★情報セキュリティ研究会（ISEC）

専門委員長　盛合志帆　副委員長　廣瀬勝一・伊豆哲也
幹事　江村恵太・面　和成　幹事補佐　山本　大・須賀祐治

日時　5月20日（水）　9：20～17：45
会場　機械振興会館地下3階研修2号室
議題

1. CSIDHを用いた同種写像に基づくRing署名方式の提案　　○木山泰晟・鈴木幸太郎（豊橋技科大）
2. Google Adiantumに対する識別，偽造，平文回復攻撃　　○土生　亮・岩田　哲（名大）
3. 3次ツイストを持つ楕円曲線上の埋め込み次数が奇数のペアリングアルゴリズムについて
   ○石井将大（東工大）・照屋唯紀（産総研）・安田貴徳（岡山理科大）
4. メモリ制限下における量子Information Set Decodingアルゴリズムの高速化
   ○木村直人・高安　敦・高木　剛（東大）
5. アニーリング計算を用いたAESの差分特性探索に向けて
   平野　遥・○垣本修吾・米山一樹（茨城大）・山口純平（富士通研）
6. A Study of Randomized Authentication in Opportunistic Networks　　○Kai Wang・Kazuya Sakai（TMU）

午後（12：50～）

7. 〔招待講演〕 対称関数を計算する効率的なPrivate PEZプロトコル（from TCC 2019）
   ○安部芳紀・岩本　貢（電通大）・太田和夫（電通大／産総研）
8. 〔招待講演〕 F4-styleアルゴリズムによるMQ問題の求解（from IWSEC 2019）
   ○伊藤琢真・篠原直行（NICT）・内山成憲（都立大）
9. 〔招待講演〕 不正検知可能な準最適（2, 2, n）ランプ型秘密分散（from CANDAR 2019）
   ○上松知貴（NEC）・尾花　賢（法政大）
10. 〔招待講演〕 Tweakable TWINE : Building a Tweakable Block Cipher on Generalized Feistel Structure（from IWSEC 2019）　　○阪本光星（兵庫県立大）・峯松一彦（NEC）・柴田　直・茂　真紀・久保博靖（NES）・船引悠生（神戸大）・Andrey Bogdanov（DTU）・森岡澄夫（インターステラ）・五十部孝典（兵庫県立大／NICT）
11. 〔招待講演〕 How to Construct CSIDH on Edwards Curves（from CT-RSA 2020）
    ○守谷共起・小貫啓史・高木　剛（東大）
12. ハッシュ関数に基づく計算問題に対するマイニング時間の小分散化
    ○穴田啓晃（長崎県立大）・櫻井幸一（九大）
13. ブロックチェーンネットワークの不均衡と収束による再中央集権化の評価
    ○今村光良（筑波大）・面　和成（筑波大／NICT）
14. NEMのブロックチェーンシステムにおける匿名信頼性付与手法の実装・評価
    ○藤谷知季（筑波大）・江村恵太（NICT）・面　和成（筑波大／NICT）
15. パスワード漏洩情報を用いた企業の特徴分析　　○今村光良・面　和成（筑波大）
16. IoT機器向けIDベース認証鍵交換と不正なPKGに対する安全性
    ○割木寿将・佐々木太良・藤岡　淳（神奈川大）・鈴木幸太郎（豊橋技科大）・富田潤一（NTT）
17. PE表層情報を用いたマルウェア検知モデルのロバスト性について
    ○鄭　万嘉（筑波大）・面　和成（筑波大／NICT）
18. 出現文字を用いた機械学習によるDNSトンネル検出の研究―評価プログラムの実装に係る考察―
    ○朝倉哲也・辰己丈夫（放送大）

☆ISEC研究会今後の予定　〔　〕内発表申込締切日
7月20日（月），21日（火）　札幌コンベンションセンター〔未定〕テーマ：セキュリティ，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．
https://www.ieice.org/ken/program/index.php

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