

★情報セキュリティ研究会 (ISEC)

専門委員長 田中俊昭 副委員長 櫻井幸一・角尾幸保

幹事 伊豆哲也・岩田 哲 幹事補佐 花岡悟一郎・三宅 優・駒野雄一

日時 5月9日(金) 13:10~17:35

会場 機械振興会館地下3階研修1号室

議題

1. リード・ソロモン符号に基づく公開鍵暗号 K(XV)SE(1)PKC, K(XVI)SE(1)PKC, K(XVII)SE(1)PKC
笠原正雄(早大/中大)
2. RSA 暗号を利用した組織暗号の一方式 ○村上恭通(阪電通大)・笠原正雄(早大/中大)
3. A Robust DWT Watermarking for Image using Quantized Domain Based on q-logarithm Function
○Ta Minh Thanh(Tokyo Inst. of Tech.)・Ta Minh Tam(VSTV)
4. 離散フーリエ変換を用いたIDSに関する一考察
○チメドツェレン エンフボルド・岩井啓輔・田中秀磨・黒川恭一(防衛大)
5. セキュアなクラウド量子計算における検証 森前智行(群馬大)
6. RC4 の Long-Term Glimpse における新しい Negative Biases ○伊藤竜馬・宮地充子(北陸先端大)
7. 国際会議 ASIACRYPT2013 参加報告 米山一樹(NTT)
8. [招待講演] Generic Key Recovery Attack on Feistel Scheme ○Takanori Isobe・Kyoji Shibutani(Sony)
9. [招待講演] Limited-Birthday Distinguishers for Hash Functions—Collisions beyond the Birthday Bound Can Be Meaningful— ○Mitsugu Iwamoto(Univ. of Electro-Comm.)・Yu Sasaki(NTT)

☆ISEC 研究会今後の予定 [] 内発表申込締切日

7月 [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.

<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)