★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　5月15日（金）　13：30～17：35

会場　機械振興会館地下3階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. 3つの素因数の分解困難性に依拠した多変数公開鍵暗号方式の提案
   ○辻井重男・只木孝太郎・五太子政史・藤田　亮（中大）
2. ブロック暗号PRINCEに対する丸め差分攻撃
   ○瀬戸口　聡・五十嵐保隆（鹿児島大）・金子敏信（東京理科大）・福島誠治・八野知博（鹿児島大）
3. 匿名通信Torの経路解析手法の提案　　○芝原幸弘・佐藤　直（情報セキュリティ大）
4. 能動的な不正に対して安全な不正検出可能パスワード付秘密分散法　　○市川敦謙・尾形わかは（東工大）
5. On the（In）Security of QUIC　　○Masaya Iseki（Tokyo Inst. of Tech.）・Eiichiro Fujisaki（NTT）
6. 〔招待講演〕 All-But-Many Encryption : A New Framework for Fully-Equipped UC Commitments
   Eiichiro Fujisaki（NTT）
7. 〔招待講演〕 Black-Box Separations for One-More（Static）CDH and Its Generalization
   Jiang Zhang・Zhenfeng Zhang・Yu Chen・Yanfei Guo（CAS）・○Zongyang Zhang（AIST）
8. 〔招待講演〕 順序保存暗号の識別不能性に関して
   ○寺西　勇（NEC）・ユング モティ・マルキン タル（コロンビア大）

【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）