ポスター番号

P-11-60

ICT重点技術の研究開発

設計・製造におけるチップの脆弱性検知手法の研究開発

研究機関（早稲田大学、KDDI総合研究所、株式会社ラック）

研究開発の概要

【政策目標】

- ハードウェアチップに故意に組み込まれた脆弱性は、サプライチェーン上の大きな脅威であり、製品に実装された不正回路は後から対処するのが困難であることから、設計・製造におけるチップの脆弱性検知手法の確立は急務となっている。
- 本研究開発では産学官連携により、ハードウェアチップの設計・製造、及びその利用における脆弱性検知手法、並びにサプライチェーン上での運用技術を確立するとともに、当該技術の社会実装を加速する。また、安全なハードウェアチップの設計･製造に関する特許取得、業界標準化、国際標準化等を通じて、同分野における我が国の国際競争力強化を図る。

【研究開発目標】

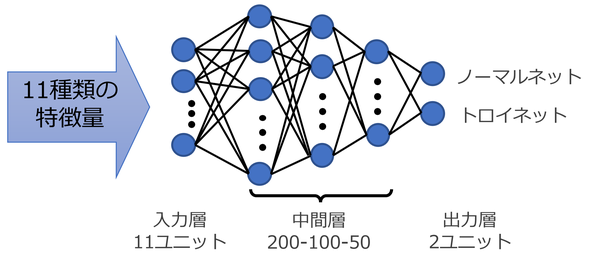
課題Ⅰ　回路情報を用いて不正回路を検知する技術：外部から調達した設計ツールや設計部品を用いたチップ設計全体の安全性を担保するために、回路情報の中に不正に改変された回路が含まれるか、機械学習等のAIを活用して検知する技術。

課題Ⅱ　電子機器の外部から観測される情報を用いて不正動作を検知する技術：市販の組込みマイコン等の、回路情報が入手できないチップの安全性を担保するために、不正回路が組み込まれたチップにより構成される電子機器に対し、電力波形の特定部分の電力量や継続時間等、電子機器の外部から観測される情報を用いて、不正動作を機械学習等のAIを活用して検知する技術。

研究開発の成果・課題Ⅰ

Ⅰ－ア）①不正回路を識別するための特徴量抽出技術に関する要素技術開発

- ベンチマーク回路を使い、11種類の特徴量を用いることで、ニューラルネットワーク識別器によるトロイ信号線を識別（識別した信号線数は合計で数十万以上のデータ）



多層ニューラルネットワークを用いた識別結果

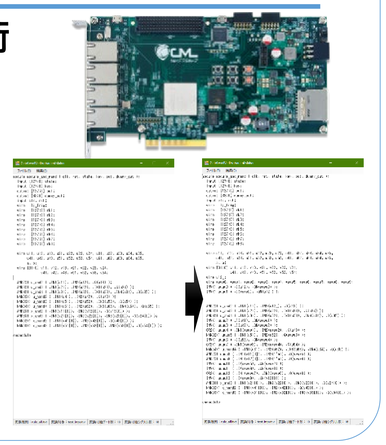
TPR（True Positive Rate）84%以上、
TNR（True Negative Rate）95%以上
（見逃し確率16%以下、誤検知率5%以下）

②設計・製造におけるチップ脆弱性検知手法に関する動向調査

- ハードウェアトロイの機能ごとに、サプライチェーン上の影響の分析を実施し、研究開発の実用化に反映
  - ➢ 情報の機密性及び安全性を脅かす機能はサプライチェーン上流のメーカに法的責任が生じ得るため、対処が必要
  - ➢ 今後の実用化・社会実装に向け、機密性を損なう回路／派生回路および安全性を損なう回路／派生回路を検知する技術を確立

Ⅰ－イ）AI/機械学習に基づく不正回路検知技術

- 実回路におけるハードウェアトロイの検知に向け、AIによる不正回路の検知技術の高度化のための調査及び不正回路サンプルの実装、亜種生成手法の開発を実施



①不正回路の体系化を完了

Trust-HUBから取得した88個のサンプルを詳細に分析し、分類

②不正回路の新規サンプル(12種類)の実装を完了

IoT開発ボード向け6種類、FPGA開発ボード向け3種類、FPGA搭載ネットワークボード向け3種類を実装

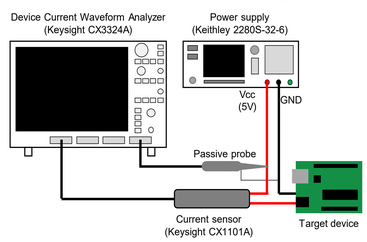
③亜種生成手法を開発

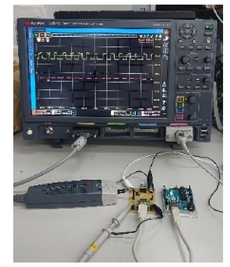
不正回路の回路情報（ゲートレベル記述のVerilog-HDL）から、亜種の回路情報を自動生成する手法を開発

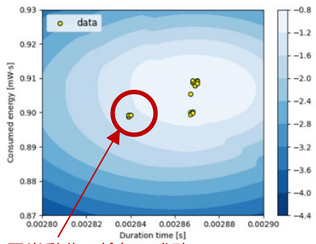
研究開発の成果・課題Ⅱ

Ⅱ－ア）外部情報を取得する電子機器の動作のモデル化技術

- 組込みマイコンに対して、異常動作をモデル化し（暗号通信に対して、まれに暗号化がなされないモデルを構築）、消費電力を利用した異常動作の検知手法を確立し、検知に成功



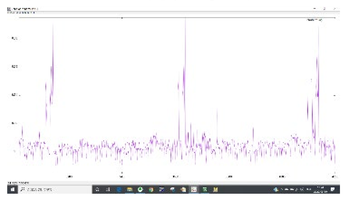




異常動作の検知に成功

Ⅱ－イ）AI/機械学習に基づく不正動作検知技術に関する研究開発

- 電子機器から観測される電力を測定可能とする高精度アナログモジュールの実装、AI実現のための事前調査、分野横断的な電子機器の調査と不正プログラムの動向調査を実施



①高精度アナログモジュールの実装

目標であるサンプリング1kHz、電力測定誤差±0.1mWに対しサンプリング5kHz、 電力測定誤差±0.01mWまで実現

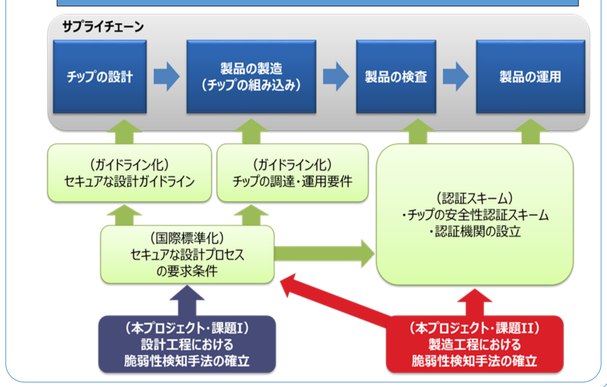
②AI実現のための事前調査の実施

AI機能についてニューラルネットワークがFPGAに対して現実的な数となるか検討し、15,000個のLUTを有するFPGAに実装可能であることを確認

③電子機器に利用されるICチップの調査と不正プログラムの動向調査の実施

- 不正回路の実在の裏付として、ICチップそのものを不正にコピーして流通させることが行われている事実を確認
- 複数アーキテクチャにおいて1000個の不正プログラムを収集

政策目標の達成に向けた計画



※本事業には内閣府「官民研究開発投資拡大プログラム(PRISM)」の予算を活用している。

【本研究開発成果に関する連絡先】KDDI総合研究所　フューチャーデザイン1部門　橘

ICTイノベーションフォーラム2020
ICT重点技術の研究開発プロジェクト