★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　9月4日（月）　10：00～17：00
会場　機械振興会館地下3階研修2号室（港区芝公園3-5-8．東京メトロ日比谷線：神谷町駅下車徒歩10分，JR：浜松町駅下車徒歩20分，都営地下鉄三田線：御成門駅・大江戸線：赤羽橋駅下車徒歩10分．http://www.jcmanet.or.jp/gaiyo/map_kaikan.htm　TEL〔03〕3434-8211）
議題
招待講演：EUROCRYPT 2017 特集
1.〔招待講演〕 CRT 秘密鍵の小さな CRT-RSA 暗号への攻撃の改良　　高安　敦（東大）
2.〔招待講演〕 Random Sampling Revisited : Lattice Enumeration with Discrete Pruning
　○青野良範（NICT）・Phong Q. Nguyen（フランス国立情報学自動制御研／フランス国立科学研究センター／東大）
3.〔招待講演〕 New Impossible Differential Search Tool from Design and Cryptanalysis Aspects
　Yu Sasaki（NTT）
4. Card-based Cryptographic Protocols Using Private Operations
　○Hibiki Ono・Yoshifumi Manabe（Kogakuin Univ.）
5. コミット型 AND プロトコルのシャッフル回数の下界について
　○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）
午後（14：30～）
6. Stabilizer Based Quantum Secret Sharing Constructed from Algebraic Curves
　○Wang Cheng（Saitama Univ.）・Takeshi Koshiba（Waseda Univ.）
7. 2進数体上の符号と多変数多項式による公開鍵暗号方式の新たな構成法
　○大久保智之・バグス サントソ（電通大）
8. Quantum Resistant Signatures based on Syndrome Decoding Problem
　○Taiyo Yamaguchi・Bagus Santoso（UEC）
招待講演：CRYPTO 2017 特集
9.〔招待講演〕 Tweakable ブロック暗号を用いた高速かつ安全なメッセージ認証コード ZMAC
　岩田　哲（名大）・○峯松一彦（NEC）・Thomas Peyrin（シンガポール南洋理工大）・Yannick Seurin（フランスネットワーク情報セキュリティ庁）
10.〔招待講演〕 Division Property を用いた非ブラックボックス多項式に対する Cube 攻撃（CRYPTO 2017 より）
　○藤堂洋介（NTT）・五十部孝典（兵庫県立大）
☆ISEC 研究会今後の予定 〔　〕内発表申込締切日
　11月9日（木），10日（金）　京都産大むすびわざ館〔未定〕テーマ：情報セキュリティ，ライフログ活用技術，ライフインテリジェンス，オフィス情報システム，一般
　12月21日（木），22日（金）　高知工科大永国寺キャンパス〔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）