★ハードウェアセキュリティ研究会（HWS）

専門委員長　松本　勉　副委員長　川村信一・池田　誠
幹事　三浦典之・国井裕樹

日時　4 月 12 日（金）　13：30～16：45
会場　東北大学
議題　ハードウェアセキュリティ，一般

1. RNS 表現によるバイナリ拡張ユークリッド互除法の改良と剰余復号法
　　○川村信一（ECSEC 組合）・駒野雄一・清水秀夫（東芝）
2. パルス方式測距 LIDAR の計測セキュリティ強化技術を評価するシステムの構築
　　○末廣達也・櫻澤　聡・吉田直樹・松本　勉（横浜国大）
3. ガロア体演算に基づく認証暗号の統合ハードウェアの設計　　○澤田石尚太郎・上野　嶺・本間尚文（東北大）
4. 180 nm CMOS プロセスを用いた Physically Unclonable Functions の実装と評価
　　○汐﨑　充・久保田貴也・白畑正芳（立命館大）・堀　洋平・片下敏宏（産総研）・藤野　毅（立命館大）
5. デバイス上の時間変化する伝搬特性を利用した秘密鍵共有についての基礎検討
　　○岡本拓実・大須賀彩希・藤本大介・林　優一（奈良先端大）
6. 送信波に漏れ出る無線モジュール内情報の分析
　　○坂本純一（横浜国大）・衣川昌宏（仙台高専）・藤本大介・林　優一（奈良先端大）・松本　勉（横浜国大）
7. 意図的な電磁波注入による任意の I/O ピンからの強制的な情報漏えいの誘発に関する基礎検討
　　○川上莉穂（奈良先端大）・衣川昌宏（仙台高専）・藤本大介・林　優一（奈良先端大）

◎研究会終了後，懇親会を予定していますので御参加下さい．

【問合先】

三浦典之（神戸大）・国井裕樹（セコム）
E-mail：hws-sec@mail.ieice.org