水木敬明（東北大）
E-mail：isec-sec@mail.ieice.org