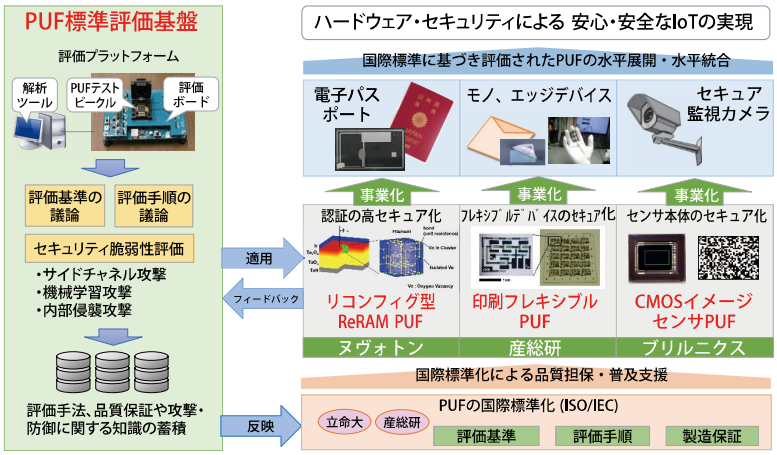
複製不可能デバイスを活用したIoT ハードウェアセキュリティ基盤の研究開発

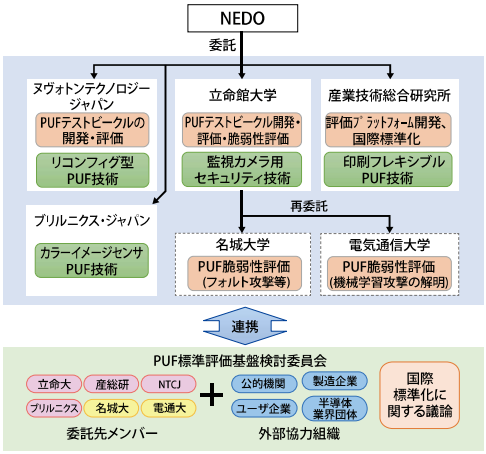
委託先　立命館大学、産業技術総合研究所、ヌヴォトンテクノロジージャパン、ブリルニクスジャパン

概　要

本研究では、「IoT末端系のハードウェアセキュリティ」に対して、機器の真正性・データの完全性や機密性を「物理複製不可能デバイスPUF」を用いることで飛躍的に向上させるための基盤技術開発を行った。新型PUF技術として「リコンフィグ型PUF　(ReRAM-PUF)」、「印刷フレキシブルPUF」、「CMOSイメージセンサPUF」を開発し、従来不可能であったセンサデバイスへのセキュリティ機能付与、多用途なフレキシブルデバイスへの低コストセキュリティ機能搭載を実現した。開発した新型PUF技術は、電子パスポート、耐タンパ封筒・フレキシブルセンサ、セキュア監視カメラ等での事業化展開を目指す。また、従来型PUFを含むテストビークルを試作し、PUFの性能指標や脆弱性評価を再委託先の大学を含む研究チームで一体となって行った。評価結果について委託先以外の組織を含む「PUF標準評価基盤検討委員会」で議論を行い、PUFの評価基準ならびに評価手順をISO/IEC 20897で国際標準化し、PUF技術が産業界で広く使われるように活動した。

事業内容

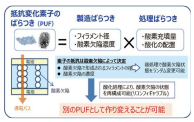




リコンフィグ型PUF (ReRAM-PUF) の開発
(ヌヴォトン テクノロジー ジャパン株式会社)

概　要

■リコンフィグ型PUFとは？
- リコンフィグ型PUFは更新可能なPUFのこと
- ReRAM-PUFは、製造プロセスと電気的ストレスのバラツキで決定される
- 電気的印加手法の工夫で別物PUFに更新

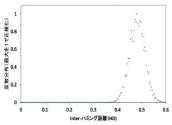


■リコンフィグ型PUFの意義
- 従来型のPUFではサプライチェーンの内部犯行者による攻撃に脆弱
- 流通業者ごとにPUFをリコンフィグし過去のPUF情報完全消去
- 下流業者へPUF漏洩リスク伝搬を防止し安全なサプライチェーンを提供

目標・成果

■研究の目標
- リコンフィグ型PUFは、リコンフィグ前後で如何にランダム(ユニーク)にデータが変化するかが重要
- リコンフィグ実行前後のユニーク指標であるハミング距離 (HD)が0.3以上を技術目標に設定

■研究の成果
- 電気的ストレスの印加手法の最適化検討を推進し、ユニーク指標であるハミング距離が0.48と大幅に目標を達成
  理想限界 (HD=0.5)に近いランダム性能を確保



事業化に向けて

■ICAO(国際民間航空機関)での技術プレゼンからの知見
- 電子パスポートはテロなども意識してサプライチェーンセキュリティーへPUFを適用する提案に高い関心が得られた

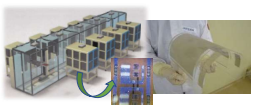
■事業化の方針
- リコンフィグ型PUFをICカードに展開し、電子パスポートにおける強固なサプライチェーンを提案しグローバル参入を推進する

■事業化に向けたリスク
- コロナ禍において電子パスポートに対する各国の投資機運の低下により参入チャンスが当初見込みから２～３年遅延の可能性が高まる

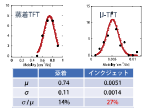
印刷フレキシブルPUF
(国立研究開発法人産業技術総合研究所)

概　要

- 低コストでフレキシブルな印刷型PUFを開発し、シリコンデバイスだけではカバーできない様々なモノにセキュリティを付与し用途拡大
- 有機材料を用いた印刷等の製造プロセスにより、バラつきの度合いを任意に付与することでPUFとして性能強化



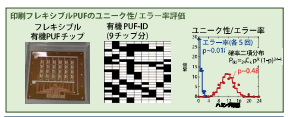
印刷デバイス製造ライン

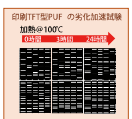


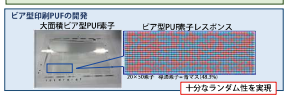
プロセス選択によるバラつきの付与

成　果

- 有機材料を用いたPUFで２V駆動、エラー率0.1%を実現
- エラー率が1.8%と低く、理想的なユニーク性(IHD:0.48)を持つPUF回路を開発
- 適切な封止膜により1年以上の安定動作を実現
- 量産化に特化したピア型PUFの製造プロセスを開発



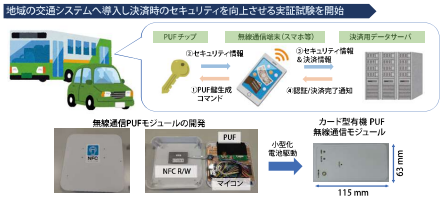




事業化・今後の展望

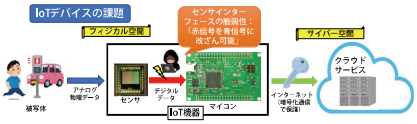
- モノへのセキュリティに関するサービス市場の３つのステージ（創出、先導、けん引）を同時進行的に進めることで**デファクトスタンダードを勝ち取る**
- 多数保有する印刷PUF特許の戦略的活用で企業連携により事業多面化

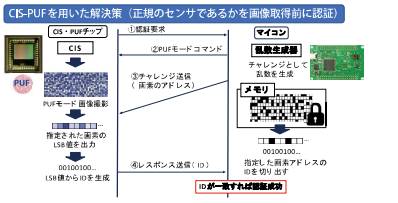
地域の交通システムへ導入し決済時のセキュリティを向上させる実証試験を開始



CMOSイメージセンサPUF
(ブリルニクスジャパン・立命館大学)

- IoT機器には様々なセンサが接続され、得られた情報をデジタル化してクラウドなどのサイバー空間上に転送し解析・制御が行われる. 得られた**センサ情報が正しいかどうかを確認できること**が重要
- センサで得られた情報の真正性を確認する手法は以下の２種
  (1)センサデバイスの認証 (正規のセンサが接続されているか？) ⬅下記図面
  (2)センサデータへの認証コード (MAC) の付与 ⬅成果最大化活動の図面

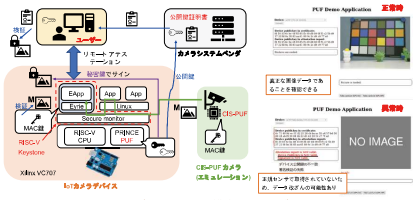




成果最大化活動 (立命大とNEDO他チーム間の連携)
PUFを信頼の基点としたRISC-V 信頼実行環境(TEE)の構築

- 目的：IoTデバイスで取得したデータを信頼できるものにする　➡**ソフトウェアとハードウェアの連携**によるデータの真正性確認が必要
  (1)ソフトウェア：TEE(信頼実行環境)としてRISC-V KeystoneをFPGA上に実装*注
  (2)ハードウェア：FPGA上に**信頼の基点となるPUF**を実装, CIS-PUFの利用を想定
  (3)PUFを信頼の基点とするRISC-V Keystoneのリモートアテステーションにより検証した実行環境で, 画像データの真正性を確保できるデモシステムを構築

*注：RISC-V Keystone環境の構築は、NEDO 革新的AIエッジコンピューティング技術の開発「セキュアオープンアーキテクチャ基盤技術とそのAIエッジ応用研究開発」の成果を利用しており、チーム間連携としてAPIを開発しました



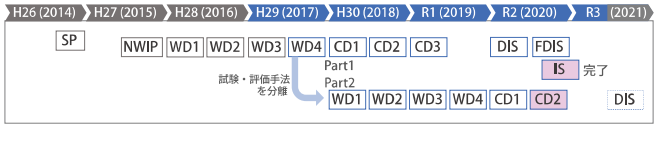
RISC-V/Keystone with PUFデモシステムの構成　　デモシステム動作画面

ISO/IEC での PUF の国際標準化活動

ISO/IEC 20897-1 (Part 1)
PUFのセキュリティ要件
Physically unclonable functions -- Part1: Security requirements
2020年12月 IS発行

ISO/IEC 20897-2 (Part 2)
PUFの試験及び評価手法
Physically unclonable functions -- Part2: Test and evaluation methods
2021年8月現在 CD2

2017.10 Berlin	WD4		2019.10 Paris	Part1		
2018.4 武漢	Part1 CD1			Part2	WD4	
	Part2 WD1		2020.4 Zoom	Part1	DIS	
2018.9 Gjøvik	Part1 CD2			Part2	CD1	
	Part2 WD2		2020.9 Zoom	Part1	FDIS→	IS
2019.4 Tel-Aviv	Part1 CD3			Part2	CD2	
	Part2 WD3		2021.9 Zoom	Part2	DIS	(見込)



SP: Study period
NWIP: New work item proposal
WD: Working draft
CD: Committee draft
DIS: Draft international standard
FDIS: Final draft international standard
IS: International standard

主な業績

受　賞

1. **ハードウェアセキュリティ研究会若手優秀賞**（後藤裕太, 汐崎充, 藤野毅, "Fuzzy Extractorの誤り訂正回路に対するサイドチャネル攻撃," HWS研究会, 2018年7月）
2. **SCIS論文賞**（前田悠磨, "サイドチャネル攻撃対策を施したAES回路に対する深層学習を用いたサイドチャネル攻撃," 暗号と情報セキュリティシンポジウム (SCIS), 2020年1月）
3. **国際規格開発賞**（濱口 総志, "Information security, cybersecurity and privacy protection -- Physically unclonable functions -- Part 1: Security requirements," 情報処理学会 情報規格調査会, 2021年1月）

特　許

1. 特願2018-008399, 固体撮像装置, 固体撮像装置の駆動方法, および電子機器
2. 特願2018-008400, 固体撮像装置, 固体撮像装置の駆動方法, および電子機器
3. 特願2018-067705, 固体撮像装置, 固体撮像装置の駆動方法, および電子機器
4. 特願2018-212194, カメラシステムおよびカメラシステムの駆動方法
5. 特願2018-241679, 不揮発性メモリ装置およびチャレンジ・レスポンス方法
6. 特願2019-039240, 固体撮像装置, 固体撮像装置の駆動方法, および電子機器

主催シンポジウム

1. 第1回 Physically Undonable Function技術シンポジウム, 立命館大学東京キャンパス, 2018年3月16日
2. 第2回 Physically Undonable Function技術シンポジウム, 立命館大学東京キャンパス, 2019年3月14日

事業者からのメッセージ

様々な機器やセンサがネットワーク上でつながるInternet of Things (IoT) では、デバイスの真正性やデータの機密性・完全性を確保することが必要不可欠です. 高信頼または低コストで信頼の基点を構築できるハードウェアとして、3種類のPhysically Unclonable Function (PUF) を開発しました。また、PUFを事業化していくための開発者やユーザにとって、セキュリティ要件や評価手法の統一した基準が必要です. 本プロジェクトではPUFを評価するための基盤を構築しその知見をもとに、ISO/IEC 20897で国際標準化しました。興味のある技術があれば是非お問い合わせ下さい。

連絡先
立命館大学理工学部　藤野 毅
E-mail: fujino@se.ritsumei.ac.jp
産業技術総合研究所デバイス技術研究部門　堀 洋平
E-mail: hori.y@aist.go.jp
産業技術総合研究所センシングシステム研究センター　植村 聖
E-mail: sei-uemura@aist.go.jp
ヌヴォトンテクノロジージャパン株式会社　吉岡 和樹
E-mail: yoshioka.kazuki@nuvoton.com

この成果は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務（JPNP16007）の結果得られたものです。