★情報セキュリティ研究会（ISEC）

専門委員長　角尾幸保　副委員長　満保雅浩・小川一人
幹事　花岡悟一郎・駒野雄一　幹事補佐　伊豆哲也・水木敬明・山下哲孝

日時　9月4日（金）　10：30～17：20

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

1. Edwards曲線の加算公式の改良　　白勢政明（公立はこだて未来大）
2. RainbowCrackにおける還元関数の改良　　○田畠佑紀・岩井啓輔・田中秀磨・黒川恭一（防衛大）
3. ハッシュ関数のGPUへの高速化実装　　○グェン ダット トゥオン・黒川恭一・岩井啓輔（防衛大）
4. An extension of cryptographic protocol in distributed in-memory caching system　　Ruo Ando（NICT）

午後（13：40～）

5. Proposal of a new class of multivariate PKC,（$u|u+v$）MVPKC—Along with a comment on K(II) Trans.—　　○Masao Kasahara（Waseda Univ./Chuo Univ.）・Ryuichi Sakai（OECU）
6. 多変数公開鍵暗号方式（MPKC）の多素数・中国人剰余定理による構成—耐量子コンピュータ・ウェアラブル化を目指して—　　○辻井重男・藤田　亮・五太子政史（中大）
7. 多機関のPrivate Set Intersection protocolのモデル化　　○西田昌平・宮地充子（北陸先端大）

招待講演（EUROCRYPT 2015特集）

8. 国際会議　EUROCRYPT 2015報告　　小暮　淳（情報処理推進機構）
9. 〔招待講演〕 Structural Evaluation by Generalized Integral Property　　Yosuke Todo（NTT）
10. 〔招待講演〕 完全群構造維持署名と圧縮コミットメント　　阿部正幸（NTT）
11. 〔招待講演〕（Batch）Fully Homomorphic Encryption over Integers for Non-Binary Message Spaces（Eurocrypt 2015より）　　黒澤　馨（茨城大）

☆ISEC研究会今後の予定　〔　〕内発表申込締切日

11月6日（金），7日（土）　神奈川大〔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18日（金）　機械振興会館〔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）