★情報セキュリティ研究会（ISEC）

専門委員長　櫻井幸一　副委員長　角尾幸保・満保雅浩
幹事　岩田　哲・花岡悟一郎　幹事補佐　伊豆哲也・川本淳平・駒野雄一・島　成佳・水木敬明

日時　9月5日（金）　12：55～17：35

会場　機械振興会館地下2階1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

1. 多次多変数方程式とリード・ソロモン符号に基づく新しい公開鍵暗号，K(X)RSE(2)PKC，K_M(X)RSE(2)PKCとK(XI)RSE(2)PKC　笠原正雄（早大／中大）
2. トレース距離を量子鍵配送の失敗確率とする解釈における課題：Part II　岩越丈尚（玉川大）
3. 信頼できる第三者機関を用いたFail-Stop署名方式及びそのUC安全性　○野村昌弘・中村勝洋（千葉大）
4. Efficient Proofs for Monotone Formulas on Attributes Excluding Restriction in Anonymous Credential System
   ○Shahidatul Sadiah（Okayama Univ.）・Toru Nakanishi（Hiroshima Univ.）・Nobuo Funabiki（Okayama Univ.）
5. Garbled searchable symmetric encryption方式の計算機シミュレーション　○佐々木圭祐・黒澤　馨（茨城大）
6. Schematic to Program Translator（SPT）を用いたGPUへの暗号実装
   ○渡部　匡・岩井啓輔・田中秀磨・黒川恭一（防衛大）
7. ハッシュ関数SHA-3のFPGA実装性能評価　○石井　潤・本多達也・佐藤　証（電通大）
8. 国際会議EUROCRYPT 2014参加報告　林　良太郎（東芝）
9. 〔招待講演〕 Dual System Encryption via Doubly Selective Security—A Generic Framework for Fully-Secure Predicate Encryption—　Nuttapong Attrapadung（AIST）
10. 〔招待講演〕 Parallelizable Rate-1 Authenticated Encryption from Pseudorandom Functions
    Kazuhiko Minematsu（NEC）

☆ISEC研究会今後の予定　〔　〕内発表申込締切日

11月21日（金），22日（土）　兵庫県立大神戸情報科学キャンパス〔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19日（金）　機械振興会館〔10月13日（月）〕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】

岩田　哲（名大）
TEL〔052〕789-5722，FAX〔052〕789-5723
E-mail：isec-sec@mail.ieice.org（幹事，幹事補佐宛）