★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

★集積回路研究会（ICD）

専門委員長　日高秀人　副委員長　永田　真
幹事　橋本　隆・夏井雅典　幹事補佐　伊藤浩之・柘植政利・廣瀬哲也

◎本研究会は参加費が必要になります.
ESS の技報電子化研究会に関する御案内ページ（HWS）
https://www.ieice.org/ess/ESS/gihou-trial-ess2018.html
エレソの技報電子化研究会に関する御案内ページ（ICD）
https://www.ieice.org/es/jpn/e-gihou-2018es/e-gihou-2018es.htm

日時　10 月 29 日（月） 13：00～16：50
会場　神戸大学梅田インテリジェントラボラトリ（大阪市北区鶴野町 1-9　梅田ゲートタワー 8 階. http://www.b.kobe-u.ac.jp/ilabo/access.html）
議題　ハードウェアセキュリティ，一般
セキュア回路
1. EDA ツールを用いた AES 回路から漏洩するサイドチャネル波形の SNR シミュレーション法の検討
　○手嶋俊彰・矢野佑典・五百旗頭健吾・豊田啓孝（岡山大）
2. 暗号モジュールにおける電源ノイズとサイドチャネル漏洩の対策（I）
　○門田和樹・佐藤聡介・月岡暉裕（神戸大）・沖殿貴朗（ECSEC）・三木拓司・三浦典之・永田　真（神戸大）
3. 格子暗号向け高精度離散ガウス乱数生成器のハードウェア実装　○古賀啓太郎・粟野皓光・池田　誠（東大）

暗号実装
4. パイプライン型剰余乗算器を用いたペアリング計算器における圧縮自乗算の高速化
　○奥秋陽太・坂本純一・吉田直樹・藤本大介・松本　勉（横浜国大）
5. Keyed RNS MR アルゴリズムの FPGA 実装時における最適な基底選択と評価
　○郡　義弘・藤本大介・林　優一（奈良先端大）・本間尚文（東北大）
6. 数論変換に基づく Ring-LWE 暗号ハードウェアの高効率実装に関する検討
　○遠藤　空・上野　嶺・青木孝文・本間尚文（東北大）

セキュリティ評価
7. OSS-RSA からのキャッシュリークの取得容易性評価
　○森　隼人・上野　嶺（東北大）・高橋順子（NTT）・林　優一（奈良先端大）・本間尚文（東北大）
8. 命令置換レーザーフォールト攻撃の ARM プロセッサ上ペアリング実装に対する効果
　○坂本純一・松本　勉（横浜国大）

◆IEEE SSCS Japan Chapter, IEEE SSCS Kansai Chapter 共催
☆HWS 研究会今後の予定 〔　〕内発表申込締切日
12 月 13 日（木） 東大武田先端知ビル〔未定〕テーマ：ハードウェアセキュリティフォーラム 2018
【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/jpn/ken/kenmoushikomi.html
【問合先】 HWS 研究会幹事
E-mail：hws-sec@mail.ieice.org
☆ICD 研究会今後の予定 〔　〕内発表申込締切日
12 月 21 日（金）～23 日（日） 宮古島（会場選定中）〔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/jpn/ken/kenmoushikomi.html
【問合先】
橋本　隆（パナソニック）
E-mail：hashimoto.takashi1967@jp.panasonic.com