IoT デバイス向け電子指紋とセキュア認証

技術分野分類	情報学 計算基盤　1106 情報セキュリティ
技術キーワード	暗号・セキュリティ、認証
産　業　分　類	Ｅ－２８：電子部品・デバイス・電子回路製造業

内容

概　要

従来技術・競合技術との比較（優位性）

本技術の有用性

○研究概要

あらゆるハードウェアがインターネットに接続される Internet of Things (IoT) では，安全性を確保するために適切な認証を行うことが重要である。本研究では，半導体の製造時に生じる電気特性のばらつきを各デバイスの固有値として認証する PUF をベースとする認証システムを開発した。提案システムでは，物理的に複製不可能なだけでなく，数学的にも複製が出来ない認証用の ID の生成を行う。また，暗号回路の一部を PUF に利用する併用アーキテクチャを考案し，小面積実装を実現している。

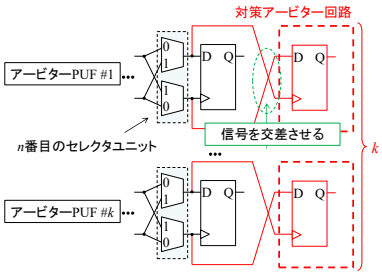
○Physical Unclonable Function（PUF）とは？

半導体製造時のばらつきを固有 ID として抽出し，チャレンジ（入力）に対してレスポンス（出力）を返す関数で指紋に相当

回路パターンが全てコピーされた場合でも，本物と偽物の判別が可能

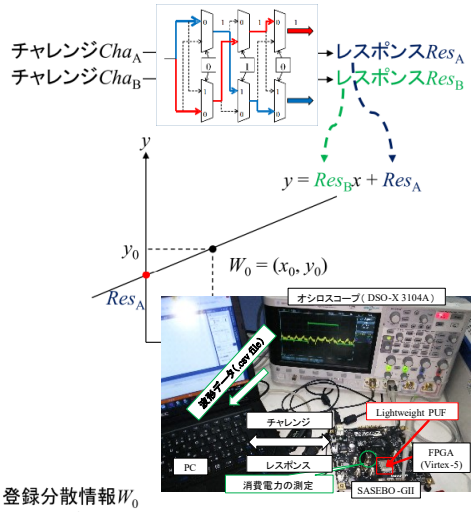
○耐タンパ Lightweight PUF

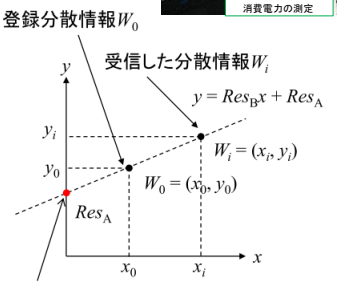
消費電力を均一化することでサイドチャネル攻撃耐性を強化



○秘密分散法をベースとした PUF 認証システム

秘密分散法を用いた ID 生成手法により，人工知能的アプローチによる不正攻撃からの耐性を向上





PUF レスポンスを秘密情報として分散情報を生成
↓
その分散情報を認証に利用

関連情報（図・表・写真等）

適用可能製品

技術シーズ保有者	氏名 所属・役職	吉川　雅弥　教授 名城大学　情報工学部　情報工学科
技術シーズ照会先	窓口 TEL/FAX e-mail	名城大学　学術研究支援センター TEL 052-838-2036　FAX 052-833-7200 sangaku@ccml.meijo-u.ac.jp

■知 的 財 産

■試作品状況　無　提示可　提供可

作成日 2023 年　2 月　10 日