★情報セキュリティ研究会（ISEC）

専門委員長　満保雅浩　副委員長　小川一人・藤岡　淳
幹事　駒野雄一・水木敬明　幹事補佐　大東俊博・須賀祐治・猪俣敦夫

日時　9月2日（金）　9：45～17：20

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. ランダム二等分割カットの安全な実行に関する考察
　○上田　格・西村明紘（東北大）・林　優一（東北学院大）・水木敬明・曽根秀昭（東北大）
2. 知識の証明のバンドリングとそのデジタル署名への応用
　○穴田啓晃（長崎県立大）・有田正剛（情報セキュリティ大）

招待講演：EUROCRYPT 2016 特集（1）

3.〔招待講演〕 Constant-round Leakage-resilient Zero-knowledge from Collision Resistance
　Susumu Kiyoshima（NTT）
4.〔招待講演〕 Anonymous Traitor Tracing : How to Embed Arbitrary Information in a Key
　○西巻　陵（NTT）・Daniel Wichs（NEU）・Mark Zhandry（MIT/Princeton）

午後

5. A New Class of Public Key Cryptosystems Constructed Based on Cyclic Codes, K（XVII）SE（1）PKC, along with Revisit to K（AII）Scheme　　Masao Kasahara（21CICRC）
6. ある種の不定方程式の求解問題に基づく準同型暗号
　○秋山浩一郎（東芝）・後藤泰宏（北海道教大）・奥村伸也（九州先端科学技研）・高木　剛（九大）・縫田光司・花岡悟一郎（産総研）
7. Implicit な Hint を用いた因数分解に関する一考察―解ベクトルの長さと格子面積との関係―
　○萩野谷一二・古宮嘉那子（茨城大）
8. データメモリを利用する耐タンパーソフトウェア　　大石和臣（静岡理工科大）
9. GUI を用いた暗号開発環境への安全性評価機能の実装　　○中村聡宏・岩井啓輔・黒川恭一（防衛大）
10. ハッシュ関数 Keccak の CUDA 実装　　○グェン ダット トゥオン・黒川恭一・岩井啓輔（防衛大）

招待講演：EUROCRYPT 2016 特集（2）

11.〔招待講演〕 Progressive BKZ アルゴリズムを用いた格子暗号の安全性評価
　○青野良範（NICT）・王　贇弢（九大）・林　卓也（NICT）・高木　剛（九大）
12.〔招待講演〕 漸近的に公開鍵が短い格子に基づく適応的攻撃者に対して安全な ID ベース暗号
　山田翔太（産総研）
13.〔招待講演〕 On the Influence of Message Length in PMAC's Security Bounds（Eurocrypt 2016 より）
　安田　幹（NTT）

☆ISEC 研究会今後の予定　〔　〕内発表申込締切日

11月7日（月），8日（火）　福井市地域交流プラザ〔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（水），22日（木）　広島大〔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）