★情報セキュリティ研究会（ISEC）

専門委員長　藤岡　淳　副委員長　盛合志帆・廣瀬勝一
幹事　大東俊博・江村恵太　幹事補佐　面　和成・須賀祐治

日時　5月17日（金）　10：00～17：30
会場　機械振興会館地下3階研修1号室
議題
招待講演：国際会議特集

1.〔招待講演〕　標準的仮定に基づくSIM-RSO-CCA安全性を満たす公開鍵暗号（from SCN 2018）
　○原　啓祐・北川冬航（東工大）・松田隆宏・花岡悟一郎（産総研）・田中圭介（東工大）
2.〔招待講演〕　Attacking Noisy Secret CRT-RSA Exponents in Binary Method（from ICISC 2018）
　○大西健斗・國廣　昇（東大）
3.〔招待講演〕　Analysis of Mixed PUF-TRNG Circuit Based on SR-Latches in FD-SOI Technology（from DSD 2019）
　Jean-Luc Dangar（Telecom ParisTech）・○Risa Yashiro（UEC）・Tarik Graba・Yves Mathieu・Abdelmalek Si-Merabet（Telecom ParisTech）・Kazuo Sakiyama（UEC）・Noriyuki Miura・Makoto Nagata（Kobe Univ.）・Sylvain Guilley（Secure-IC）
4. 匿名化データを復元する攻撃手法の定量的評価の検討　○山添貴哉・面　和成（筑波大）
5. 情報理論的PIRにおける効率の良い誤り訂正方法　黒澤　馨・○柴田敬斗・石成寿行・加倉井一平（茨城大）

午後（14：30～）

6. K（I）Sch-CBPKC Based on Message-Dependent Transformation　Masao Kasahara（Waseda Univ.）
7. The amount of information leakage of decryption keys through timing attacks on RSA decryption system
　○Tomonori Hirata・Yuichi Kaji（Nagoya Univ.）
8. IoT機器に適したセキュアプロビジョニング方式の提案
　○山本　大・小久保博崇・町田卓謙・森川郁也（富士通研）・金岡　晃（東邦大）

招待講演：国際会議特集

9.〔招待講演〕　複数用途からなる交通ICカードデータの再識別リスク分析（from AINA 2018）
　○伊藤聡志・原田玲央・菊池浩明（明大）
10.〔招待講演〕　セキュアチャネルフリー検索可能暗号と公開鍵暗号との安全な併用について（from ISPEC 2018）
　○鈴木達也（東海大／NICT）・江村恵太（NICT）・大東俊博（東海大／NICT）
11.〔招待講演〕　Five-Card AND Protocol in Committed Format Using Only Practical Shuffles（from APKC 2018）
　○阿部勇太（東北大）・林　優一（奈良先端大）・水木敬明・曽根秀昭（東北大）

【問合先】
面　和成（筑波大）
E-mail：isec-sec@mail.ieice.org（幹事，幹事補佐宛）