ハードウェアセキュリティフォーラム2016プログラム

場所: 武蔵大学・50周年記念ホール, 日時: 12月3日(土) 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	10:00-10:15	松本勉	横浜国立大学	ハードウェアセキュリティ(HWS)時限研究専門委員会の紹介
	講演2	10:15-10:45	松本勉	横浜国立大学	IoTを支えるハードウェアセキュリティと計測セキュリティ
	講演3	10:45-11:15	池田誠	東京大学	IEEE SSCS (ISSCC, VLSI symposium, A-SSCC, ESSCIRC)における動向
	講演4	11:15-11:35	上野嶺・森岡澄夫・本間尚文・青木孝文	東北大学	CHESの紹介と日本からの発表
	講演5	11:35-11:55	藤本大介・長浜佑介・松本勉	横浜国立大学	高機能暗号実装に向けた剰余乗算器のエネルギーに着目した実装検討
	講演6	11:55-12:15	三浦典之・永田真	神戸大学	チップ・パッケージ・ボードレベルの物理攻撃対策回路技術
	講演7	13:30-13:50	高比良賢一・宮内成典	ルネサスエレクトロニクス	ルネサスにおける自律したIoTのためのセキュリティ技術の取組み(仮)
	講演8	13:50-14:10	高橋順子	NTT	自動車のサイバー攻撃対策技術に関するNTTの取組み
	講演9	14:10-14:30	佐伯稔・塚元卓・櫻井玄弥・橋本徹	情報処理推進機構・三菱電機	ホワイトボックス暗号の実装安全性に関する一考察 ～ ホワイトボックス暗号に対する攻撃の試行 ～
	講演10	14:30-14:50	松木隆宏	FFRI	Black Hatの概要と研究動向の紹介
	講演11	14:50-15:10	三上修吾・崎山一男	日立製作所・電気通信大学	プライバシ保護可能な認証プロトコルのRFIDタグ実装と性能評価
	講演12	15:10-15:30	国井裕樹	セコム株式会社	サービス事業者からみるハードウェアセキュリティ
ポスタ発表	講演13	15:30-16:00	ポスターライトニングトーク (各ポスター1分程度の紹介)		
	ポスタ1	16:00-17:00	野崎佑典・吉川雅弥	名城大学	Minalpherに対する電磁波解析とその評価
	ポスタ2	16:00-17:00	宮元景冬・崎山一男	電気通信大学	DSP C6678における剰余乗算の高速実装評価
	ポスタ3	16:00-17:00	白畑正芳・名倉優輝・大倉俊介・石川賢一郎・盛一也・汐崎充・久保田貴也・高柳功・藤野毅	立命館大学・ブリルニクスジャパン	CMOSイメージセンサのばらつきを利用したPUF技術の検討
	ポスタ4	16:00-17:00	坂本純一・藤本大介・松本勉	横浜国立大学	組込みメモリに対するレーザー照射と電力解析を用いた複合攻撃
	ポスタ5	16:00-17:00	池田司・池田誠	東京大学	1024bitまでの有限体上の演算と256bitまでの楕円曲線上の演算のための汎用暗号プロセッサ
	ポスタ6	16:00-17:00	相馬一樹・藤本大介・松本勉	横浜国立大学	測距パルスLIDARに対する反射光偽装と計測セキュリティ
	ポスタ7	16:00-17:00	吉田直樹・松本勉	横浜国立大学	耐タンパー性とナノ人工物メトリクス
	ポスタ8	16:00-17:00	中山淑文・清川貴仁・藤本大介・松本勉	横浜国立大学	CANおける電気的データ改竄攻撃と電圧波形解析による検知手法
	ポスタ9	16:00-17:00	葛西誠也・清水克真・佐々木健太郎・殷翔・法元盛久・成瀬誠・松本勉	北海道大学・大日本印刷・NICT・横浜国立大学	ナノ人工物メトリクスのための2次元ナノ構造電気的識別手法の基礎検討
	ポスタ10	16:00-17:00	斎藤僚介・池田誠	東京大学	楕円曲線暗号の小規模実装への取り組み
	ポスタ11	16:00-17:00	市橋忠之・池田誠	東京大学	高機能暗号向けペアリング演算器の実装
	ポスタ12	16:00-17:00	神内良太・猪俣敦夫・新井イスマイル・藤川和利	奈良先端科学技術大学院大学・東京電機大学	IoT機器のエンドポイントセキュリティ用ハードウェアデバイスの提案
	ポスタ13	16:00-17:00	稲葉光太郎・今井雅	弘前大学	非同期式回路に対するハードウェアトロイ挿入に関する一考察
	ポスタ14	16:00-17:00	熊木武志・吉川雅弥・小倉武・藤野毅	立命館大学・名城大学	ハードウェアトロイ検証環境の開発とTDES/AES回路を用いた実装及び評価
	ポスタ15	16:00-17:00	佐伯稔・塚元卓・櫻井玄弥・橋本徹	情報処理推進機構・三菱電機	これからのセキュリティ製品に求められること～開発者が知っておきたいハードウェアセキュリティ～
	ポスタ16	16:00-17:00	佐伯稔・塚元卓・櫻井玄弥・橋本徹	情報処理推進機構・三菱電機	暗号モジュール試験及び認証制度(JCMVP)～国際規格ISO/IEC19790に基づく試験・認証～
	ポスタ17	16:00-17:00	汐崎充・久保田貴也・藤野毅	立命館大学	耐タンパ車載セキュリティシステムの開発
	ポスタ18	16:00-17:00			SIPサイバー「IoTのセキュリティを実現する超低電力暗号実装技術」
	ポスタ19	16:00-17:00			先導研究「高機能暗号を活用した革新的ビッグデータ処理の研究開発」
	ポスタ20	16:00-17:00			IoT横断「Sensor-to-Cloud Security ～ ビッグデータを守る革新的IoTセキュリティ基盤技術の研究開発」

ハードウェアセキュリティフォーラム 2016 プログラム

場所: 武蔵大学・50 周年記念ホール, 日時: 12 月 3 日(土) 10:00-17:00

講演 1 10:00-10:15
松本勉 (横浜国立大学)
ハードウェアセキュリティ(HWS)時限研究専門委員会の紹介

講演 2 10:15-10:45
松本勉 (横浜国立大学)
IoT を支えるハードウェアセキュリティと計測セキュリティ

講演 3 10:45-11:15
池田誠 (東京大学)
IEEE SSCS (ISSCC, VLSI symposium, A-SSCC, ESSCIRC)における動向

講演 4 11:15-11:35
上野嶺・森岡澄夫・本間尚文・青木孝文 (東北大学)
CHES の紹介と日本からの発表
概要: 暗号実装やハードウェアセキュリティに関する最も主要な国際会議の一つである Cryptographic Hardware and Embedded Systems (CHES) について、その概要や最新の動向を紹介する。また、今年の同会議で講演者らが発表した高効率暗号プロセッサ設計について紹介する。

講演 5 11:35-11:55
藤本大介・長浜佑介・松本勉 (横浜国立大学)
高機能暗号実装に向けた剰余乗算器のエネルギーに着目した実装検討
概要: 本発表では高機能暗号に重要な剰余乗算器について、専用ハードウェア実装をエネルギーに着目して検討する。 KC705 ボード上に実装を行い、回路規模, 演算速度、エネルギーなどをまとめ議論する。

講演 6 11:55-12:15
三浦典之・永田真 (神戸大学)
チップ・パッケージ・ボードレベルの物理攻撃対策回路技術
概要: 本発表では、暗号処理回路に対するサイドチャネル攻撃をはじめとした物理攻撃に対抗するチップ・パッケージ・ボードレベルの回路対策技術を紹介する。

お昼休み 12:15-13:30
第三回ハードウェアセキュリティ時限研究専門委員会
(専門委員の皆さんはご参集ください。場所は追ってご連絡いたします。)

講演 7 13:30-13:50
高比良賢一・宮内成典　（ルネサスエレクトロニクス）
ルネサスにおける自律した IoT のためのセキュリティ技術の取組み

講演 8 13:50-14:10
高橋順子　（NTT）
自動車のサイバー攻撃対策技術に関する NTT の取組み
概要: NTT が取り組む自動車のサイバー攻撃対策技術に関する取り組みを発表する。具体的には、車載ネットワークに対する攻撃手法・対策、イモビライザーといった自動車関連ハードウェアに関する攻撃手法・対策を発表する。

講演 9 14:10-14:30
佐伯稔・塚元卓・櫻井玄弥・橋本徹　（情報処理推進機構・三菱電機）
ホワイトボックス暗号の実装安全性に関する一考察 ～ ホワイトボックス暗号に対する攻撃の試行～
概要: ハードウェアセキュリティに対する IPA の取り組みを簡単に紹介する。 また、ホワイトボックス暗号に対して DCA(Differential Computation Analysis)と DPA(Differential Power Analysis)を試行した結果を報告する。

講演 10 14:30-14:50
松木隆宏　（FFRI）
Black Hat の概要と研究動向の紹介
概要: 未知の脆弱性や脅威を実証する研究が多数発表される産業系セキュリティ国際会議 Black Hat の概要とそこで発表されたハードウェアに関する研究の一部をご紹介します。

講演 11 14:50-15:10
三上修吾・崎山一男　（日立製作所・電気通信大学）
プライバシ保護可能な認証プロトコルの RFID タグ実装と性能評価
概要: RFID タグにおけるプライバシ問題の解決策として、暗号アルゴリズムを用いた認証プロトコルが提案されているが、性能検証はされてこなかった。本発表では上記の認証プロトコルを実行可能な RFID タグの設計、実装と性能評価を報告する。

講演 12 15:10-15:30
国井裕樹　（セコム株式会社）
サービス事業者からみるハードウェアセキュリティ
概要: IoT/CPS のセキュリティの重要性が多く議論されているが、ハードウェアセキュリティは最重要な分野である。本発表ではサービス事業者の立場からハードウェアセキュリティに必要な視点と今後のこの分野への期待を述べる。

講演 13 15:30-16:00
ポスターライトニングトーク（各ポスター講演者から 1 分程度の研究紹介をして頂きます。）

ポスター展示 16:00-17:00
ポスター1
野崎佑典・吉川雅弥　　（名城大学）
Minalpher に対する電磁波解析とその評価
概要: 本研究では、代表的な認証暗号である Minalpher に対する電磁波解析を提案する。そして、FPGA を用いた評価実験により提案手法の有効性を実証する。

ポスター2
宮元景冬・崎山一男　　（電気通信大学）
DSP C6678 における剰余乗算の高速実装評価

ポスター3
白畑正芳・名倉優輝・大倉俊介・石川賢一郎・盛一也・汐崎充・久保田貴也・高柳功・藤野毅
　　（立命館大学・ブリルニクスジャパン）
CMOS イメージセンサのばらつきを利用した PUF 技術の検討
概要: CMOS イメージセンサの PUF 提案を行い、既にシミュレーション検討、実測データより PUF の可能性を示した。今回、さらなる実測を加え、温度・電圧依存性など PUF としての性能について議論する。

ポスター4
坂本純一・藤本大介・松本勉　　（横浜国立大学）
組込みメモリに対するレーザー照射と電力解析を用いた複合攻撃
概要: レーザー照射および電力解析を組み合わせて、組み込みメモリから読み出される値を抽出する手法を提案する。本研究では DUT に実装されたフラッシュメモリから読み出し中の値を復元できた結果が示される。

ポスター5
池田司・池田誠　（東京大学）
1024bit までの有限体上の演算と 256bit までの楕円曲線上の演算のための汎用暗号プロセッサ

ポスター6
相馬一樹・藤本大介・松本勉　　（横浜国立大学）
測距パルス LIDAR に対する反射光偽装と計測セキュリティ
概要: 光パルス伝播方式で測定を行う距離計を対象とし、測定光以外の光を入力し出力を操作する攻撃について紹介する。また、あるパルス伝播方式 LIDAR に対して、実際に反射光を偽装する実験についても紹介する。

ポスター7
吉田直樹・松本勉　　(横浜国立大学)
耐タンパー性とナノ人工物メトリクス
概要: 耐クローン性を向上させる技術の 1 つとして、ナノオーダーの微細な凹凸を利用したナノ人工物メトリクスが挙げられる。本発表では、実際にクローンを作製し、その耐クローン性の評価を行った結果を報告する。

ポスター8
中山淑文・清川貴仁・藤本大介・松本勉　　(横浜国立大学)
CAN おける電気的データ改竄攻撃と電圧波形解析による検知手法
概要: CAN において、バスに流れたデータを送信側と受信側の ECU に気付かれずに改竄を行う電気的データ改竄の脅威を指摘する。更に、バスの電圧波形解析によりこの攻撃を検知する手法の提案を行う。

ポスター9
葛西誠也・清水克真・佐々木健太郎・殷翔・法元盛久・成瀬誠・松本勉　　(北海道大学・大日本印刷・NICT・横浜国立大学)
ナノ人工物メトリクスのための２次元ナノ構造電気的識別手法の基礎検討
概要: 半導体プロセスにより形成されるランダム２次元ナノ構造を利用するナノ人工物メトリクスにおいては小型かつ高速な構造識別可能な手法が望まれている。ここでは半導体 FET を応用した２次元構造電気的識別手法を考案し基礎的検討を行った結果について報告する。

ポスター10
斎藤僚介・池田誠　　(東京大学)
楕円曲線暗号の小規模実装への取り組み

ポスター11
市橋忠之・池田誠　　(東京大学)
高機能暗号向けペアリング演算器の実装

ポスター12
神内良太・猪俣敦夫・新井イスマイル・藤川和利　　(奈良先端科学技術大学院大学・東京電機大学)
IoT 機器のエンドポイントセキュリティ用ハードウェアデバイスの提案
概要: 本発表では、プラント等の制御システムで使用することを想定した IoT 機器に対して、攻撃検知を行うデバイスを回路に追加することにより特定の攻撃からエンドポイントでセキュリティを確保する方法を提案する。

ポスター13
稲葉光太郎・今井雅　　(弘前大学)
非同期式回路に対するハードウェアトロイ挿入に関する一考察
概要: 非同期式回路は遅延変動に対して高耐性な VLSI システムを実現出来 るが、遅延非依存特性は攻撃者にとって有利に働くことがある。本 稿では非同期式オンチップネットワークルータにトロイを挿入し、 評価した結果を紹介する。

ポスター14
熊木武志・吉川雅弥・小倉武・藤野毅　　(立命館大学・名城大学)
ハードウェアトロイ検証環境の開発と TDES/AES 回路を用いた実装及び評価
概要: 本発表では、ハードウェアトロイの概要について述べるとともに、開発した検証用ボードについて説明する。そして、トリプル DES と AES 暗号化回路に仕込んだハードウェアトロイについて詳述する。実験では、検証用ボードを用いた ARM コアベースの SoC において、暗号処理の無効化、及び秘密鍵の流出という被害を確認することができた。

ポスター15
佐伯稔・塚元卓・櫻井玄弥・橋本徹　　(情報処理推進機構・三菱電機)
これからのセキュリティ製品に求められること～開発者が知っておきたいハードウェアセキュリティ～

ポスター16
佐伯稔・塚元卓・櫻井玄弥・橋本徹　　(情報処理推進機構・三菱電機)
暗号モジュール試験及び認証制度(JCMVP)～国際規格 ISO/IEC19790 に基づく試験・認証～

ポスター17
汐崎充・久保田貴也・藤野毅　　(立命館大学)
耐タンパ車載セキュリティシステムの開発
概要: これまで本研究室で取り組んできた自動車のネットワーク化により顕在化した車載セキュリティに関する研究と、車載デバイスにおけるサイドチャネル攻撃の脅威と対策技術に関する研究を紹介する。

ポスター18
SIP サイバー「IoT のセキュリティを実現する超低電力暗号実装技術」

ポスター19
先導研究「高機能暗号を活用した革新的ビッグデータ処理の研究開発」

ポスター20
IoT 横断「Sensor-to-Cloud Security ～ ビッグデータを守る革新的 IoT セキュリティ基盤技術の研究開発」