NICT 組織間秘密通信のための公開鍵システムの研究開発 キックオフミーティング

❖開催日　2013年11月1日（金）　13：00～17：30
　　2日（土）　10：00～15：00

❖会場　後楽園キャンパス 3号館12階 31219号室

❖11月1日 出席者（敬称略）

笠原正雄、村上恭通、境 隆一、黒澤 馨、尾形わかは、師玉康成、岡崎裕之、村山優子、辻井重男、趙 晋輝、才所敏明、飯島 努、五太子政史、只木孝太郎、藤田 亮

時間			発表者	タイトル
13:00	～	13:30	辻井重男	NICT研究プロジェクトの説明
13:30	～	14:15	辻井重男	組織間通信と情報セキュリティの概念の高度化
14:20	～	15:30	笠原正雄	組織暗号に関する基礎的考察
14:30	～	15:00	黒澤　馨	多受信楕円エルガマル･クラマーシュープ暗号
15:00	～	15:30	休憩	
15:30	～	16:15	趙 晋輝	楕円･超楕円暗号に対する攻撃とその対策
16:15	～	17:10	全員による組織暗号に関する議論	
15:10	～	17:40	師玉 康成	論理学暗号と定理証明

❖11月2日出席者（敬称略）

笠原正雄、村上恭通、境 隆一、尾形わかは、岡崎裕之、村山優子、亀山幸義、辻井重男、才所敏明、飯島 努、辻 敏雄、五太子政史、只木孝太郎、藤田 亮

10:00	～	11:30	村上恭通	ナップザック暗号による鍵共有法
11:30	～	12:00	才所敏明	組織間機密通信のマネジメント
12:00	～	13:00	昼食	
13:00	～	13:40	境 隆一	IDベース放送暗号と組織暗号について
13:40	～	14:15	村山優子	災害コミュニケーションの課題
14:15		15:25	亀山幸義	最近の研究とNICTプロジェクトについて
15:25	～	16:35	岡崎裕之	暗号理論のための定理証明の応用
16:35	～	17:15	辻　敏雄	楕円エルガマル暗号の実装
17:15	～	17:45	五太子政史	組織間機密通信公開鍵システム デモシステム概略案
17:45	～	18:20	尾形わかは	Searchable Symmetric Encryption - 安全性と実用性
18:20	～	18:30	只木孝太郎	計算可能性解析による暗号理論の再構築
18:30	～	18:35	飯島　努	多受信楕円エルガマル･クラマーシュープ暗号、楕円暗号に関する最近の研究動向