★ハードウェアセキュリティ研究会（HWS）

専門委員長　永田　真　副委員長　林　優一・鈴木大輔

幹事　山本弘毅・藤本大介

★集積回路研究会（ICD）

専門委員長　高橋真史　副委員長　池田　誠

幹事　宮地幸祐・新居浩二　幹事補佐　塩見　準・吉原義昭・久保木　猛

日時　10 月 25 日（火）　9：50～17：30

会場　立命館大・びわこ・くさつキャンパス（〒525-8577　草津市野路東 1 丁目 1-1．JR 京都駅から JR にて約 20 分，「南草津駅」で近江鉄道バス「立命館大学行き」または立命館大学経由「松ヶ丘五丁目」行き・「県立長寿社会福祉センター」行きに乗り換え約 20 分．http://www.ritsumei.ac.jp/accessmap/bkc/）

議題　ハードウェアセキュリティ，一般

午前　HWS（1）：サイドチャネル攻撃（10：00～11：15）

1. Romulus の TI 付きハードウェア実装と電力リークのシミュレーション評価
   ○根本昌也・浅野多聞・菅原　健（電通大）
2. AES-CTR に対するプロファイリングサイドチャネル解析の検討　○蝦名克海・上野　嶺・本間尚文（東北大）
3. 暗号 IC チップの電源電流シミュレーションとサイドチャネル漏洩評価
   ○長谷川陸宇・弘原海拓也・門田和樹・三木拓司・永田　真（神戸大）

HWS（2）：乱数／ハードウェアトロイ（11：25～12：15）

4. ERO-TRNG に対する振幅確率分布を用いた乱数性評価に関する基礎検討
   ○尾崎慧一・藤本大介（奈良先端大）・大須賀彩希・川村信一（産総研）・林　優一（奈良先端大）
5. ハードウェアトロージャン検出にむけた光学顕微鏡による半導体デバイスの観察
   ○坂根広史・坂本純一・川村信一（産総研）・永田　真（神戸大）・林　優一（奈良先端大）

午後　HWS（3）：故障注入（13：25～14：40）

6. レッドシフト：連続波レーザーを用いて信号の伝搬遅延を操作する攻撃
   ○山下晃平（電通大）・シア ベンジャミン・フーケビン（UMich）・バールソン ウェイン（UMass）・菅原　健（電通大）
7. イメージセンサインターフェースへのフォルト攻撃による Adversarial Examples 攻撃の検討
   ○大山達哉・吉田康太・大倉俊介・藤野　毅（立命館大）
8. Direct ToF LiDAR に対する距離偽装攻撃評価における攻撃光照射タイミング決定法に関する基礎検討
   ○富島み登り・藤本大介・林　優一（奈良先端大）

ICD/HWS（4）：暗号アルゴリズム／実装方法／プロトコル（1）（14：50～16：05）

9. 確率的秘匿演算ハードウェアの設計とプロトタイプ評価　○田村佑樹・上野　嶺・本間尚文（東北大）
10. GMT8-544 曲線上ペアリング計算の省メモリソフトウェア実装
    ○宮田大翔・坂本純一・吉田直樹・安西　陸・松本　勉（横浜国大）
11. Hardware Acceleration of TFHE-based Adder by Controlling Error
    ○Yinfan Zhao・Ikeda Makoto（Univ. of Tokyo）

HWS（5）：暗号アルゴリズム／実装方法／プロトコル（2）（16：15～17：30）

12. 車載ネットワーク CAN に対する軽量暗号を用いた MAC 実装と評価
    ○壷井智也・野上保之・日下卓也（岡山大）
13. CMOS イメージセンサに適した小面積 HMAC-SHA256 回路の検討
    ○関岡悠羽・大山達哉・龍野隼人・吉田康太・大倉俊介・藤野　毅（立命館大）
14. CAN メッセージの物理的伝送方向を識別する方法
    ○前川陽介・カミーユ ゲ（トヨタ自動車／横浜国大）・松本　勉（横浜国大）

◆IEEE SSCS；Japan Chapter/Kansai Chapter 共催

☆HWS 研究会

【問合先】

藤本大介（奈良先端大）・山本弘毅（ソニーセミコンダクタソリューションズ）

E-mail：hws-sec@mail.ieice.org

☆ICD 研究会今後の予定　〔　〕内発表申込締切日

11 月 28 日（月）～30 日（水）　金沢市文化ホール〔締切済〕テーマ：デザインガイア 2022―VLSI 設計の新しい大地―

【問合先】

新居浩二（TSMC デザインテクノロジージャパン）
E-mail：nii.koji@gmail.com