★ハードウェアセキュリティ研究会（HWS）

専門委員長　池田　誠　副委員長　島崎靖久・永田　真
幹事　小野貴継・高橋順子

★集積回路研究会（ICD）

専門委員長　永田　真　副委員長　高橋真史
幹事　柘植政利・廣瀬哲也　幹事補佐　新居浩二・宮地幸祐・久保木　猛

日時　10 月 26 日（月） 9：00～18：05
会場　オンライン開催
議題　ハードウェアセキュリティ，一般
サイドチャネル攻撃（9：00～10：15）
1. 暗号 IC の電力解析攻撃耐性評価基板に対する要求仕様の検討―PDN の伝達インピーダンスの漏洩強度への寄与―
　○菅　智信・五百旗頭健吾・豊田啓孝（岡山大）
2. ペアリングハードウェアに対するパイプラインスケジューリングを利用した電力解析攻撃
　○山﨑満文・坂本純一・松本　勉（横浜国大）
3. デジタル出力回路のインピーダンス変化に着目した意図的な電磁的情報漏えい評価法の検討
　○鍛治秀伍・藤本大介（奈良先端大）・衣川昌宏（福知山公大）・林　優一（奈良先端大）
実装攻撃（10：30～11：45）
4. 超音波センサに対するレーザー利用攻撃　○末廣達也・外山　拓・坂本純一・松本　勉（横浜国大）
5. シェアシリアル型 Threshold Implementation へのプロービング攻撃　○菅原　健・李　陽・﨑山一男（電通大）
6. 楕円曲線 DSA に対する格子簡約攻撃の実行可能性評価　○阿部浩太郎・池田　誠（東大）
午後　ハードウェア及びシステムセキュリティ（13：00～14：15）
7. 即時に故障検出可能な高効率 AES ハードウェアの検討　○柳生佑介・上野　嶺・本間尚文（東北大）
8. IoT デバイスにおけるアプリケーション電力抽出手法を用いた異常検知手法の評価
　○高崎和成（早大）・木田良一（ラック）・戸川　望（早大）
9. 光コンピューティングのモデルにおけるセキュリティリスクと対策　○高橋順子・千田浩司・坂本　健（NTT）
ハードウェアトロイ（I）：動向とトロイ挿入（14：30～16：10）
10. 国内におけるハードウェアトロージャン研究動向　○川村信一・林　優一（産総研）
11. 半導体チップのハードウェアトロージャンに対する物理レベルの取り組み（Ⅱ）
　○坂根広史・川村信一・今福健太郎・堀　洋平・永田　真・林　優一・松本　勉（産総研）
12. AI 推論器の LUT 構造に着目したハードウェアトロイ　○野崎佑典・竹本　修・池崎良哉・吉川雅弥（名城大）
13. 低遅延実装の対策回路を指向したハードウェアトロイ挿入とその検知
　○竹本　修・池崎良哉・野崎佑典・吉川雅弥（名城大）
ハードウェアトロイ（II）：検知手法（16：25～18：05）
14. 暗号ハードウェアのネットリストに対するハードウェアトロイ検知手法
　○伊東　燦・上野　嶺・本間尚文（東北大）
15. トリガ回路の性質に基づく特徴量を利用したランダムフォレストによるハードウェアトロイ識別
　○栗原　樹・戸川　望（早大）
16. ハードウェアトロイ識別における敵対的サンプル用改変の体系的分類
　○野澤康平（早大）・披田野清良・清本晋作（KDDI 総合研究所）・戸川　望（早大）
17. セキュア IC チップにおける物理設計改竄の検出に向けた高効率シミュレーション手法の検討
　○安田一樹・門田和樹・中川大地・永田　真（神戸大）

☆HWS 研究会
【問合先】
小野貴継（九大）・高橋順子（NTT）
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 17 日（火），18 日（水） オンライン開催〔締切済〕テーマ：デザインガイア 2020―VLSI 設計の新しい大地―
12 月 18 日（金）～20 日（日）〔未定〕テーマ：学生・若手研究会
【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.
https://www.ieice.org/ken/program/index.php
【問合先】
柘植政利（ソシオネクスト）　E-mail：icd-contact@mail.ieice.org