★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

★コンピュテーション研究会（COMP）

専門委員長　伊藤大雄　副委員長　宇野裕之

幹事　脊戸和寿・斎藤寿樹

日時　12 月 21 日（水）　9：30～15：50

22 日（木）　9：30～16：20

会場　広島大学東広島キャンパス本部棟 4 階会議室（東広島市鏡山 1-3-2．JR 西条駅からバス（広島大学行き）で広大中央口か山中池下車．http://hiroshima-u.jp/access/higashihiroshima　http://hiroshima-u.jp/access/campusmap/higashihiroshima　亀井清華）

議題

21 日午前　ISEC（1）

1．アキュームレータを用いたブラックリスト型匿名認証システムの改良　　○愛甲　悠・中西　透（広島大）

2．ID ベース暗号における匿名性定義の考察　　○大友萌夢・藤岡　淳・佐々木太良（神奈川大）

COMP 招待講演（1）

3．〔招待講演〕 量子アニーリングが拓く機械学習と計算技術の新時代　　大関真之（東北大）

21 日午後　ISEC 招待講演：CRYPTO 2016 特集（1）（12：30～）

4．国際会議 CRYPTO の概要説明　　小川一人（NHK）

5．〔招待講演〕 整数計画を用いた高速拡張可能双線型型変換
　○星野文学・阿部正幸（NTT）・大久保美也子（NICT）

6．〔招待講演〕 Cryptanalysis of GGH15 Multilinear Maps（CRYPTO 2016 より）　　ティブシ メディ（NTT）

7．〔招待講演〕 Backdoors in Pseudorandom Number Generators : Possibility and Impossibility Results
　Jean Paul Degabriele・Kenneth Paterson（RHUL）・○Jacob Schuldt（AIST）・Joanne Woodage（RHUL）

COMP（1）

8．2 部グラフのスタックキューミックスレイアウト　　宮内美樹（NTT）

9．Sensitivity が 3 の論理関数について　　天野一幸（群馬大）

10．極大独立集合問題を解く緩安定個体群プロトコルの提案
　○清洲星顕・首藤祐一・角川裕次・増澤利光（阪大）

11．ホストとスイッチから成る相互結合網の理論モデル
　○安戸僚汰（慶大）・鯉渕道紘（NII）・天野英晴（慶大）・中野浩嗣（広島大）

22 日午前　ISEC（2）

1．Mix Columns が Minalpher の安全性に与える影響　　○岸　優樹・藤岡　淳・佐々木太良（神奈川大）

2．CARDIS 2015 の Re-keying 方式の再考察（その 2）　　駒野雄一（東芝）

COMP 招待講演（2）

3．〔招待講演〕 簡潔データ構造の理論と実践　　定兼邦彦（東大）

22 日午後　ISEC 招待講演：CRYPTO 2016 特集（2）（12：30～）

4．〔招待講演〕 セミスムーズな部分群を持つ RSA 数の素因数分解困難性に基づく攻撃者依存損失落し戸関数
　○山川高志（東大）・山田翔太・花岡悟一郎（産総研）・國廣　昇（東大）

5．〔招待講演〕 Extended tower number field sieve : A new complexity for the medium prime case
　Taechan Kim（NTT）

6．〔招待講演〕 The SKINNY Family of Block Ciphers and its Low-Latency Variant MANTIS　　Yu Sasaki（NTT）

COMP 招待講演（3）

7．〔招待講演〕 無向グラフの直径をどこまで小さくできるか？―低遅延な大規模相互結合網を求めて―
　藤原一毅（NICT）

COMP（2）

8．等価性構造保持仮定の下での等価性構造抽出における探索数削減
　○佐藤聖也（産総研）・高橋良暢（電通大）・潮　旭（慶大）・山川　宏（ドワンゴ AI ラボ）

9．カラーグローブを用いた指輪郭抽出の特殊事例に対する改善　　○森内光太郎・藤嶋教彰（松江高専）

☆ISEC 研究会今後の予定　〔　〕内発表申込締切日

2017 年 3 月 9 日（木），10 日（金）　東海大高輪キャンパス〔未定〕テーマ：IT・ISEC・WBS 合同研究会

【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）

☆COMP 研究会今後の予定 〔 〕内発表申込締切日

2017 年 3 月 7 日（火） 南山大〔未定〕

【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】

斎藤寿樹（神戸大大学院工学研究科）

〒657-8501 神戸市灘区六甲台町 1-1

E-mail：saitoh@eedept.kobe-u.ac.jp