

ハードウェアセキュリティフォーラム2017 プログラム
場所: 東京大学・武田ホール, 日時: 12月15日(金) 10:00-17:00

番号	時間	講演者/著者	所属	講演/ポスター題目	
口頭 発表	講演1	10:00-10:10	松本勉・本間尚文	横浜国立大学・東北大学	開会の挨拶
	講演2	10:10-10:40	松本勉	横浜国立大学	フィジカルオブジェクトとデジタルオブジェクトの対応を保障するセキュリティ技術
	講演3	10:40-11:10	永田真	神戸大学	ICチップのハードウェア・ロジックと対策の技術動向
	講演4	11:10-11:40	植村泰佳	EGSEC.TRA	ハードウェアセキュリティと標準 ~ ハードウェア分野における情報セキュリティ評価認証技術の進展 ~
	講演5	11:40-12:10	成吉雄一郎	ルネサスエレクトロニクス	コモンライテリアの観点から考察したセキュアLSI設計・製造の課題
	休憩				
	講演6	13:45-14:05	遠山毅	トヨタIT開発センター	自動車向けセキュリティテストベッドの開発
	講演7	14:05-14:25	舘橋玄武・原田貴史・伊藤宏樹	NTT	V2Xシステムにおけるセキュリティの取り組み ~ 自律型モビリティシステムの高信頼化に向けた取り組みについて ~
	講演8	14:25-14:45	夏徹帆・駒野雄一・川端健・清水秀夫	東芝	擬似乱数を利用した車載CANの不正通信検出技術
	講演9	14:45-15:05	野上保之	岡山大学	楕円曲線暗号に対するSW/HW攻撃に関する報告
	講演10	15:05-15:25	本間尚文	東北大学	CHES2017報告
休憩					
講演11	15:40-16:20	ポスターライトニングトーク (各ポスター2分程度の紹介)			
ポスタ 発表	ポスタ1	16:20-17:00	長浜佑介・藤本大介・松本勉	横浜国立大学	バイナリ拡張ユークリッド互除法を用いた逆元計算器による254ビット素数BN曲線上の optimal ateペアリング計算高速化手法のFPGA実装評価
	ポスタ2	16:20-17:00	市橋忠之・粟野皓光・池田誠	東京大学	BN曲線上におけるペアリング演算プロセッサの最適実装
	ポスタ3	16:20-17:00	松本年史・小野寛享・日下卓也・野上保之	岡山大学	Raspberry Pi上におけるID-base認証の性能評価
	ポスタ4	16:20-17:00	古賀啓太郎・粟野皓光・池田誠	東京大学	格子暗号の高速化に向けた数論変換に基づく多項式乗算器の設計
	ポスタ5	16:20-17:00	斎藤徹介・粟野皓光・池田誠	東京大学	楕円曲線上のデジタル署名アルゴリズムに向けた小面積プロセッサの設計
	ポスタ6	16:20-17:00	杉山昇太郎・粟野皓光・池田誠	東京大学	準同型論理演算のハードウェア実装によるスループットの向上
	ポスタ7	16:20-17:00	三浦典之・高橋雅典・松田航平・永田真	神戸大学	チップ・パッケージ・ボード非接触インターアクションとカオス発振を利用したPUF
	ポスタ8	16:20-17:00	野崎佑典・吉川雅弥	名城大学	遺伝的プログラミングに基づくレスポンス推定手法
	ポスタ9	16:20-17:00	伊東燦・上野嶺・本間尚文・青木孝文	東北大学	ハードウェアトロイ挿入が困難な公開鍵暗号データパスに関する検討
	ポスタ10	16:20-17:00	任翔太・藤本大介・林優一・ 三浦典之・永田真・松本勉	奈良先端科学技術大学院大学・ 神戸大学・横浜国立大学	インピーダンス計測に基づくICの周辺に実装されたHT検出手法の検討
	ポスタ11	16:20-17:00	宮田大輔・ヴィッレ・ウリマウル・ 本間尚文・林優一・青木孝文	東北大学・ 奈良先端科学技術大学院大学	スマートデバイスからの電磁的情報漏えいの評価に関する検討
	ポスタ12	16:20-17:00	五百旗頭健吾・矢野佑典・手嶋俊彰・ 熊野靖也・河田直樹・豊田啓孝	岡山大学	暗号ICのSCA安全性評価技術に関する検討
	ポスタ13	16:20-17:00	奥富賢哉・坂本純一・松本勉	横浜国立大学	希出現波形に着目したテンプレート攻撃
	ポスタ14	16:20-17:00	楠卓朗・久保田貴也・汐崎充・藤野毅	立命館大学	AUTOSAR仕様に基づくTruncated MAC付きCANメッセージを想定したサイドチャネル攻撃手法
	ポスタ15	16:20-17:00	白井和樹・清川貴仁・松本勉	横浜国立大学	CANにおける波形置換型電氣的データ改ざん
	ポスタ16	16:20-17:00	井上侑哉・野平浩生・吉田直樹・ 藤本大介・松本勉	横浜国立大学	超音波センサに対する煤質操作攻撃の可能性

