戦略的創造研究推進事業　CREST
研究領域「ディペンダブル VLSI システムの基盤技術」
研究課題「耐タンパディペンダブル VLSI システムの
開発・評価」

研究終了報告書

研究期間　平成21年10月～平成27年3月

研究代表者：藤野　毅
（立命館大学　理工学部　教授）

§1 研究実施の概要

（1）実施概要

交通・流通系で急速に普及した非接触 IC カードなどに見られるように，LSI を利用した金銭情報や個人情報を保管するシステムが社会基盤として広く普及している．このような IC カード上の LSI（以降セキュリティ LSI と記す）のディペンダビリティを向上させるためには，IC カード上の機密情報への悪意ある攻撃に対する対策を施さなければならない．

本研究では，動作時の消費電力や電磁波などの漏えい情報を解析するサイドチャネル攻撃，LSI にスパイクノイズ等を印加して誤動作を誘起することで機密情報を窃取するフォールト攻撃，パッケージを開封し，内部を直接観測・改造する侵襲攻撃，さらに，偽造 LSI の製造に対する防御方法を備えた，耐タンパ LSI を実現するための技術開発を，3項目に分類して実施し，以下の研究成果を得た．成果の内容は§4に記載をおこなっている．

（1）耐タンパ性 LSI 設計プラットフォーム

物理解析攻撃に対する，耐タンパ性を有する LSI の設計指針を提示し， LSI を容易かつ低コストで設計・製造するための設計プラットフォームを提供する．

4．1 HMDR-ROM を用いた耐タンパ共通鍵暗号回路設計方式（立命館大グループ）

4．2 MDR-ROM を用いた PUF と耐タンパ AES 暗号回路の統合アーキテクチャ（立命館大グループ）

4．3 非同期ランダムクロックによる簡易攻撃耐性改善手法（名城大グループ）

4．4 設計段階での脆弱性の簡易評価手法（名城大グループ）

4．5 設計段階での脆弱箇所の解析手法（名城大グループ）

4．6 設計段階での実機攻撃耐性予測手法（名城大グループ）

（2）耐タンパ性能評価プラットフォーム

セキュリティ LSI の耐タンパ性能を評価する指針を提示するとともに，上記の様々な物理解析攻撃実験用の LSI ボードを開発し，評価試験環境を構築する．

4．7 暗号モジュールの安全性評価環境の構築と国際標準化活動 （産総研グループ）

4．8 車載セキュリティーへの暗号回路の適用とサイドチャネル攻撃（立命館大グループ）

4．9 公開鍵暗号の厳密な実装安全性評価技術 （三菱電機グループ）

4．10 電磁波解析における厳密な実装安全性評価技術の開発（三菱電機グループ）

4．11 FSA シミュレータの開発 （三菱電機グループ）

4．12 フォールト攻撃評価システムの開発（三菱電機，名城大グループ）

（3）偽造 LSI を識別する PUF を用いたセキュリティシステム

IC カードなどの偽造複製防止対策として，各 LSI に固有の物理特性の差異を識別する PUF（Physical Unclonable Function）の回路設計・開発を行うとともに，PUF と暗号技術を融合した新しいセキュリティシステムの提案を行う．

4．13 遅延時間差検出アービターPUF と Fuzzy Extractor を用いた誤り訂正回路（立命館大グループ）

4．14 PUF の構成に関する提案（名城大グループ）

4．15 高効率な PUF および鍵生成方式の開発と PUF の定量的性能評価手法（産総研グループ）

4．16 新型 PUF および誤り訂正技術を用いた秘密鍵生成回路（三菱電機グループ）

4．17 暗号回路と PUF を用いた耐タンパキーレスエントリーデモシステム（立命館大学，三菱電機）

上記，耐タンパ性 LSI 設計プラットフォームで設計・試作された暗号回路は，耐タンパ性能評価プラットフォームによって評価され高い安全性が確かめられた．さらに，耐タンパ性 LSI 設計プラットフォームで設計した暗号回路の鍵を PUF 技術を用いて安全に格納できるセキュリティーシステムを構築し，キーレスエントリーシステムを模したデモンストレーションをおこなった．本研究で開発した技術は，従来の IC カード分野での応用だけでなく，ネットワークと接続される自動

運転車やセンサーネットワーク等のセキュリティー向上に貢献できる.

(2)顕著な成果

＜優れた基礎研究としての成果＞

1. サイドチャネル攻撃が一般 LSI においても実際の脅威であることの実証研究

概要:(200 字程度)

本プロジェクト開始時には, 一般的な LSI 業界においては, サイドチャネル攻撃はあまり知られておらず,「暗号回路以外の回路ノイズで攻撃は成功しない」,「キャパシタを入れれば電力解析攻撃の対策になる」,「電磁シールドを入れれば電磁波攻撃の対策になる」,「微細化が進むとリーク電流が大きくなるので攻撃が困難」, 等漠然と考えられてきた. 本プロジェクトでは, これらすべての仮説に対して実証実験を行い, 攻撃を成功させることで危険性を論文で示した. また, わかりやすい脅威事例として, 車載 OS が動作し, CAN の暗号通信をおこなっている ECU でもサイドチャネル攻撃が成功することを実証した.

2. 微細電磁波プローブによる LSI 構成部品の安全性評価研究

概要:(200 字程度)

本プロジェクト開始時には, 電磁波を利用したサイドチャネル攻撃は, 攻撃可能であるという研究発表はされていたが, 電力解析攻撃と同じような情報が得られると漠然と考えられていた. メモリのワード線位置やスタンダードセル内部の非線形ゲートの振る舞いが, 微小電磁波プローブを用いて観察可能であるとの実験結果を 2013 年の CHES(採択率 30%以下)で学会発表した. 本学会は従来安全と考えられていた LSI 構成部品に脆弱性が内在することを始めて示したものであり, IC カード関連のサイドチャネル攻撃の専門家の間で大きく評価され, 暗号ジャーナルでも invite され掲載された.

3. 各種新型 PUF 技術の発明と安定動作実証の研究

概要:(200 字程度)

PUF(Physical Unclonable Function)とは LSI のチップ製造時のばらつきを利用してチップ固有の ID を発生する技術であり, 本プロジェクト開始の数年前に発表された新しい技術である. 本プロジェクトでは. アービターPUF などの既存の PUF を試作し, 安定性・ユニーク性や攻撃脆弱性等の問題点を抽出した. これらの知見を元に, 遅延時間差検出型アービター PUF, グリッジ PUF, Pseudo-LFSR PUF, 改良リングオシレータ PUF, MDR-ROMPUF などの新しい PUF の提案と実装をおこない, 実際に安定して動作することを実証した.

＜科学技術イノベーションに大きく寄与する成果＞

1. 耐タンパ性 LSI 設計プラットフォーム HMDR-ROM 方式の研究

概要:(200 字程度)

本プロジェクト開始前に学会等で提案されていた既存の対策手法は, 汎用 LSI ツールで設計するとサイドチャネル情報がリークし, また回路面積や消費電力が非常に大きくなる問題を抱えていた. 提案した HMDR(Hybrid Masked Dual Rail)-ROM 方式ではサイドチャネル攻撃リーク元源である SBox 回路に MDR-ROM マクロを使うことで, 標準設計 CAD フローで設計しても, 高いサイドチャネル攻撃耐性が実現できる. また, ROM を使用していることで他方式と比べて小面積かつ低消費電力が達成できる. MDR-ROM は日米で特許が成立.

2. 耐タンパ性能評価プラットフォーム SASEBO ボードの展開

概要:(200 字程度)

暗号 LSI を統一的に評価できる標準ボードとして, 本プロジェクトに先行して産総研により,

SASEBO(Side-channel Attack Standard Evaluation BOard)の開発が行われてきた. CREST プロジェクトでは本ボードを発展させ, 各種 ASIC 仕様にカスタマイズできる RII, 最先端 FPGA(28nm)を使用した GIII, 教育用の ZUIHO, IC カード形状の MiMICC の4種類のボードを開発し, 成果を民間企業に移転した. SASEBO 用の攻撃ソフトウエアも, 実際に AES 暗号回路の評価を進めながら改良を進め, 耐タンパ LSI 設計プラットフォームの開発に大きく貢献した.

3. PUF による安全な鍵保管をおこなうセキュリティーシステム

概要:(200 字程度)

PUF は LSI 個別の ID を生成することができ, かつこの情報は不揮発性メモリ等に書き込まれないことから耐タンパ性が高く, 複製防止などのセキュリティー強化技術として使用できる. ただし, PUF が生成した ID は温度・電圧などの環境変化で変動しやすいため, そのままでは暗号鍵として使用することはできない. ファジーエクストラクタという誤り訂正符号技術を用いて PUF が生成した ID から暗号鍵を生成し, その暗号鍵を用いて認証用の鍵を暗号化して不揮発性メモリに保管するセキュリティー認証システムを実現した. 車載キーレスエントリーシステムとしてデモ動作を実証・展示した.

§2. 研究構想

(1)当初の研究構想、課題設定

① 本研究の背景、社会や産業に存在する問題と本研究の課題設定

交通・流通系で急速に普及した非接触 IC カードなどに見られるように, LSI を利用した金銭情報や個人情報を保管するシステムが社会基盤として広く普及している. このような IC カード上の LSI (以降セキュリティ LSI と記す)に保管されている機密情報や個人情報が窃取される, あるいは LSI 複製によるカード偽造などが発生すると, 大きな社会的混乱を引き起こす可能性があり, このような攻撃に対して, 情報の防御システムを LSI 上で構成する研究が必要とされている.

セキュリティ LSI への主な物理的解析・攻撃手法としては, 動作時の消費電力や電磁波などの漏えい情報を解析するサイドチャネル攻撃, LSI にスパイクノイズ等を印加して誤動作を誘起することで機密情報を窃取するフォールト攻撃, パッケージを開封し, 内部を直接観測・改造する侵襲攻撃などが挙げられる. さらに, 機密情報の窃取にとどまらず, 回路パターンを解析複製した偽造 LSI の製造と悪用など, さまざまな脅威が存在する. 耐タンパ性を指向したディペンダブル VLSI システム実現のためにはこれらの攻撃への対策が不可欠である.

②本研究チームの達成目標。

本研究では, 機密情報の観点でディペンダブルなセキュリティ LSI すなわち, 上記 3 種の物理攻撃と偽造 LSI の製造に対する防御方法を備えた, 耐タンパ LSI を実現するための技術開発を行い, 以下3つの成果物を得ることを目標とする.

(1)耐タンパ性 LSI 設計プラットフォーム

物理解析攻撃に対する, 耐タンパ性を有する LSI の設計指針を提示し, LSI を容易かつ低コストで設計・製造するための設計プラットフォームを提供する. 具体的な目標は以下の通りである.

(i)128bitAES 暗号回路の同一の HDL 記述から, 通常 ASIC フローとほぼ同等の設計・検証時間でレイアウト設計できる耐タンパ LSI 設計環境を整備する.

(ii)未対策 LSI が1万回程度の波形取得攻撃で 128bit の暗号鍵をすべて特定可能な攻撃環境で, 対策 LSI は 100 万回の測定を行っても 64bit 以下の鍵特定しかできないことを確認する.

(2)耐タンパ性能評価プラットフォーム

セキュリティ LSI の耐タンパ性能を評価する指針を提示するとともに，上記の様々な物理解析攻撃実験用の LSI ボードを開発し，評価試験環境を構築する．具体的な目標は以下の通りである．

(i)攻撃用異常電源電圧およびクロックを供給する機能の評価ボードへの追加とレイアウトデータが明らかな攻撃検証チップを作成し，それを用いて様々なフォールト攻撃手法と侵襲攻撃手法の評価実験を行いその有効性を検討する．

(ii)未対策 AES 暗号回路に対して，輻射電磁波を用いた差分電磁波解析（DEMA）において，差分電力解析（DPA）と同等の波形取得数で暗号鍵特定が可能な攻撃環境を構築する．

(3)偽造 LSI を識別する PUF を用いたセキュリティシステム

IC カードなどの偽造複製防止対策として，各 LSI に固有の物理特性の差異を識別する PUF（Physical Unclonable Function）の回路設計・開発を行うとともに，PUF と暗号技術を融合した新しいセキュリティシステムの提案を行う．具体的な目標は以下の通りである．

(i)固有 ID を発生させる PUF 回路として，従来手法を含めた様々な回路方式の検討を行い，チップを試作し，実用化にむけて各方式の環境変化（電圧・温度），経時変化による固有 ID 値の揺らぎの差異を評価する．

(ii)PUF により生成された固有 ID と公開鍵暗号による電子署名を組み合わせた IC カード複製防止セキュリティシステムの提案を行い，プロトタイプシステムを構築する．

③本研究の特徴

(1)耐タンパ性 LSI 設計プラットフォーム

消費電力を利用したサイドチャネル攻撃に対する耐タンパ性を実現するためには，回路を構成する AND や OR 等のプリミティブゲートが，入力値に依存せず均一の電力を消費するようにするという，プリミティブゲートレベルの対策が，どのような暗号アルゴリズムに対しても適用可能であるため，汎用性が高い．このプリミティブゲートレベルの対策として，立命館大学で提案しているドミノ RSL 方式を耐タンパ LSI 設計技術の中心技術として，本方式を用いた各種暗号回路の実装を行い，提案方式の耐タンパ性の実チップを用いた実証をおこなう．また，このドミノ RSL 技術を用いた LSI 設計技術を，各種暗号回路に容易に適用するための LSI 設計技術および耐タンパ性検証技術の開発をおこなう．最終的には，他機関で提案されている2線式相補動作ゲートなどプリミティブゲートレベルの対策に対して，ドミノ RSL 技術の優位性のベンチマークをおこなう．

(2)耐タンパ性能評価プラットフォーム

様々な実験を通してセキュリティ LSI の耐タンパ性能評価の指針を策定し，国際標準規格化を進めるためには，第三者が同じ環境で実験の検証や評価手法の有効性を検証できる標準のハードウェア・プラットフォームの開発が不可欠である．そこで，産総研では平成 18-20 年度に経済産業省の委託事業の中で，SASEBO(Side-channel Attack Standard Evaluation BOard)の開発を行い，国内外の研究期間での利用を促進してきた．そこでは SASEBO はあくまで研究用のプロトタイプボードとしての位置付けであったが，多くの研究者が利用できる標準の評価環境としてさらなる普及を図るために，企業の協力のもと製品化を進めるとともに，そのボードを用いた計測環境の整備や解析ツールの開発を行う．さらに，自ら行った様々な実験の成果や知見を，論文学会発表だけでなく Web で公開して行く．

(3)偽造 LSI を識別する PUF を用いたセキュリティシステム

IC カードなどの偽造複製防止対策として，各 LSI に固有の物理特性の差異を識別する PUF

(Physically Unclonable Function)の回路設計・開発を行う. 半導体を用いたPUFとしては, 等価な2経路間の遅延時間差のばらつきを利用する「アービターPUF」(米国 Verayo 社)およびメモリなどデータをラッチする回路の電源投入時のばらつきを利用する「SRAM PUF」(オランダ Intrinsic-ID 社:フィリップスからのスピンアウト)が 2008 年から商品化を開始しているが, 具体的な回路の設計手法や, 発生されるIDのユニーク性(同一のIDが発生しないことの保証), IDの安定性(測定環境の変化や経年劣化に対する保証)などの定量化が発表されておらず, 技術的にはいまだ未成熟であると考えられる.

アービターPUF 回路をリファレンス技術としてとらえ, 主としてFPGAを用いて実装し, PUF が満足すべき評価手法・指標を確立する. また, 従来型のアービターPUF 回路のテストチップを試作し, 回路の設計パラメータ(マルチプレクサ段数)と ID のユニーク性および測定環境安定性の関連を評価する. これらの検討結果を踏まえて, ID のユニーク性および測定環境安定性を向上させる, 改良アービターPUF 回路および新型 PUF 回路設計技術を新たに提案し, 従来型のアービターPUF に対する技術優位性を実証する.

さらに, PUF 回路のユニークな ID を暗号技術と組み合わせ, LSI 毎にユニークな暗号鍵を生成することで, 偽造が極めて困難な IC カードシステムや, FPGA のビットストリームを個別に暗号化して保護する等, セキュリティシステムのプロトタイプを構築し, その有効性を検証する.

④研究実施方法

1) 本研究チーム運営の方針、研究グループ間の分担・協力関係

下図に示すように, 各グループの得意とする技術分野をそれぞれ担当することで, 本研究の目的である, (1)耐タンパ性 LSI 設計プラットフォーム(2)耐タンパ性能評価プラットフォーム(3)偽造LSIを識別するPUFを用いたセキュリティシステムを実現する. (1)に対しては, 耐タンパLSI設計方式の技術開発とチップ実装を立命館大学が行い, 耐タンパ性の検証などの設計 CAD 構築を名城大学で行う. (2)に関しては, プラットフォームの構築を産総研が行い, この攻撃プラットフォームを使用して(1)で設計した耐タンパ LSI の評価実験を立命館大学で行う. (3)に関しては, PUF の設計方式検討およびPUFを用いたセキュリティシステム構築を三菱電機および産総研が行い立命館大学 PUF チップの LSI 実装と PUF 単体での特性評価を行う.

2) 領域外部の企業等との連携

本事業でサイドチャネル攻撃やPUF等の様々な実験に利用しているFPGAボードSASEBO-GIIは, 東京エレクトロンデバイス株式会社に製造を依頼しており, 本 22 年度に正式に製品化を行った. 今後も, 本研究成果を同社から教育用ツール等へ展開していく予定である.

(2)新たに追加・修正など変更した研究構想、発展テーマ

① 中間評価で受けた指摘や助言、それを踏まえて対応した結果について

A. LSI の設計時に電力差分解析を用いたサイドチャネル攻撃に対する耐タンパ性を検証できる, 耐タンパ検証 CAD システムを構築する. (領域会議コメントに基づき, H23 年度より追加)

B. AES 暗号回路などの暗号モジュールレベルの耐タンパ性の検証だけでなく, セキュア SoC 上には, CPU やバス, メモリ等の機密情報を扱う回路が存在し, これら回路のサイドチャネル攻撃に対する脆弱性の評価をおこなうことが必要である. オープンソースの CPU 等を用いて, システムレベルのサイドチャネル評価をおこなうことのできる LSI の試作と耐タンパ性評価環境構築を行う. (H23 年度三菱電機参加により発展テーマとして追加)

§3 研究実施体制

(1)研究チームの体制について

① 「立命館大学」グループ
研究参加者

	氏名	所属	役職	参加時期
○	藤野 毅	立命館大学理工学部	教授	H21.10～
	久保 博嗣	同上	同上	H24.10～
	冨山 宏之	同上	同上	H26. 4～
	熊木 武志	同上	任期制講師	H22 .4～
*	汐崎 充	立命館大学 総合科学技術研究機構	専門研究員	H22 .4～
*	浅川 俊介	同上	研究補助員	H21.10～
*	久保田 貴也	同上	研究員	H24 .4～
	竹内 章浩	立命館大学 理工学研究科	M2	H24 .7～
	堤 大樹	同上	M2	H24 .7～
	中井 綱人	同上	M2	H24 .7～
	西村 隆志	同上	M2	H24 .7～
	中野 将志	同上	M1	H25 .7～
	北村 俊樹	同上	M1	H25 .7～
	田中 将貴	立命館大学理工学部	B4	H26 .7～
	福野 貴仁	同上	B4	H26 .7～
	福水 洋平	同上	(旧)助教	H21 .10～ H22. 3
*	Hoang Ahn Tuan	同上	(旧)助手	H21 .10～ H22. 3
	福井 正博	同上	教授	H21 .10～ H23. 3
	小島 憲司	立命館大学 理工学研究科	(旧)M2	H21 .10～ H23. 3
	黒川 悠一朗	同上	(旧)M2	H22. 4～H23. 3
	岩井 克彦	同上	(旧)M2	H22. 4～H24. 3
	古橋 康太	同上	(旧)M2	H22. 4～H24. 3
	吉川 弘起	同上	(旧)M2	H22. 7～H24. 3
	佐野 真規	同上	(旧)M1	H22. 4～H23. 9
	穂積 康平	同上	(旧)B4	H23.12～ H24. 3
	奥山 一樹	同上	(旧)M2	H21.10～ H22. 3
	山田 翔太	同上	(旧)M2	H21.10～ H22. 3
*	Hoang Ahn Tuan	立命館大学 総合科学技術研究機構	ポスドク研究員	H22. 5～ H24.10
	伊藤 弘樹	立命館大学	(旧)M2	H22. 4～H25. 3

		理工学研究科		
	岡本　卓朗	同上	(旧)M2	H22. 7～H25. 3
	小川　昂佑	同上	(旧)M2	H22. 7～H25. 3
	橋本　祐樹	同上	(旧)M2	H22. 7～H25. 3
	濱崎　慎也	同上	(旧)M2	H22. 7～H25. 3
	村山　貴彦	同上	(旧)M2	H22. 7～H25. 3
	望月　陽平	同上	(旧)M2	H22. 4～H25. 3
	村上　佑馬	同上	(旧)M2	H22. 4～H25. 3
	菅谷　周平	同上	(旧)M2	H23.12～ H26. 3
	柴谷　恵	同上	(旧)M2	H23.12～ H26. 3
	鵜飼　慎太郎	同上	(旧)M2	H23.12～ H26. 3
	谷口　雅人	同上	(旧)M2	H23.12～ H26. 3
	板屋　修平	同上	(旧)M2	H24. 4～H26. 3
	本多　隼也	同上	(旧)M2	H24. 4～H26. 3
	堀　遼平	同上	D2	H22. 4～H26. 3

研究項目
- 電力・電磁波を利用したサイドチャネル攻撃に対する対タンパ LSI 設計手法の研究
- 耐タンパ性 LSI マクロの回路設計
- PUF デバイス回路実装と特性評価およびモデル化

② 「産総研」グループ
研究参加者

	氏名	所属	役職	参加時期
○	堀　洋平	(独)産業技術総合研究所	主任研究員	H22 . 4～
	坂根　広史	同上	主任研究員	H21 .10～
	片下　敏宏	同上	主任研究員	H21 .10～
*	藤原　充	同上	テクニカルスタッフ	H26. 4～
*	恩田　泰則	同上	テクニカルスタッフ	H26. 7～
*	伊藤　剛	同上	研究補助員	H26.12～
	佐藤　証	同上	チーム長	H21.10～ H24. 3
*	姜　玄浩	同上	ポスドク研究員	H22. 9～H25. 3
*	佐々木 明彦	同上	技術員	H22.12～ H25. 5
*	飯島 賢吾	同上	テクニカルスタッフ	H25. 6～H26. 3
*	久保田　貴也	同上	技術員	H22. 4～H24. 3
*	佐藤　弘季	中央大学　理工学研究科	M1	H22. 9～H23. 3
*	野口　正俊	中央大学　理工学研究科	M2	H22. 9～H23. 3

研究項目
- サイドチャネル攻撃・フォールト攻撃用プラットフォーム開発
- 防御手法・解析手法の開発および有効性検証
- PUF の実装および測定

・ PUF と暗号技術を融合したセキュリティシステムの構築

③ [三菱電機」グループ
研究参加者

	氏名	所属	役職	参加時期
○	鈴木 大輔	三菱電機株式会社 情報技術総合研究所 情報セキュリティ技術部	主席研究員	H23. 4～
	佐伯 稔	同上	主席研究員	H23. 4～
	清水 孝一	同上	研究員	H23. 4～
	菅原 健	同上	研究員	H23.12～
	粕谷 智巳	同上	(旧)主席研究員	H23. 4～H25. 3

研究項目
・SoC に対する包括的なサイドチャネル評価・対策技術開発
・PUFを用いたSoCのセキュア化技術開発
・セキュア SoC の構築とセキュリティシステムへの応用

④ 「名城大学」グループ
研究参加者

	氏名	所属	役職	参加時期
○	吉川 雅弥	名城大学理工学部	教授	H21.10～
	旭 健作	同上	助教	H26. 2～
*	浅井 稔也	同上	研究技術員	H22. 5～
	杉岡 恭太	名城大学大学院	M2	H25. 4～
	野崎 佑典	同上	M1	H26. 4～
	松久 僚真	同上	M1	H26. 4～
	野原 康平	同上	M1	H26. 4～
	成瀬 郷	同上	M2	H21.10～ H23. 3
	勝部 真人	同上	M2	H21.10～ H24. 3
*	小野みどり	名城大学理工学部	研究補助員	H23. 4～ H24.10
	吉田 将之	名城大学大学院	M1	H24. 4～ H24.10
	佐藤 隆亮	同上	M2	H23. 4～H25. 3
	松島 大祐	同上	M2	H23. 4～H25. 3
	後藤 輝	同上	M2	H24. 4～H26. 3
	塚平 峻矢	同上	M2	H24. 4～H26. 3

研究項目
・ プログラマブル LSI を指向した配線アーキテクチャと遅延モデルの開発と評価
・ 耐タンパ性を考慮するためのレイアウト制約の開発
・ 耐タンパドリブン CAD システムの構築

⑤「中央大学」グループ ※H22.8 をもって産総研グループへ統合
研究参加者

	氏名	所属	役職	参加時期
○	吉田　隆弘	中央大学　研究開発機構	専任研究員/ 機構助教	H22. 4～H22. 8
	今井　秀樹	中央大学　理工学研究科	教授	H21.10～ H22. 8
*	姜　玄浩	中央大学　研究開発機構	専任研究員/ 機構助教	H22. 4～H22. 8
*	野口　正俊	中央大学　理工学研究科	(旧)M2	H21.10～ H22. 8
*	佐藤　弘季	同上	(旧)M1	H22. 4～H22. 8
	堀　洋平	中央大学　研究開発機構	専任研究員/ 機構助教	H21.10～ H22. 3

研究項目

- 暗号モジュールのフォールト攻撃に対する安全性評価
- フォールト攻撃の対策技術の開発・有効性評価
- サイドチャネル情報に基づく新攻撃手法に関する研究
- PUF の評価とプロトタイプの開発

(2)国内外の研究者や産業界等との連携によるネットワーク形成の状況について

A. 情報処理推進機構(IPA)

IPA は IC カードのセキュリティー評価技術の認定機関であり，高精度のサイドチャネル攻撃ツール(高精度電磁波プローブ)や，レーザーや電磁波を用いたフォルト攻撃の設備を有している．平成26年度からは，立命館大学で試作した LSI の評価のために，定期的に訪問実験をおこなってきた．この関連で，逆に IPA 側からは評価 LSI の開発の協力依頼を受けている．

B. 名古屋大学　組込みシステム研究センター （高田研究室）

名古屋大学高田研究室を中心とする組込みシステム研究センターは，車載組込みOSの開発を産業界と密接に協力しておこなっている．次世代の AUTOSAR 仕様の OS にセキュリティー機能を実装する取り組みに関して，ハードウエア設計側としての協力をすすめている．高田研究室の本田准教授の指導のもと，ヴィッツ株式会社と三菱電機の協力を得て，AES 暗号回路を実装した FPGA ボードで車載通信(CAN)通信をおこなうシステムをくみ上げた．現在立命館大学・名城大学の学生が名古屋大学の組込みシステム教育プログラムのもとで，車載セキュリティー応用の教育・研究を進めている．

§4 研究実施内容及び成果

【A・耐タンパ性LSI設計プラットフォーム】

4．1 HMDR-ROM を用いた耐タンパ共通鍵暗号回路設計方式（立命館大グループ）

① 実施内容

サイドチャネル攻撃の主なターゲットとなる非線形回路部を提案した IO-Masked Dual-Rail ROM (MDR-ROM)に置き換え，MDR-ROM 以外の回路の消費電力相関を隠蔽するための乱数発生回路を追加するだけで，小面積且つ低消費電力な耐タンパ LSI が設計できる方式である．共通鍵暗号である AES 暗号の GF(2^8)逆元演算を MDR-ROM で実現し，我々の研究グループが新たに発見した Geometric Leak （漏洩電磁波から EM プローブとメモリ内のワード線との距離情報リーク）への対策として乗算マスクを適用したサイドチャネル攻撃対策 AES 暗号回路(Hybrid MDR-ROM AES ： HMDR-ROM AES)を 180nm CMOS プロセスで試作し，耐性評価を行った．

② 創造性

既存の対策手法は汎用ツールで設計するとサイドチャネル情報がリークする，回路面積や消費電力が非常に大きくなる問題を抱えていた．提案した HMDR-ROM 方式では SRAM マクロを使った標準設計 CAD フローで実装できる．また，ROM を使用することでサイドチャネル攻撃対策が小面積且つ低消費電力が達成できる．また，Geometric Leak に注目した世界初の対策手法である．

③ 有用性

サイドチャネル攻撃（電力解析攻撃と電磁波解析攻撃）を実施するために 100 万波形それぞれ取得した．よく知られた既存の対策手法との耐性評価を行った結果を図 4.1 に示す．Threshold Implementation (TI)方式以外のよく知られている既存対策が 40 万波形以内に全ての暗号鍵が窃取できているのに対して，本方式は 100 万波形で1Byte の鍵も窃取できず，高いサイドチャネル攻撃耐性が実現できることを示した．

④ 優位比較

既存の対策手法との回路面積と消費電力を比較した結果を図 4.2 に示す．各結果は未対策 AES 暗号回路の回路面積と消費電力で正規化している．図 4.1 より本方式が高いサイドチャネル攻撃耐性を達成し，サイドチャネル攻撃対策 AES の中で最も小面積且つ低消費電力が実現できていることがわかる．

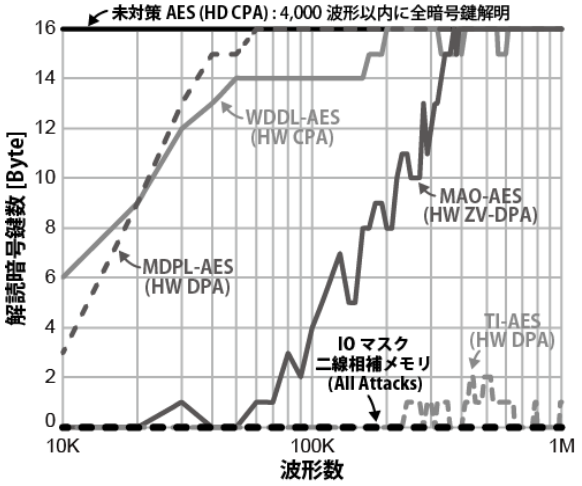


図 4.1 サイドチャネル攻撃耐性評価結果

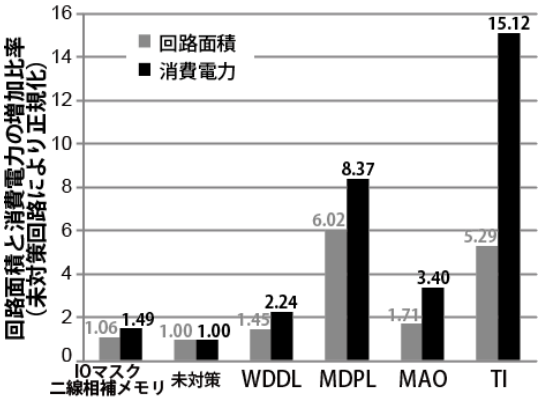


図 4.2 回路面積・消費電力比較

4．2 MDR-ROM を用いた PUF と耐タンパ AES 暗号回路の統合アーキテクチャ（立命館大グループ）

① 実施内容

サイドチャネル攻撃対策手法として，どのような入力値に対しても消費電力が一定になる MDR-ROM を用いる手法を提案，AES 暗号回路への適用を行ってきた．そして，我々の提案する耐タンパ認証システムには PUF も必要不可欠な技術であることを示してきた．立命大では面積ペナルティ無しに MDR-ROM が PUF としても機能する新たな回路技術の検討を行った．

② 創造性

サイドチャネル攻撃対策と PUF の両技術が必要である場合，サイドチャネル攻撃対策を施した共通鍵暗号回路と DTM PUF 回路がそれぞれ実装する必要であり，回路面積が増加する．MDR-ROM から PUF レスポンスも出力できるようにすることで，ASIC の標準設計 CAD フローで実装可能という特長をそのままに，MDR-ROM を使うだけでサイドチャネル攻撃対策を施した暗号回路の実現と，秘密情報の物理解析攻撃から守る PUF 技術の実現ができる．

③ 有用性

図 4.3 に示す AES と PUF の統合回路を 180nm CMOS プロセスで試作し，AES 暗号回路のサイドチャネル攻撃耐性と PUF の性能評価を行った．サイドチャネル攻撃耐性は図 4.1 で示した攻撃結果と同じ結果が得られ，十分な攻撃耐性が得られていることを確認した．PUF の性能評価は図 4.4 に示す結果となり，チップ毎にユニークな ID が生成できていることを確認した．

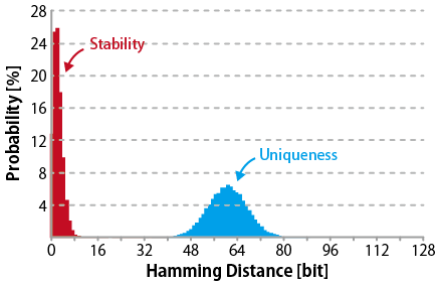


図 4.4 MDR-ROM を用いた PUF の性能評価結果

④ 優位比較

180nmCMOS プロセスを用いて，MDR-ROM を用いてサイドチャネル攻撃対策 AES と PUF を統合した回路の試作を行った．PUF レスポンスの平均ビット反転確率は 1.64%であり，Arbiter-PUF(128 段 Arbiter-PUF の平均ビット反転確率：8%)よりも安定したレスポンスが得られることがわかった．AES と PUF の統合回路の面積は 710,000μm² で，未対策 AES 暗号回路（710,000μm²）と殆ど同じ回路面積で実現できることがわかった．

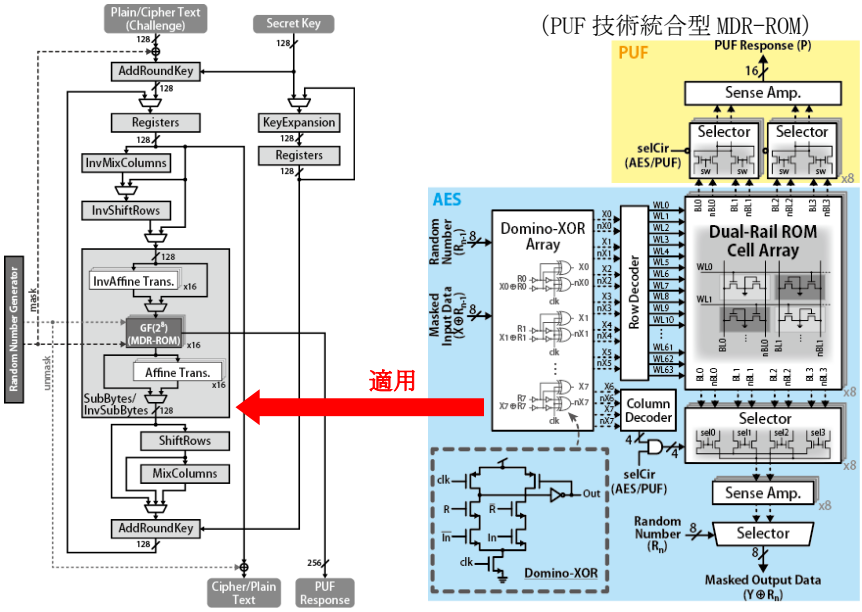


図 4.3 サイドチャネル攻撃対策と PUF を統合した MDR-ROM を用いた AES 暗号回路

4．3 非同期ランダムクロックによる簡易攻撃耐性改善手法（名城大グループ）

①実施方法・実施内容

本手法は，サイドチャネル攻撃に対する耐性を向上させるためのクロック供給側での対策手法である．内蔵リングオシレータから出力されるクロックにより暗号回路を駆動し，そのクロックの周期をランダムに可変させたり，データバスのビット間スキューを故意に発生させる．これにより，電力・電磁波リーク成分が時間的に分散し，攻撃時の統計処理の効率が著しく低下するため，攻撃耐性が改善される．クロック周期の変動は，暗号処理間，暗号処理内のクロック間，の双方で発生させる．図 4.5 に試作チップで観測したクロック周期の変動の様子を示す．また，暗号処理回路のクロック信号ラインはデバイス外部からは隠蔽されている為，外部からのクロック操作及びクロック位相の推定が困難である．

②創造性

クロック周期のランダム化に加え，システムクロックとの二重化＆非同期動作，内部クロック間スキューの付加により，対策パーツを組み合わせて適用することができる．アライメント攻撃に対しても耐性を高められるよう，ランダム化の程度を設定により調節することができる．

③有用性

暗号回路そのもののサイドチャネル攻撃対策と併用することが可能であり，クロック系のみの変更により，簡易的に耐性を向上させることができる．暗号処理クロックによる波形への影響が，LSI の IO を定義するシステムクロックによる影響より小さく，かつ非同期であるため，内部の暗号処理タイミングの特定を困難にし，攻撃耐性を改善できる．さらに，暗号処理用のクロック発振回路の隠蔽により，クロック操作を用いたフォールト攻撃を防止する．レーザーによるフォールト注入に対しても，タイミングの特定が困難であるため，耐性が高まることが期待できる．

④優位比較

周波数変動やダミーディレイ挿入などによる時間軸上の攪乱により耐性を向上させる提案は従来も存在したが，本研究ではスキューを付加したり，周期変動についても耐性とスループットを考慮し，変動の程度を調節可能とした．

また，クロックフォールトの対策として内蔵 PLL を用いて暗号処理クロックを生成する方法があるが，PLL の場合，外部クロックとロック関係にある点で内部クロックを推測される危険性がある．本研究の場合は完全な非同期であるため，より推定が困難である．

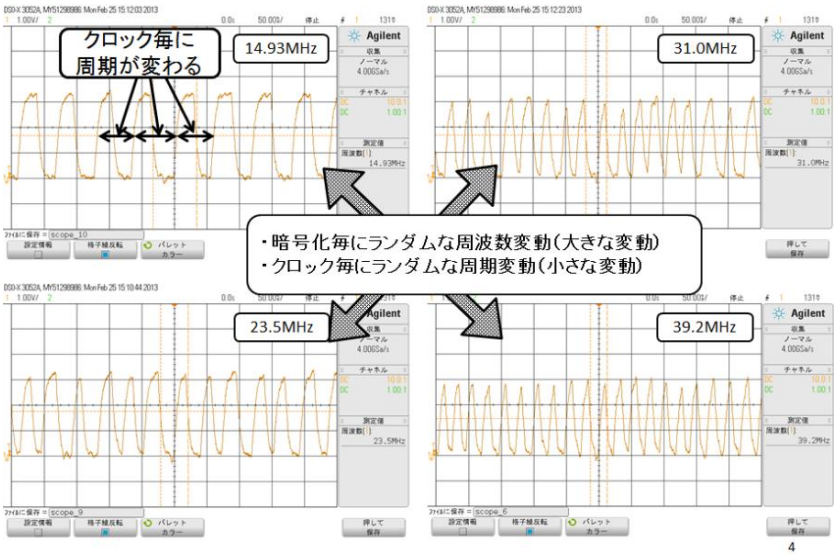


図 4.5 ランダムクロックの観測結果

4．4　設計段階での脆弱性の簡易評価手法（名城大グループ）

①実施方法・実施内容

暗号ハードウェアの電力解析攻撃耐性を設計段階で簡易的に評価するための手法である．従来のように攻撃シミュレーションで安全性を判定するのではなく，攻撃対象回路が消費電力に及ぼす影響について，どの箇所からのリーク（秘密鍵に関連する情報）が多いかを多重線形回帰により評価する．暗号回路内の秘密鍵関連中間値と消費電力との間に線形相関があると仮定し，複数の要因からの影響の大きさをまとめて算出する．図 4.6 に評価結果の例を示す．本手法では，ビットごとの相関の大小，乱数との相関の有無，などを 1 度の解析で比較評価可能である．また，さらに上流の設計にあたる，暗号処理のアルゴリズムや回路のアーキテクチャを検討する段階での脆弱性評価を想定し，脆弱性が危惧される各モジュールごとに消費電流モデルを作成して暗号処理ソフトウェアに組み込むことで，ソフトウェアで攻撃可能性を検討する手法についても提案した．

一方，消費電流シミュレーション全般に適用可能な検証時間の短縮手法についても提案した．ある平文と暗号文の入出力に伴う電流波形をシミュレーションで求めるにあたり，簡単な仕組みでネットリストを操作し，不要なラウンドをスキップさせることで，攻撃対象ラウンドの波形のみを出力させるシミュレーションが可能となる．図 4.7 にその例を示す．これにより，検証に必要な消費電力波形の取得作業での大幅な時間短縮を実現する．

②創造性

多重線形回帰による脆弱性の評価では，1 度の解析で複数の要因による脆弱性の傾向を評価することができる．個別に脆弱性を評価し比較するのに比べて効率的である．このとき，乱数ビットの影響も一緒に算出することができ，乱数の推定可能性についても評価できる．

また，回帰係数に対して t 検定を使って評価することにより，攻撃に必要な波形数の評価を行うことも可能である．

③有用性

暗号ハードウェア設計工程の早期の段階でサイドチャネル攻撃のリスク評価を行い，対策に結び付けることで，詳細設計前にリスクを軽減できる．

④優位比較

評価ボードを使ってサイドチャネル攻撃実験により評価する方法と比べ，実際の設計データに基づく評価を設計の早期段階に行うことができるので，評価時間や評価環境のコストを抑えることができる．

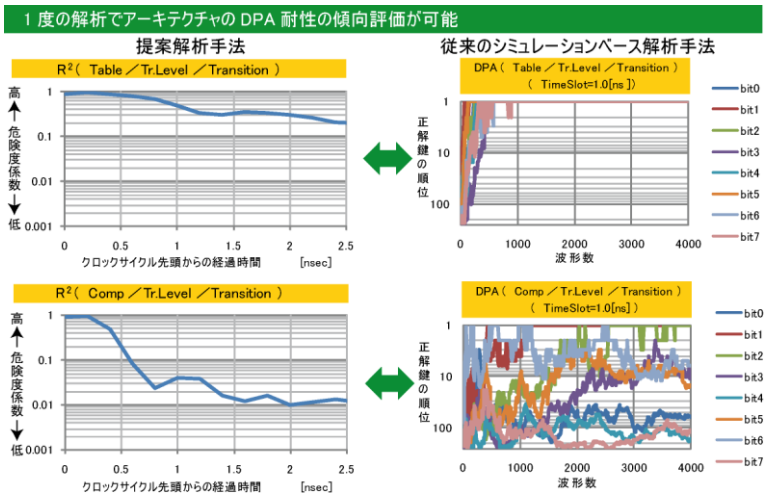


図 4.6　脆弱性の簡易評価

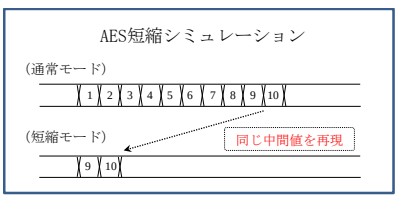


図 4.7 短縮化シミュレーション

4．5 設計段階での脆弱箇所の解析手法（名城大グループ）

①実施方法・実施内容

本手法は，暗号 LSI の設計段階で，攻撃耐性評価を詳細に行うものである．従来の，回路全体の消費電流シミュレーション波形を用いて評価を行う方法に対し，さらに詳細な解析を行うために回路セルごとの消費電流情報を元に評価を行う．このような消費電流情報を用い，図9に示すように暗号回路内の各セルの動作パターンの傾向をクラスタリングによって調べ，その結果を元に攻撃評価を行う．脆弱性が検出された場合，その要因となっている箇所を推定することができる．攻撃が成功したタイミングで動作していた回路セルを特定できるため，要因の絞り込みが可能となる．なお，回路セルごとの消費電流情報は，図 4.8 に示すように，SPICE と Verilog のシミュレーションを組み合わせたイベントモデルシミュレーションの手法によって算出する．

②創造性

回路セルごとの消費電流情報を元に脆弱性を解析することで，詳細な解析を可能としている．具体的には，クラスタリングを用いることで線形相関に限らない広範な脆弱性を探ることができること，また，個々の回路セルの動きを用いた解析であることから，脆弱性が検出されたときにその原因をトレースすることが可能なこと，である．

③有用性

暗号 LSI の設計段階で，サイドチャネル攻撃に対する脆弱性を詳細に評価し，脆弱性があれば，その原因の推定までを行うことができる．

④優位比較

回路セルごとの消費電流情報を使ったクラスタリングにより，従来の攻撃で用いられたハミング重みやハミング距離のような線形相関だけでなく，より複雑な相関の抽出も可能になる．また，攻撃の可否判定のみでなく，その原因を探るヒントを提供できる．

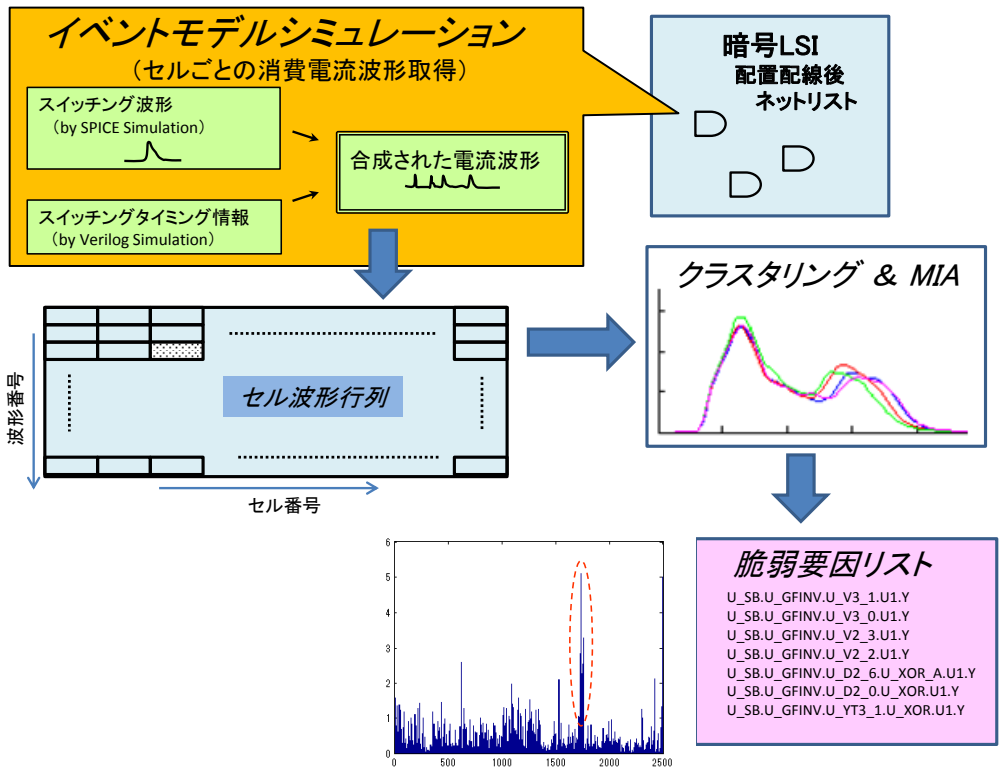


図 4. 8 セルごとの消費電流とクラスタリングを用いた脆弱性評価

4．6 設計段階での実機攻撃耐性予測手法（名城大グループ）

①実施方法・実施内容

電力・電磁波解析攻撃の対象となる基板上で，リーク源である暗号 LSI 内部での電流波形と実際にオシロスコープで観測される波形は異なる．ここで，設計段階で，後に暗号LSIを実機上で動作させたときの脆弱性がどの程度になるかの見積もりができることは有用である．なぜなら，観測系までの伝達により波形は変形するが，その結果，LSI 単体のシミュレーション波形を用いるのに比べ，むしろ攻撃しやすくなる場合も出てくる為である．本研究では，LSI と観測系との間にある基板や電源系をシンプルな応答モデルで近似することで，実機上で観測される波形の予測を可能にする．

予測手法は大きく分けて 2 種類ある．方法1は，LSI のシミュレーション電流波形から観測波形への伝達を表す応答波形をシミュレーションにより求める方法である．電力解析攻撃の場合は SPICE シミュレーションを，電磁波解析攻撃の場合は FDTD シミュレーションを利用して応答モデルを作成する．図 4.9 は電力波形の予測の例である．方法2は各回路セルの遷移情報から観測波形への伝達を表す応答波形を似たような仕様のサンプル基板を用いてプロファイリングする方法である．サンプル基板上の LSI の論理シミュレーション結果及びサイドチャネル観測波形から応答モデルを同定し，得られた応答モデルを使って評価に必要な数の予測波形を算出する．図 4.10 は，電磁波波形の観測結果と，応答モデルにより算出した波形の比較例である．

②創造性

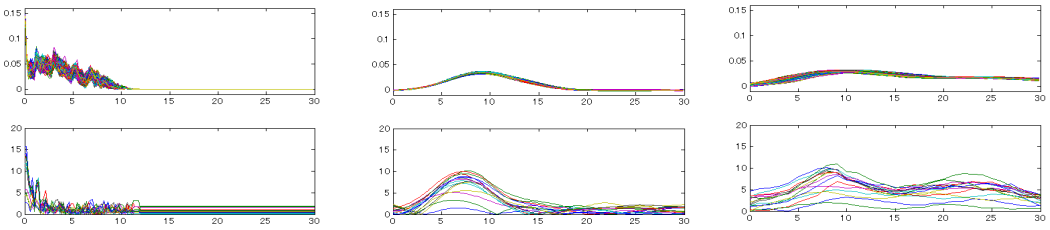
実機でのサイドチャネル観測波形を近似的かつ効率的に予測することができる．電磁波観測波形に対しては，プローブの特性まで考慮した波形を予測することができる．

③有用性

従来，LSI のシミュレーション波形だけでは困難であった，設計段階で実機での攻撃耐性を見積もることができる．実機での耐性評価を前倒しで検討することが可能である．

④優位比較

設計段階で攻撃シミュレーション用の波形を予測するにあたっては，回路の論理動作と，基板上のデバイスのシミュレーションを同時に行う必要があるが，SPICE でこれを実行することは，処理が重すぎて困難である．本研究は，近似的ではあるが，攻撃シミュレーション用の波形を多数求める目的に沿う現実的な予測手法である．



(1) LSI シミュレーション (SASEBO)　(2) 提案手法（予測）　(3) 実　機

図 4.9 実機での電流波形と攻撃耐性の予測

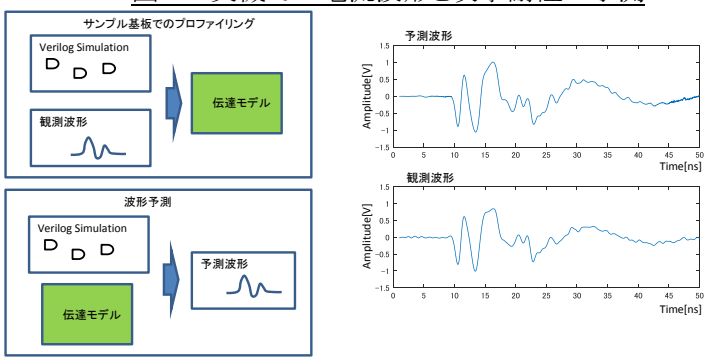


図 4.10 プロファイリングによる攻撃耐性の予測

【B・耐タンパ性能評価プラットフォーム】

4．7　暗号モジュールの安全性評価環境の構築と国際標準化活動（産総研グループ）

①実施方法・実施内容

立命館大 G の耐タンパ暗号 LSI および PUF LSI の評価環境の構築を通じ，ハードウェアセキュリティの評価指針の検討と国際標準化に貢献するため，以下の評価プラットフォームを開発した．

(i) SASEBO-RII: LSI ソケット搭載，暗号 ASIC 用評価ボード（図 4．11（a））

(ii) SASEBO-GIII: 28-nm FPGA 搭載，微小プロセス向けサイドチャネル攻撃評価ボード（図 4．11（b））

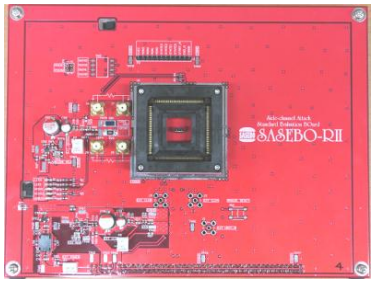
(iii) ZUIHO: Spartan-3 FPGA 搭載，教育用サイドチャネル攻撃評価ボード（図 4．11（c））

(iv) MiMICC: Spartan-6 FPGA 搭載，IC カード型の安全性評価ボード（図 4．11d））

(v) MiMICC-X: Spartan-6 FPGA 搭載，MiMICC のバッテリ駆動改良版（図 4．11e））

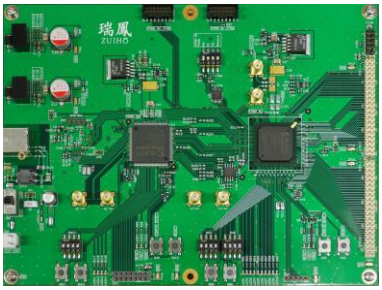
(vi) MiMICC-Z: ARM 内蔵 FPGA（Zynq）搭載，MiMICC の Zynq 搭載・バッテリ駆動改良版（図 4．11f））(vii) 高性能磁界プローブ及び高性能小型磁界スキャナ

(viii) サイドチャネルデータ解析ソフトウェア．

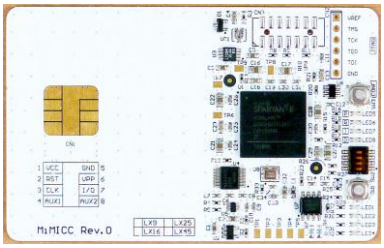


（a）SASEBO-RII

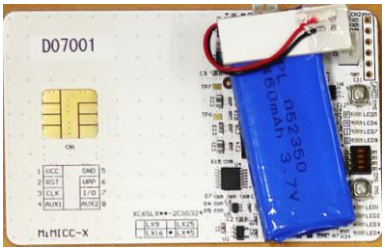
（b）SASEBO-GIII



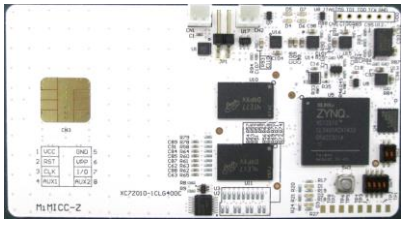
（c）ZUIHO （瑞鳳）



（d） MiMICC



（e）MiMICC-X



（f） MiMICC-Z

図 4.11 サイドチャネル攻撃評価ボード

これら評価プラットフォームを用いた実験に基づき，暗号モジュールに対する安全性評価指針を検討し国際標準化活動に貢献した．米国 NIST における FIPS140-3 の制定作業に協力し，その 2nd ドラフトをベースに国際標準 ISO/IEC19790 が更新された．また，CMVP（Cryptographic

Module Validation Program)のディレクターかつ ISO/IEC19790 のエディタである NIST の Randall Easter 氏とともに国際会議 Non-Invasive Attack Testing workshop(NIST2011)を開催し，さらに，暗号ハードウェアで最も権威のある国際会議 Cryptographic Hardware and Embedded Systems (CHES2011)を佐藤が実行委員長となって開催した．2011 年 10 月に ISO/IEC で暗号モジュールに対する非侵襲攻撃(≒サイドチャネル攻撃)に関する具体的な安全性評価手法を Newwork item として策定することとなり，そのドラフトを Easter 氏と佐藤，坂根で執筆した．そのドラフトは 2015 年に発効予定の ISO/IEC17825 として審議が進み，本プロジェクトで蓄積した環境構築や攻撃方法のノウハウを生かし評価のための具体的な試験手順を提示する等，積極的に貢献した．

現在，ISO/IEC 17825 に関連し、評価のためのより詳細な試験手順や試験ツールのキャリブレーション方法に関する新たな国際標準の策定が検討されている．試験ツールのキャリブレーションとは，例えば，標準評価ボードに標準暗号モジュールを実装して攻撃を行った場合に秘密情報が抽出されるまでに必要な時間やデータ数がおおよそ一定となるよう，各国の試験機関の評価能力を(高いレベルで)平準化することである．本プロジェクトで蓄積した評価環境や評価手法に関するノウハウに基づき，既に各国と協力して標準策定を先導しているが，今後も具体的な試験手順やキャリブレーション手法の構築に貢献してゆく予定である．

ISO/IEC のセキュリティ評価に関する SC27 WG3 国内委員会には、佐藤が 2011 年 11 月から参加し，2012 年度からは坂根が引き継いでいる．また SC27 WG3 では、PUF を用いた非格納式セキュリティパラメータの生成方式について，他国と協力して Study Period proposal を行い，国際標準の策定に向けて各国を先導している．

このほか、2012 年度から，国際的なセキュリティ評価標準 Common Criteria の国内部会 ICSS-JC の委員を堀が務めている．

②創造性および③有用性

暗号 ASIC を評価するための評価ボードの開発は，一般的な研究者にはコスト的・技術的に困難であった．SASEBO-RII の設計データは公開され，学術研究目的に限り自由に利用可能である．これにより，これまで困難であった ASIC 化された暗号のサイドチャネル攻撃研究の促進に貢献している．

SASEBO-GIII は最先端の 28nm プロセスの Kintex-7 FPGA を搭載しており，現時点(2014 年 10 月)で最も微細なプロセスを利用したサイドチャネル攻撃評価ボードである．本成果物によって，半導体プロセスの微細化がサイドチャネル攻撃やその防御手法に及ぼす影響を評価することができる．図 4.12 は，SASEBO-GIII (28nm)と従来の GII (65nm)上で CPA および EMA 実験を行った結果である．秘密鍵 16 バイトを正しく推定するのに要した電力(電磁波)波形数は少ないほうから，65-nm CPA (5,000 波形)，28-nm EMA (7,000 波形)，28-nm CPA (9,000 波形)，65-nm EMA (32,000 波形)であり，今回の実験から電力および電磁波解析攻撃の有効性はプロセスによって異なることが明らかとなった．

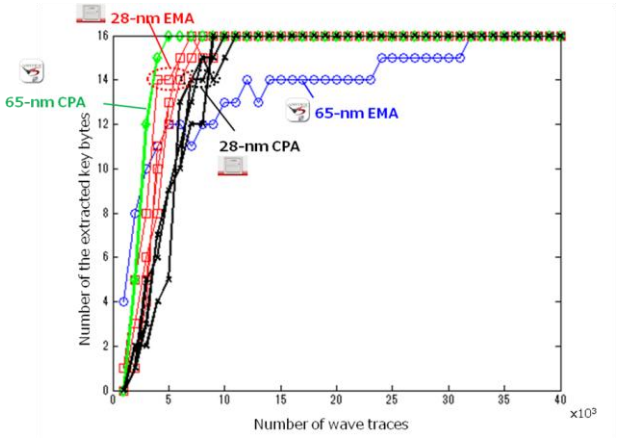


図 4.12.　SASEBO-GIII と GII 上の CPA および EMA

ZUIHO は，サイドチャネル攻撃の教育や技術研修による技術の普及や，防御手法の開発環境構築を目的とした評価環境である．ZUIHO には 90nm というやや大きいプロセスの FPGA が搭載されており，サイドチャネル情報の漏洩量が多くなるように意図的に開発されたものである．これにより，初学者でもサイドチャネル攻撃やしやすく，評価技術者の育成やスキル向上に貢献すると期待される．また，漏洩情報量の多くなる環境で防御技術を開発することで，攻撃を防げた原因がプロセスの微細化によって漏洩情報量が小さくなったためではなく，確かに実装した防御技術によるものであると示すことが可能となる．

MiMICC は IC カード型の FPGA ボードであり，その形状は IC カードの標準規格 ISO/IEC 7810 にほぼ準拠している．MiMICC は 45nm プロセスの Spartan-6 FPGA を搭載しており，対策済み暗号回路を実装して評価するための十分なリソースを有している．これまで，一般ユーザが利用できるプログラマブルな IC カードは汎用組込プロセッサを搭載したものに限られており，ソフトウェア実装された暗号モジュールしか評価できなかった．MiMICC の開発によって，IC カード上の暗号ハードウェアの評価が可能となった．MiMICC は電源供給方式の関係で市販の IC カードリーダでは利用できなかったが，これをバッテリ駆動として市販品に対応した MiMICC-X を開発した．また，ソフトウェアとハードウェアのハイブリッドシステムの評価が可能な ARM 内蔵 FPGA を搭載した MiMICC-Z を開発した．これらにより，IC カードのセキュリティ機能がソフトウェア・ハードウェアのどちらに（あるいは両方に）実装されても評価可能なプラットフォームができた．

SASEBO-RII，SASEBO-GIII，ZUIHO および MiMICC は民間企業に技術移転されて市販化されており，一般的な研究者も容易に入手可能である．これら安全性評価プラットフォームを汎用製品として世界各国の研究者に提供することで，当該研究分野の促進や国際標準化の検討に貢献した．

本研究では，サイドチャネル攻撃の評価環境の構築に必須となる磁界スキャナの開発も行った．本磁界スキャナによって，電磁波解析攻撃に必要となる磁界データの測定を高精度かつ自動で行うことができるようになった．これまでの手動による電磁波測定では計測位置の再現性や計測時間に問題があったが，本研究で XYZ 軸方向に 10μm の精度でモーター制御が可能なステージを開発した．さらに，オシロスコープと磁界スキャナを連動して電力波形を自動的に取得することが可能なソフトウェアの開発も行った．

④優位比較

一般の研究者が容易に入手可能な市販のサイドチャネル攻撃評価ボードは，SASEBO，ZUIHO,MiMICC 以外にはなく，我々のボードは，当該分野の研究を加速するために他に類を見ない大きな貢献を果たしたと言える．

過去にもサイドチャネル攻撃の評価を目的として開発された環境・ボードは複数存在したが，それらのボードは特定のプロジェクトの中で開発されたものであって，当該プロジェクトの関係者以外が入手することはできなかった．また，ボードの詳細について公開されている情報は限られていた．表 4.1 に過去に発表されたサイドチャネル攻撃評価環境を挙げる．なお，OpenADC (http://www.newae.com/openadc)というプロジェクトは，測定装置の設計データやサイドチャネル攻撃のドキュメントを公開している点で我々と類似しているが，ユーザが装置を自作するしかなく容易に購入できないため，表からは除外した．

表 4.1　過去に開発されたサイドチャネル攻撃評価ボード

サイドチャネル攻撃評価ボード	国名・企業名
SCARD (Side-Channel Analysis Resirient Design Flow)	欧州8カ国
MARS (matériel robuste pour systèmes sûrs)	フランス
INSTAC-8	日本規格協会 情報技術標準化センター
INSTAC-32	日本規格協会 情報技術標準化センター
SCAPE (Side-Channel Attack Platform for Evaluation)	三菱電機
SCARF (Side-Channel Analysis Resirient Framework)	ETRI (韓国)

4．8　車載セキュリティーへの暗号回路の適用とサイドチャネル攻撃（立命館大学）

(1) 研究実施内容及び成果

①実施方法・実施内容

≪車載セキュリティーへの暗号回路の適用≫

車載組込み向けシステム・リアルタイム OS に造詣の深い名古屋大学と連携し，車載ネットワークシステムの暗号回路を用いたセキュア化を行なっている．FPGA 上に汎用 CPU コアとハードウェ

ア AES コアを構築し，名古屋大学が開発したリアルタイム OS を動作させ，これまで盗聴や偽造パケットに対し無防備だった CAN(Controller Area Network) プロトコルメッセージの AES 暗号化・セキュア化を目指している．同一 CAN ネットワーク上に不正 ECU（不正な成り済ましパケットを送信する ECU）も設置可能とし，設定変更によって暗号化有無の効果(不正 ECU からアクセル，ブレーキ，ステアリング情報を偽装し，模型カーがドライバーの意図しない挙動を示す)を視覚的に確認できるようなデモシステムを構築，ET2014 にて公開している（図 4.13）．

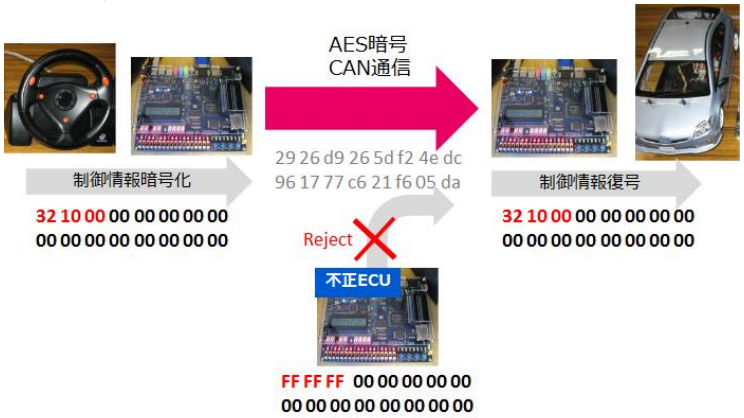


図 4.13 CAN 通信の暗号化による車載不正侵入対策手法

≪車載 ECU を想定したサイドチャネル攻撃≫

ネットワークに対する安全性は前項で対策できるが，各 ECU 単体はサイドチャネル攻撃に対しては無防備なままであり，ネットワーク全体のセキュリティー対策としては不十分である．暗号回路単体だけを動作させていた従来の攻撃者に有利な SASEBO のような環境とは異なり，前項と同一のシステム上でリアルタイム OS が動作し CAN 通信をするという，自動車の走行環境に近い環境において，電磁リークを用いたサイドチャネル攻撃を行い，その潜在的な脅威と危険性について，確認を進めている(図 4.14,15)．

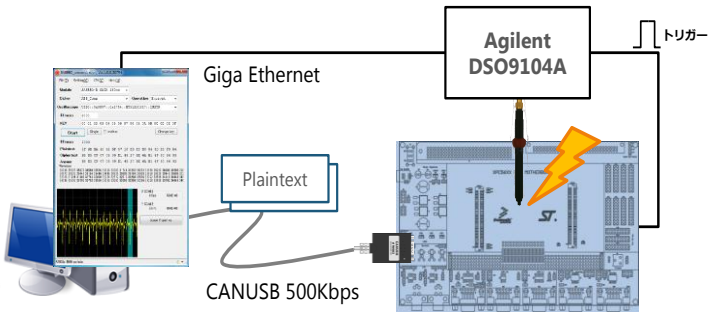


図 4.14 車載 ECU へのサイドチャネル攻撃手法

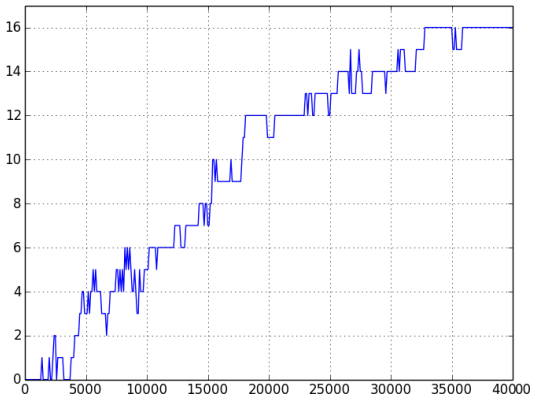


図 4.15 サイドチャネル攻撃結果

②創造性

自動車業界全体において車載ネットワークのセキュア化という課題は緒に就いたばかりである．車載ネットワークの暗号化についても，各自動車業界に関連する企業・研究機関からさまざまな案が提示されているのが現状であり，FPGA ハードウェア AES コアによる CAN メッセージの暗号化等はまだ事例が少なく，高い創造性があるといえる．

また応答性能，ネットワーク帯域の使用効率など実用化観点から，さらなる改良の余地もあり今後の研究の広がりも期待できる．

③有用性

実用済みのドライビングアシスト機能や将来の自動走行システムにみられるように，今後も自動車の車載ネットワークが多様化・高インテリジェント化していくことは自明であり，そのとき課題となるは，さらなる安全性とセキュリティーの向上である．自動車産業は我が国の経済をけん引していく基幹産業分野であり，日本の自動車産業へ，これまでの我々のディペンダブル VLSI の研究成果の浸透・貢献が見込まれる．現在，国内自動車部品メーカーと協力関係・共同研究体制を構築しつつある．

④優位比較

これまで我々が取り組んできたLSIの耐タンパー技術・サイドチャネル対策の知見が生かせる．従来の暗号コア単体を動作させるというサイドチャネル攻撃者優位の環境ではなく，汎用 CPU 上でソフトウェアを動作させ，車載 LAN 通信を行うという，車載ネットワークの実環境に近い測定環境下において，電磁波リークを用いた CEMA 攻撃に成功している．

4．9 公開鍵暗号の厳密な実装安全性評価技術 （三菱電機グループ）

①実施方法・実施内容

車車間通信などで用いられる公開鍵暗号の厳密な実装安全性評価技術を開発した。

②創造性

秘密情報の大部分が単一波形で復元があると考える。本成果は公開鍵暗号への、単一波形を用いたきることを実証した。これは、従来の対策手法のほとんどが無効化されることを意味する。この点に、サイドチャネル攻撃技術であり、開封したチップの近傍からの磁界計測において、乗数・被乗数として同じデータを使用した場合に発生する内部コリジョンを利用した攻撃である(内部コリジョン攻撃)。 ASIC に実装した RSA を対象とした実験を通して、内部コリジョン攻撃によって指数の大部分が単一波形で復元できることを実証した．

③ 有用性および④優位性

既存のアルゴリズムによる対策は単一波形では攻撃できない前提で構成さえており、本成果のインパクトは大きい。また、攻撃で利用するリークの強度が，乗数・被乗数の双方のオペランドについて非対称であることを示す。その性質は，対策と内部コリジョン攻撃の拡張の両方に応用できることを示した。最後に、整数乗算器のオペランド非対称性は，高速乗算アルゴリズム(Booth recoding)に起因することを示した。これは本攻撃に使用されたリークの機序を明らかにしたことを意味する。

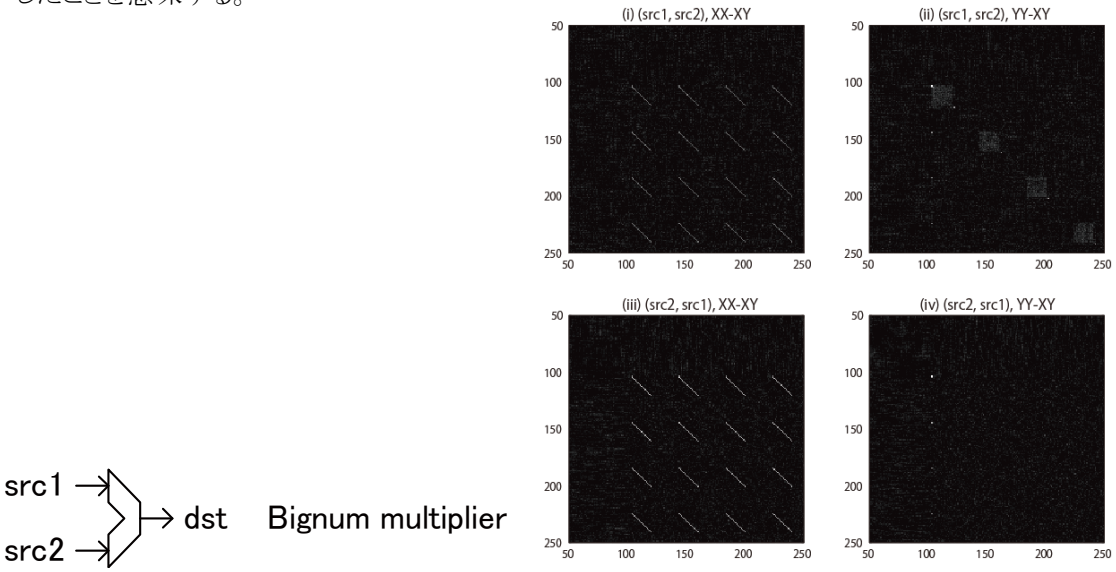


図 4.16 乗数・被乗数とリークの関係

4．10 電磁波解析における厳密な実装安全性評価技術の開発（三菱電機グループ）

①実施方法・実施内容

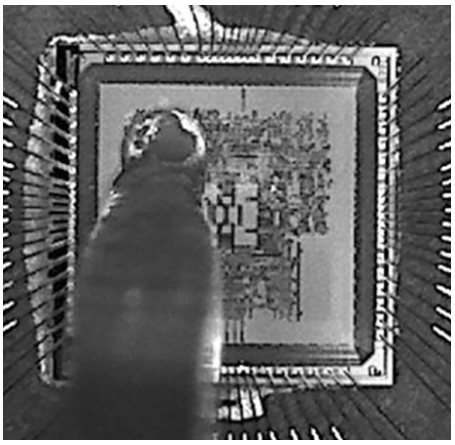
チップの電磁界の計測に基づく暗号解読法（サイドチャネル攻撃）については，10年以上に渡り研究がなされてきた。一方で、攻撃者の計測能力（の限界）については基礎データなしに議論されており論理ゲートより小さい粒度は計測不可能と信じられてきた。本研究では、論理ゲートの「内部」に起因するリークが，計測可能であることを実証。

②創造性

本研究では、スタンダードセル内部に起因するリークが存在しうることに着目した点に創造性がある。従来までは論理ゲートより小さい粒度は計測不可能と信じられており、研究者らの共通認識になっていた。

③有用性および④優位性

スタンダードセル「内部」に起因するリークが，電磁界により計測可能であることが判明した。これは、論理ゲートとして想定される以上の情報が漏洩していることを意味する。この結果は、現状存在するスタンダードセルに安全境界を置く，多くの対策が本質的に脆弱性を抱えていること示唆している。本研究は、レイアウト・トランジスタレベルの対策を検討する上で有用な結果となる。



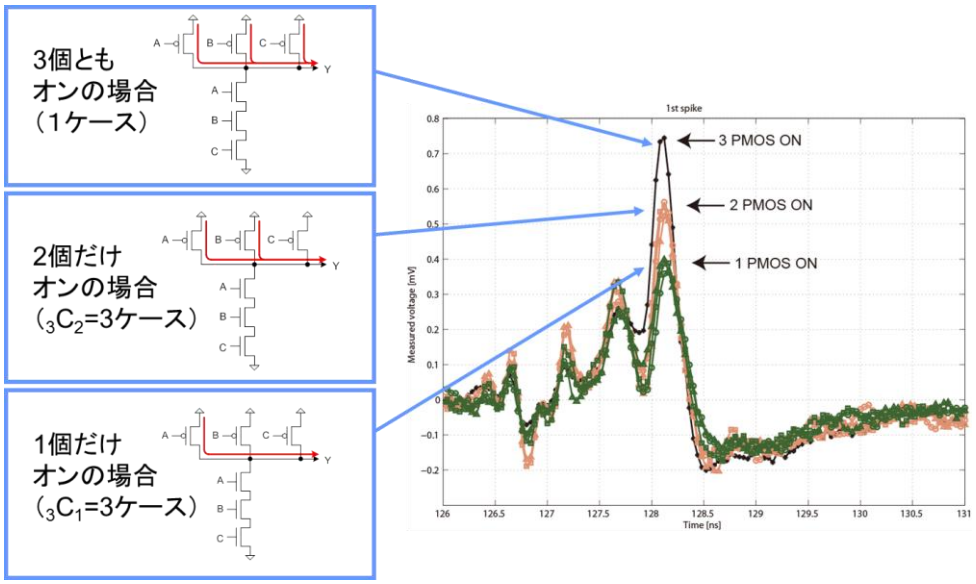


図 4.17 トランジスタの ON の個数と電磁波解析の関係

4．11　FSA シミュレータの開発（三菱電機グループ）

①実施方法・実施内容

近年提案された強力なフォルト解析である Fault Sensitivity Analysis（FSA）に対する安全性を、設計段階にて評価可能なシミュレーション環境を開発し、攻撃者の能力に応じた FSA に対する回路設計上の安全性要件を定義した。尚、FSA は safe error attack と呼ばれる攻撃に属する。safe error attack は、フォルト対策の基本である「エラーを検出したらシステムをリセットする」という機能があっても成立する攻撃であり、一般的な対策が困難な攻撃である。

②創造性

近年提案された強力なフォルト解析である Fault Sensitivity Analysis（FSA）に対する安全性を、設計段階にて評価可能なシミュレーション環境を開発し、攻撃者の能力に応じた FSA に対する回路設計上の安全性要件を定義する点に創造性があると考える。

③有用性および④優位性

本成果によって、FSA に対する脆弱性と対策による効果を論理設計段階で把握することが可能となる。これにより、セキュリティレベルに応じた対策を実施することが可能となる。尚、H22 年度に産総研 G で開発された暗号 LSI の AES 回路は本攻撃によってすべて脆弱性が発見されており、対策は必須である。

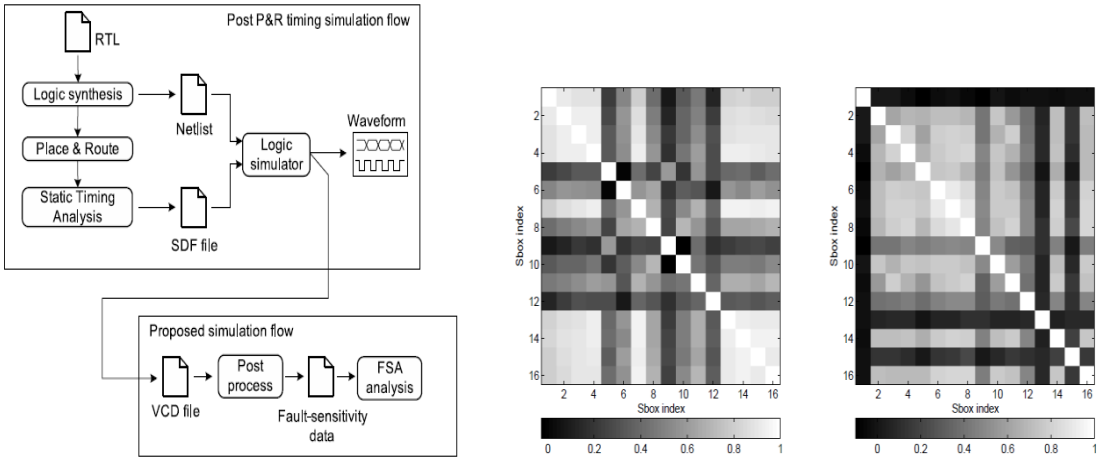


図4.18 開発した FSA シミュレータの動作フローと結果（右図の白色は脆弱性のあるモジュールを意味する）

現時点では解析手法が提案されて間もないため、設計環境や対策についてほとんど議論されていない状況にある。本成果により国内外の研究者に先んじて FSA への対応策を設計フロー込みで示すことができる。一方で、現状 FSA を欧州の研究者と同程度以上の精度で実施可能な環境が国内には存在していない。つまり、現時点では設計は実施できるが、FSA を実機では厳密に評価できない状況にある。

4．12 フォールト攻撃評価システムの開発（三菱電機，名城大グループ）

①実施方法・実施内容

（1）フォールト攻撃評価システム：開発したシステムは、暗号演算中の任意のタイミングでLSIに対してクロックグリッチを挿入し、誤動作（エラー）を誘発させることが可能であり、考案した新しい差分推定法を用いて誤動作によって得られるデータが秘密情報の導出につながるかを本システムで評価可能である。

（2）FSA シミュレータの開発：近年提案された強力なフォールト解析である Fault Sensitivity Analysis（FSA）に対する安全性を、設計段階にて評価可能なシミュレーション環境を開発し、攻撃者の能力に応じた FSA に対する回路設計上の安全性要件を定義した。

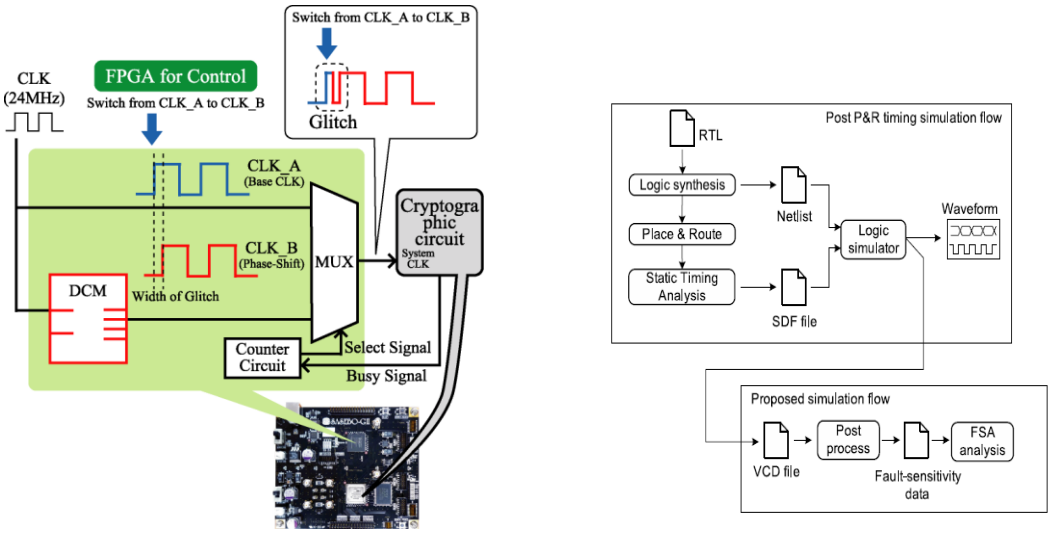


図 4.19 フォールト攻撃評価システム（左：フォールト評価システム、右：FSA シミュレータ）

②創造性・有用性

（1）提案手法では，実機に対して，実際の攻撃者と同じく，故障が発生する場所（ビット位置）や回路の詳細な情報がない場合においても，解析が可能である。さらに，提案手法では，複数のフォールト（エラー）が同時に発生した場合でも，エラーが起きた場合の暗号処理の結果から，どのようなエラーが発生したかを推定可能である。

（2）本成果によって、FSA に対する脆弱性と対策による効果を論理設計段階で把握することが可能となる。これにより、セキュリティレベルに応じた対策を実施することが可能となる。尚、H22 年度に産総研 G で開発された暗号 LSI の AES 回路は本攻撃によってすべて脆弱性が発見されており、対策は必須である。

③優位比較

（1） 不正クロックや不正電圧による誤動作は，供給回路全体が反応してしまうため，発生するエラーの個数や場所の制御は困難であり，従来の解析手法では詳細な解析が難しい。これに対して，提案手法では，発生するエラーの個数や場所を制御しなくても容易に脆弱性を解析することができる。

（2）現時点では解析手法が提案されて間もないため、設計環境や対策についてほとんど議論されていない状況にある。本成果により国内外の研究者に先んじて FSA への対応策を設計フロー込みで示すことができる。一方で、現状 FSA を欧州の研究者と同程度以上の精度で実施可能な環境が国内には存在していない。つまり、現時点では設計は実施できるが、FSA を実機では厳密に評価できない状況にある。今後は評価精度向上のための環境構築を実施していく。

【C・偽造LSIを識別するPUFを用いたセキュリティーシステム】

4．13 遅延時間差検出アービターPUFとFuzzy Extractorを用いた誤り訂正回路（立命館大学グループ）

① 実施内容

PUFはチップ製造時のランダムなばらつきを抽出して固体固有のIDを生成する回路であり，立命大では，簡易なチャレンジ―レスポンス認証に適用可能な，多段接続セレクタチェイン型Arbiter-PUFを研究対象にアーキテクチャの検討，問題点の抽出，およびPUFの性能評価手法の開発を行った．PUF では製造ばらつきという微小な差異を扱っているため出力レスポンスが安定しない問題がある．この不安定レスポンスから誤り訂正技術を用いて安定した暗号鍵を生成するFuzzy Extractor 技術をベースに環境変化（電源電圧変動や温度変化）に強くする手法も検討した．

② 創造性

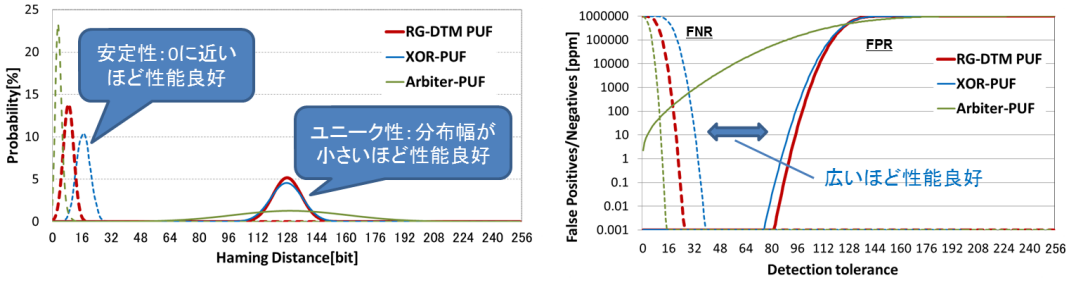
Arbiter-PUF は，PUFの性能指標の1つであるユニーク性（異なるデバイス間でのIDのハミングディスタンス）に原理的な問題を抱えていた．本提案方式の遅延時間検出(Delay-Time Measurement)型 Arbiter-PUF は回路面積や消費電力の増加が 5%と殆どなくユニーク性を向上させた．Fuzzy Extractor に関しては，環境変化も含めて安定した出力（暗号鍵）を得るための具体的な手法が今まで報告されていなかったため，軟判定と信頼度情報の生成手法に関する技術確立を行った．

③ 有用性

Arbiter-PUF のユニーク性の問題点を解決する提案として，立命大では，遅延時間差検出(DTM: Delay Time Measurement)型 Arbiter-PUF の提案を行った．通常の Arbiter-PUF では，2つの等価な経路間でどちらの経路が早く信号を伝搬したかによって出力を決定しているが，本 DTM 方式 PUF では，経路の時間差を測定し，その大きさによってレスポンスを 0,1 に決定する点が特徴であり，実測によりユニーク性が向上することを確認した．また，Arbiter-PUF は機械学習を用いた攻撃による脅威が報告されているので，本提案方式の機械学習攻撃耐性も評価して十分な耐性が達成できることを確認した．Fuzzy Extractorのブロックエラー率を図 4.22 に示す．軟判定における信頼度情報に環境変化時のデータも含ませることにより 1 桁程度ブロックエラー率が改善されることを確認した．

④ 優位比較

180nmCMOS プロセスを用いて，DTM 方式 Arbiter-PUF と，従来型 Arbiter-PUF の試作を行った．前記の2方式に加えて，従来型の改良案として，Verayo 社が提案している XOR Arbiter-PUFとの比較結果を図 4.20 に示す．従来型アービターPUFと比較すると，DTM 方式アービターPUFとXORアービターPUFはユニーク性に優れており，かつ，DTM 方式とXOR 方式を比較すると DTM 方式の方が多数回測定したときの安定性に優れることが分かった．チャレンジ―レスポンス方式の簡易認証でも，DTM 方式が最も認証誤認率が最も低いことが明らかとなった．本 PUF の成果は，採択率 50%以下の国際会議 2011ISCAS(International Symposium on Circuits and Systems)に採択され，暗号実装に関するもっともレベルの高い国際会議 2011CHES(Cryptographic Hardware and Embedded Systems)でもポスター発表を行った．また，電子情報通信学会英文誌 IEICE Trans.Electron.の 2012 年4月号に掲載された．
機械学習攻撃に対する耐性評価結果を図 4.21 に示す．Arbiter-PUFとXOR Arbiter-PUFのチャレンジ-レスポンスを10万サンプル集めれば，残りのレスポンスは予測率 95%以上で予測できるのに対して，本提案方式は全くレスポンスが予測できないことが明らかとなった．本成果は電子情報通信学会英文誌 IEICE Trans.Electron.の 2014 年 1 月号に掲載された．



(a) ユニーク性と安定性の総合評価　　(b)チャレンジ-レスポンンス方式認証での性能比較

図 4.20　DTM 方式 Arbiter-PUF と他の Arbiter-PUF の性能比較

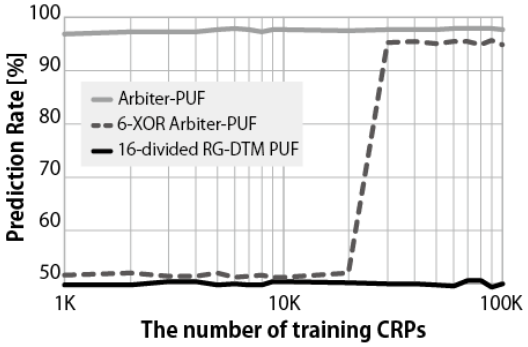


図 4.21　機械学習攻撃耐性比較

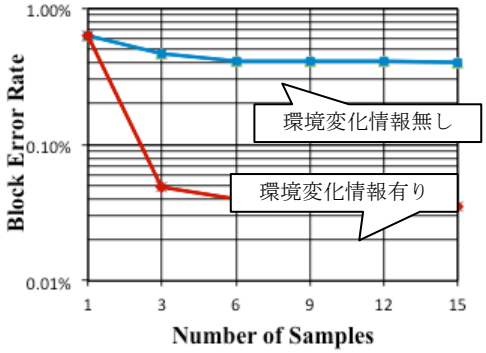


図 4.22　環境変動情報の有無と
ブロック誤り率との関係性

4．14　PUF の構成に関する提案（名城大グループ）

①実施方法・実施内容

PUF については，様々な構成が提案されているが，従来報告されている PUF をベースにした 2 種類の PUF について提案を行った．1 つ目はリングオシレータ PUF について，2 つ目はアービターPUF についての新たな構成法を考案し，特性の改善を実現した．

まず，提案したリングオシレータ PUF は，図 4.23 に示すように，レスポンス補正を行うことを大きな特徴としている．リングオシレータ PUF は選択した 2 つの発振器のどちらの周波数が高いかで 1 ビットのレスポンスを生成する．このとき，各発振器の物理的なばらつきを反映できていれば PUF として使うことができるが，その前提として各発振器の特性が同等である必要がある．しかし，特に FPGA では実装上のばらつきが大きく PUF としての基本性能を確保することが困難であったため，改良型のリングオシレータ PUF を提案した．提案した構成では，比較する 2 つの発振器の組について，1 ビットのレスポンスではなく，位相差を複数ビットの数値で表したレスポンスを出力するように改造し，さらにプロファイリングにより補正用データを生成し，これを用いてレスポンスの補正処理を行うようにすることでユニーク性を大きく改善した．

次にアービターPUF については，従来の 2:1 セレクタを用いる方式に対し，3:1 セレクタを用いて構成したものを提案した．従来，2 系統の信号のどちらが早いかでレスポンスを決めたのに対し，3 系統の信号の到着順位をレスポンス生成に用いている．図 4.24 にその構成を示す．この構成に対して，さらに機械学習攻撃対策としてフィードフォワード機構を組み合わせている．1 セレクタ段あたりのチャレンジは 3 ビットであるが，経路選択は 1 セレクタ段あたり 6 通りであるので，余った 2 通りが指定されたときにフィードフォワードパスを選択するようにした．また，レスポンスについても 3 ビットあることを利用して，エラー訂正と組み合わせたときにその効率を最適化するようなマッピングとした．

②創造性

リングオシレータ PUF に関しては，発振器の位相差を求めるにあたり，非同期型の簡単な回路で実現した．また，経路選択型のリングオシレータに関し，各径路ディレイをパラメータ化して管理することで，補正データの総数を削減した．この構成について，特許出願済みである．3 列アービターPUF は，列数が増えるに従って等長配線の難易度も増すものの，その難易度と多重化によるメリットのバランスを取った構成として研究の余地がある．

③有用性

リングオシレータ PUF は実装面積が大きいという問題があるが，FPGA での IP 保護のための技術の 1 つとして有用である．3 列アービターPUF は，実装規模では従来 PUF よりやや増加するが，等長の配線に留意することで，従来 PUF の代わりとして有用である．

④優位比較

提案したリングオシレータ PUF は従来のリングオシレータ PUF に比べて，実装ばらつきを補正することでユニーク性を大きく改善している．また，3 列アービターPUF は，従来 PUF と比較して機械学習攻撃に対しての耐性の点で有利である．

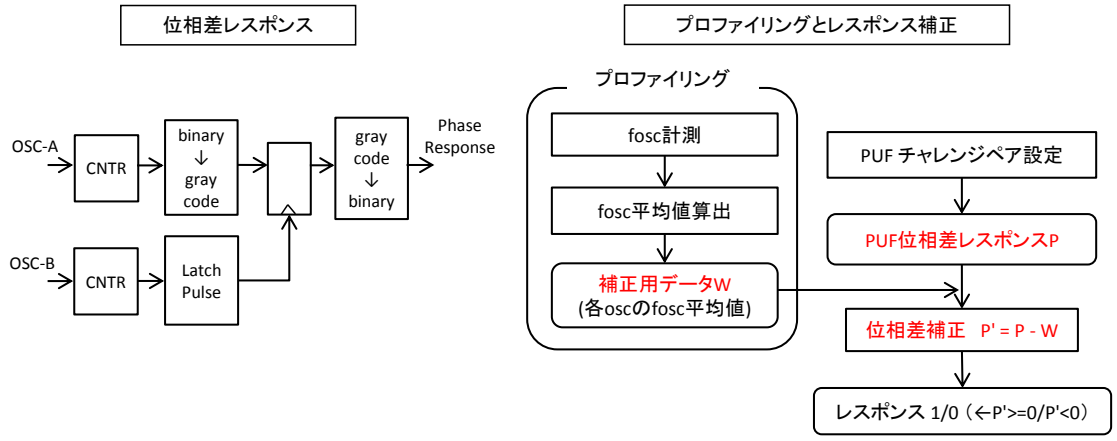


図 4.23 Ring Osc. PUF のレスポンス補正

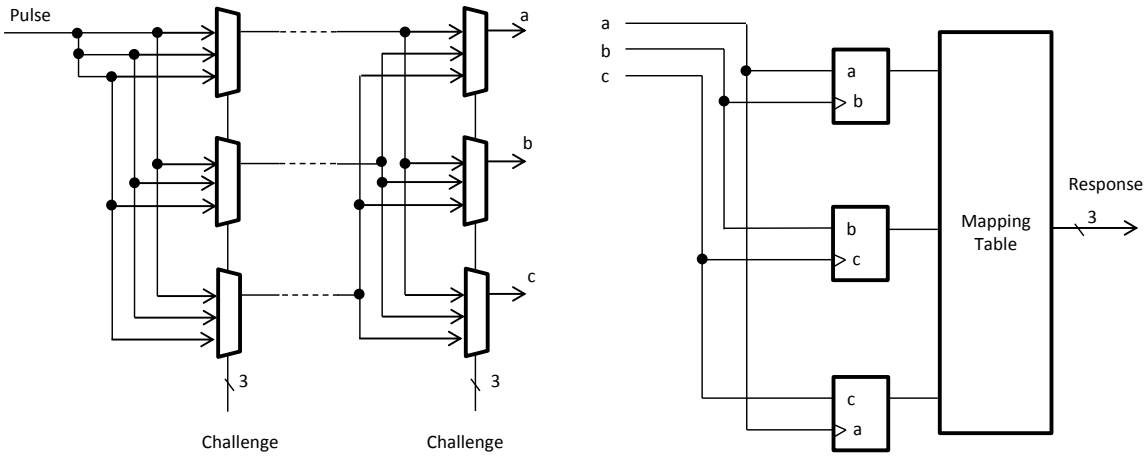


図 4. 24 3:1 セレクタを用いたアービターPUF

4．15　高効率な PUF および鍵生成方式の開発と PUF の定量的性能評価手法
（産総研グループ）

①実施方法・実施内容

Linear Feedback Shift Register (LFSR)の構造を模した小型で高スループットな Pseudo-LFSR PUF（PL-PUF）（図 4.25）を開発した．PL-PUF は動作させるサイクル数を変えることで出力が変化するため，レスポンス空間の極めて広い PUF を実現できる．動作サイクル数が小さい場合は再現性やユニーク性が高くデバイス認証に有効な PUF として働く一方で，動作サイクル数を大きくすると再現性が低くなりランダム性が増すため真性乱数生成器として利用することも可能である．さらに，PL-PUF は機械学習を用いたクローン攻撃にも安全であると考えられる．

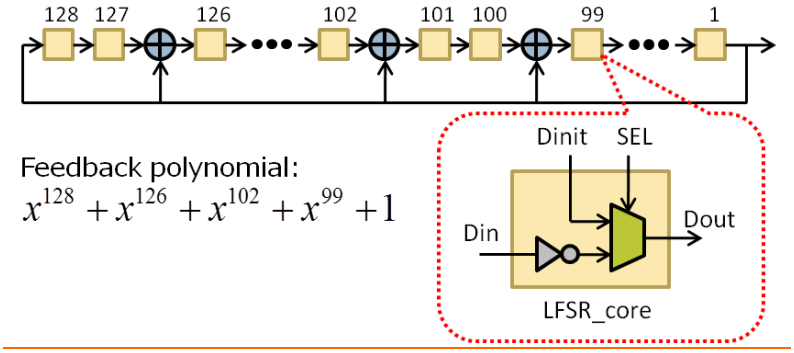


図 4.25 Pseudo-LFSR PUF(PL-PUF)の構造

また，PUF の重要な特性として，同一チャレンジに対する再現性，異なるチャレンジに対する非衝突性，異なるデバイス間でのユニーク性等が挙げられる．これらの性能を定量的に評価する方法はいくつか存在するが確立されているとは言えず，さらに人間にとって非直観的であるため，様々なデバイス上で様々なアーキテクチャの PUF を比較評価するには不向きである．本研究では，直感的でわかり易い PUF の定量的性能指標を開発した．この評価ツールは MATLAB に実装され，Web 上で公開されている．

上記回路方式のほか，PUF の出力から効率よく秘密情報を生成する方式を開発し，これを用いた認証方式のデモシステムを開発した．PUF の出力にはノイズが多く含まれるため，PUF の出力から秘密情報を一意に作成するための補助データ（helper data）が必要となる（補助データは秘密情報ではない）．補助データを用いて秘密情報を復元するための既存の手法として，Fuzzy Extractor [1)] がある．ただしこの方式は，補助データのサイズが大きくなる傾向にある．

1)　Y. Dodis et al., “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data,” SIAM J. Comput., 38(1), 2008.

一方，我々の方式を図に示す．我々の方式では，チャレンジ C と，それに対する PUF のレスポンスの一部をシンドロームとしてデータベースに格納する．これによって，データベースに格納するデータのサイズを大幅に削減可能（図の場合は従来方式の約 1/4）とし，秘密情報復元のために必要となる回路サイズも大幅に縮小される．

②創造性および③有用性

従来方式の PUF は，128 ビットや 256 ビット等の長いチャレンジから高々1 ビットのレスポンスを得ることが普通であったが，本研究で開発した PL-PUF はレスポンスのスループットを高めることに着目している点が新しい．また，発振時間を長くすることで真性乱数生成器としても利用可能であるのは，他の方式にはない特長である．秘密情報を生成するモジュールと乱数生成器は共に現代の IT 機器において必須のコンポーネントであり，同一の PUF 回路でこれらの機

能を有することは画期的である.

提案手法の PL-PUF は 128 ビットの入力から 128 ビットの出力が得られ, 動作周波数 24MHz の下で 3Gbps 以上のスループットを実現可能であり, 暗号鍵を頻繁に変更するようなアプリケーションでも利用可能である. また, 従来方式の PUF の中には, 機械学習攻撃によって内部の遅延パラメータを推測することが可能なものが知られているが, PL-PUF は複雑な発振をするためモデル化が難しく, 機械学習による攻撃にも強いと期待される.

PUF の性能を定量的かつ容易に評価できることは, PUF を利用する安全なシステムの開発に重要である. 提案手法は, PUF の性質を Randomness, Steadiness, Correctness, Diffuseness, Uniqueness の 5 つの指標によって評価することを可能にする. すべての性能指標は 0〜1 までの値をとり, 0 が最低で 1 が最高の性能を表す. これら性能指標は直感的に理解しやすく, PUF の比較評価のために有効である. この評価指標は MATLAB に実装され Web サイトで公開されており, 高性能な PUF の開発に貢献している.

また本研究では, ノイズの含まれる PUF 出力から秘密情報を復元するための効率のよい方式を開発した. M2M や IoT においては膨大な数のデバイスが人間を介することなく相互認証することが求められており, これらデバイスに PUF を搭載することが有効であると期待される. しかし, 多数の PUF の入出力データや補助データを登録するために極めて巨大なデータベースが必要となってしまうため, データベースのサイズを抑える技術が重要となる. また, M2M や IoT で大多数を占めるモバイル機器やセンサデバイスでは, 搭載可能な回路サイズが制限されるため, 回路の小型化も必須である. 本研究で開発した鍵生成方式は, 補助データのサイズを従来方式の 1/4 に抑えることが可能であり, データベースのサイズ削減に極めて有効である. また, 秘密情報を復元するために必要な回路リソースも大幅に削減可能である. これにより, M2M 等において PUF を利用した相互認証システムを実現することが期待される.

④優位性

従来方式の PUF は長いチャレンジ入力に対して 1 ビットのレスポンスを得るため, 秘密情報を生成する際のスループットが低いという問題があると同時に, 1 つの秘密情報を復元するために必要な入出力データ・補助データのサイズが大きくなってしまうという問題がある. PUF から秘密情報を復元するためには, チャレンジとそれに対応する補助データをデータベースに格納しておく必要があるためである. 本方式の PUF は, スループットの高さやデータベース占有サイズの小ささで他の方式に対して大きな優位性を有する. また, シンドロームを用いた秘密情報の復元方式により, データベース占有サイズをさらに小さくできると共に, 回路サイズも大幅に削減される見込みである. これにより, PUF 回路の低コスト化はもちろん, データベースを含む認証システムの構築においても, 他の方式と比較して最も低コストで実現可能であると期待される.

4．16 新型 PUF および誤り訂正技術を用いた秘密鍵生成回路（三菱電機グループ）

①実施方法・実施内容

PUF はチップ製造時のランダムなばらつきを抽出して固体固有の ID を生成する回路であり、三菱電機では、複雑な回路内で生成されるグリッジの情報を利用する「グリッジ PUF」を提案している。PUF は生成される ID のユニーク性（異なる PUF からは異なる ID が生成されること）、再現性（異なる ID 生成環境でも安定な ID を生成できること）、機械学習攻撃耐性（PUF に対するチャレンジ―レスポンスを多数収集しても、新たなチャレンジに対するレスポンスを予測することができないこと）などを評価対象としてアーキテクチャの検討，問題点の抽出、および PUF の性能評価手法の開発を行った。

②創造性

ランダムロジックで発生する過渡現象(グリッチ)が回路間の遅延関係によって異なる振る舞いをする。このため、同一回路を実装しても、LSI の遅延ばらつきによって固体毎にグリッチの振る舞いが異なる。この現象を利用して LSI 毎にユニーク ID を生成する技術に創造性があると考える。

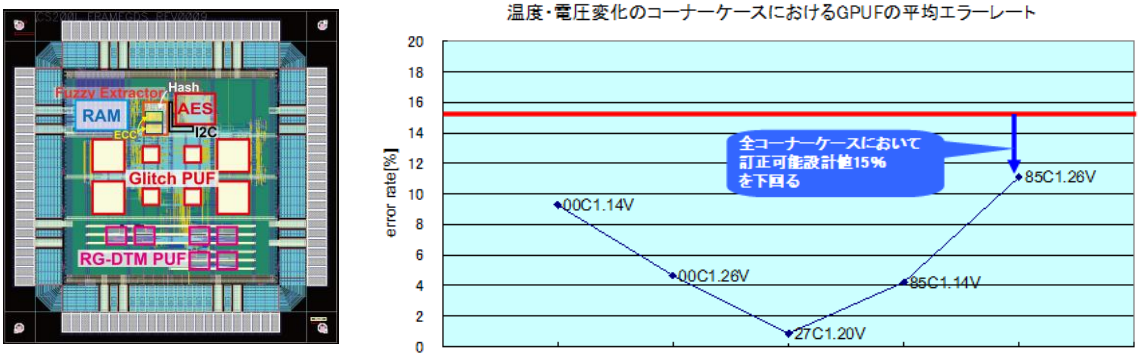
③有用性および④優位性

PUF は本質的にレスポンスに揺らぎを持つため、そのままでは1ビットの誤りも許されない暗号鍵を生成することはできない。これに対して、グリッチ PUF 回路、誤り訂正回路、汎用ハッシュ関数回路を組み合わせることにより、PUF 回路の不安定な出力ビット列を訂正して秘密情報を安定に生成する鍵生成回路を国内で始めて開発した。本回路を搭載した LSI を e-Shuttle 65nm プロセスで製造し評価した結果、図 4.26 に示す通り、0℃～80℃の温度，±5%の電圧変動に対しても安定に鍵を生成できることを確認した

欧州の Intrinsic-ID 社は既にいくつかのプロセスで鍵生成回路の試作が完了しており、複数の実績を積んでいる。一方で、Intrinsic-ID 社の方式は完全に SRAM の特性で性能が決定するため調整には半導体ベンダの協力が不可欠であるという設計制約上の問題と、SRAM はグリッジ PUF 方式と比較して、場所の特定が容易であるという耐タンパ性の問題を持っている。耐タンパ性の高いグリッジ PUF 方式で，Intrinsic-ID 社と同様の鍵生成が可能であることを 65nmCMOS 実チップで実証できたという点で優位性がある．

＜非公開＞

模倣品対策としてグリッチ PUF を社内向け ASIC 開発でプロセス向けに改良することにより、製品搭載を実施した。



(a) 65nm CMOS チップレイアウト (b)グリッジ PUF で生成した ID のエラーレート評価結果

図 4.26 新型 PUF 回路と誤り訂正回路等を用いた鍵生成回路搭載テストチップと評価結果

4．17　暗号回路と PUF を用いた耐タンパキーレスエントリーデモシステム（立命館大学，三菱電機）

① 実施内容

セキュリティー認証は IC カードだけでなく，センサーネットワークや車載セキュリティーへと応用分野が広がっている.しかし，暗号アルゴリズムは理論的に安全であっても，共通鍵暗号を用いた認証においては，サイドチャネル攻撃や鍵保存メモリの不正読み出しによる共通鍵を入手する攻撃の危険性が指摘されている.そこで，サイドチャネル攻撃対策済 AES 暗号回路と共通鍵を PUF 生成鍵を用いて暗号化し，保管することにより攻撃対策を施したセキュアな認証システムとして，キーレスエントリーを模した認証システムの実装を行い，高セキュアな認証システムが実現可能であることを示した．（図 4.27）

② 創造性

提案手法を用いることで，共通鍵を保管する耐タンパ不揮発性メモリを必要としない低コスト認証システムの構築が可能である.さらに，車載制御システムへの応用として，ECU などの車載機器に搭載することにより，車載ネットワークにおける通信相手の認証を行うことで，安全な通信が可能である車載 LAN 通信のセキュア化手法の提案を行った.また，本提案手法を用いることで，改造をされた MCU 制御ソフトのインストールの禁止やネットワークを介したアップデートにおける ECU(MCU)制御プログラムの正真性の確保，正規品でない部品への交換の認証を行うことで模造品対策としても役立つことが期待される.

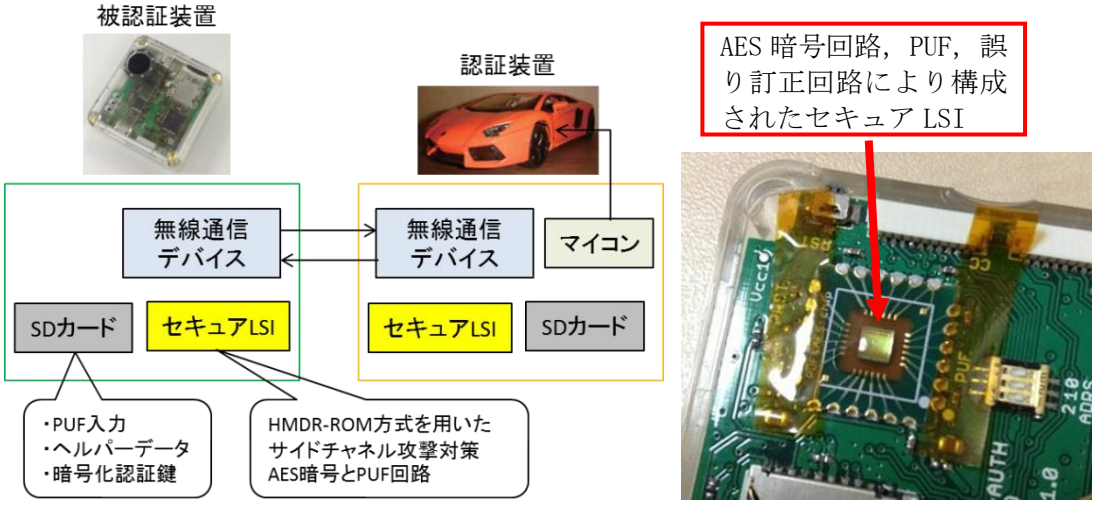


図 4.27　開発したキーレスエントリーを模した認証システムとセキュア LSI

③ 有用性と優位比較

サイドチャネル攻撃による暗号鍵の窃取，鍵保存メモリからの暗号鍵不正読み出しの危険から守る手法を，キーレスエントリーを模したデモンストレーションという目に見える形で示したことで，ET 展などで幅広い方々に耐タンパ技術の重要性を理解して頂いた．今後耐サイドチャネル攻撃暗号回路 HMDR-ROM AES，PUF 回路，そして PUF の出力から安定した暗号鍵を生成する Fuzzy Extractor 回路をセットで提供できるソリューションを提供することで，暗号鍵を保管するのに耐タンパ不揮発性メモリを必要しない，低コスト・高セキュリティー認証システムの構築が可能となる.

§５ 成果発表等

(1)原著論文発表 (国内(和文)誌 11 件、国際(欧文)誌 54 件)

[1] Akashi Satoh, Toshihiro Katashita, and Hirofumi Sakane, “Secure Implementation of Cryptogpraphic Modules -Development of Standard Evaluation Environment for Side Channel Attacks-,” Synthesiology - English edition, vol. 3, no. 1, pp. 86-95, (2010-07).

[2] Kenji Kojima, Kazuki Okuyama, Katsuhiro Iwai, Mitsuru Shiozaki, Masaya Yoshikawa, and Takeshi Fujino, “LSI Implementation Method of DES Cryptographic Circuit utilizing Domino-RSL Gate Resistant to DPA Attack,” SASIMI Digest of Technical Papers, (2010-10).

[3] M.Yoshikawa, Y.Kokusyo, and T.Fujino, “Placement Tool Dedicated for a Via-programmable Logic Device VPEX”, Proc. of 23rd International Conference on Computer Applications in Industry and Engineering, pp.21-25, (2010-11).

[4] Yohei Hori, Takahiro Yoshida, Toshihiro Katashita and Akashi Satoh, “Quantitative and Statistic Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs”, International Conference on ReConFigurable Computing and FPGAs (ReConFig2010), pp.298-303, (2010-12).

[5] Anh-Tuan Hoang, Masaya Yoshikawa, and Takeshi Fujino, “AES Side Channel Attack Using Final to First Rounds Hamming Distance”, NCSP 2011 Technical Papers, (2011-03).

[6] Mitsuru Shiozaki, Teruri Fukushima, Kota Furuhashi, Takahiko Murayama, and Takeshi Fujino, “Evaluation of Uniqueness and Environmental Stability of IC Identification Generated by Arbiter-PUF,” NCSP 2011 Technical Papers, (2011-03).

[7] Masaya Yoshikawa and Toshiya Asai, "High-Level Simulation for Side Channel Attacks", Proc. of The International MultiConference of Engineers and Computer Scientists, Vol.2, pp.1565-1568, (2011-03).

[8] Kota Furuhashi, Mitsuru Shiozaki, Akitaka Fukushima, Takahiko Murayama and Takeshi Fujino, “The Arbiter-PUF with High Uniqueness utilizing Novel Arbiter Circuit with Delay-Time Measurement”, Digest Paper of The IEEE International Symposium on Circuits and Systems (ISCAS), pp.2325-2328, (2011-05).

[9] Katsuhiko Iwai, Mitsuru Shiozaki, Anh-Tuan Hoang, Kenji Kojima, and Takeshi Fujino, “Implementation and Verification of DPA-Resistant Cryptographic DES Circuit using Domino-RSL”, Proceeding of The IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp.28-33, (2011-06).

[10] Takeshi Kumaki, Hiroki Yoshikawa, Yuichiro Kurokawa and Takeshi Fujino, “Highly-parallel Bitslice AES Implementation with Massive-parallel SIMD Matrix for Mobile Processor”, Proceeding of The 26th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), pp.237-240, (2011-06).

[11] M.Yoshikawa, K.Sakaue, "Dedicated hardware for RC5 cryptography and its implementation", Proc. of International Conference on Embedded Systems and

Applications, pp.135-139,(2011-07).

[12] M.Yoshikawa, M.Sugiyama, "Multi-rounds masking method against DPA attacks", Proc. if IEEE International Conference on Information Reuse and Integration, pp.100-103, (2011-08).

[13] M.Yoshikawa, Y.Kojima, "Efficient random number for the masking method against DPA attacks", Proc. of International Conferences on Systems Engineering, pp.321-324,(2011-08).

[14] M.Yoshikawa, T.Asai, "DPA Attacks Simulator against Cryptography System on Algorithm Design Phase", Proc. of World Congress on Engineering and Computer Science, Vol.1, pp.792-796,(2011-10).

[15] 吉川雅弥, 浅井稔也, 汐崎充, 藤野毅「上流設計工程でのサイドチャネル攻撃に対する耐タンパ検証手法とその評価」, 電気学会論文誌C, Vol.131, No.11, pp.1940-1949, (DOI: 10.1541/ieejeiss.131.1940) (2011-11).

[16] Yohei Hori, Hyunho Kang, Toshihiro Katashita, and Akashi Satoh, “Pseudo-LFSR PUF: A Compact, Efficient and Reliable Physical Unclonable Function”, 7th International Conference on ReConFigurable Computing and FPGAs (ReConFig'11), pp.223-228, 2011. (2011-12).

[17] 吉川雅弥, 浅井稔也, 汐崎充, 藤野毅「統計補正処理を用いた経路選択リングオシレータPUFとその実装評価」, システム制御情報学会論文誌, Vol.25, No.1, pp.1-10,(2012-01).

[18] Anh-Tuan Hoang and Takeshi Fujino, “2012 Intra-Masking Dual-Rail Memory on LUT Implementation for Tamper Resistant AES on FPGA,” 20th ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (FPGA), (2012-02).

[19] M.Yoshikawa, T.Asai, "Dedicated Evaluation System for Fault Attacks", Proc. of International Conference on Information and Computer Networks, vol.27, pp.254-257, (2012-02).

[20] 吉川雅弥, 浅井稔也, 汐崎充, 藤野毅「多重化ユニットを用いた物理的複製不可能関数とその実装評価」, 電気学会論文誌C, Vol.132, No.3, pp.364-373,(2012-03). DOI: 10.1541/ieejeiss.132.364

[21] Kousuke Ogawa, Mitsuru Shiozaki, Kota Furuhashi, Kohei Hozumi and Takeshi Fujino, “Performance Comparison of RG-DTAM PUF and Arbiter-based PUFs,” Proc. of The 17th Workshop on Synthesis And System Integration of Mixed Information technologies (2012-03).

[22] Hiroki Yoshikawa, Takeshi Kumaki and Takeshi Fujino, “Highly-parallel AES processing for five confidentiality modes with massive-parallel SIMD matrix processor,” Proc. of The 17th Workshop on Synthesis And System Integration of Mixed Information technologies (2012-03).

[23] R.Satoh, D.matsusima, M.Yoshikawa, "Subkey Driven Power Analysis Attack in Frequency Domain against Cryptographic LSIs", Proc. of The 17th Workshop on Synthesis And System Integration of Mixed Information technologies pp.262 -267

(2012-03).

[24] Masaya Yoshikawa, Toshiya Asai, "A vulnerability evaluation method for power analysis attacks against cryptography circuits", Proc. of ISCA 27th International Conference on Computers and Their Applications. pp.167-172 (2012-03)

[25] Mitsuru Shozaki, Kota Furuhashi, Takahiko Murayama, Akitaka Fukushima, Masaya Yoshikawa, Takeshi Fujino, “High Uniqueness Arbiter-Based PUF Circuit Utilizing RG-DTM Scheme for Identification and Authentication Applications”, IEICE TRANSACTIONS on Electronics, Vol. E95-C, No.4, pp.468-477, (2012-04)

[26] Kousuke Ogawa, Mitsuru Shiozaki, Kota Furuhashi, Takeshi Fujino, “Experimental Security Evaluation against Machine Learning Attacks on RG-DTM PUF,” Proc. of 27th International Technical Conference on Circuit/Systems, Computers and Communications, C-T1-02 (2012-7)

[27] 堀洋平, 片下敏宏, 姜玄浩, 佐藤証「45nm プロセス FPGA 上の Physical Unclonable Function の特性評価」, マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO2012), pp.1928-1933, (2012-07).

[28] Hyunho Kang, Yohei Hori, Toshihiro Katashita, and Akashi Satoh, "PUF Evaluation against Linear Programming Model on SASEBO-GII", マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO2012), pp.1947-1950, (2012-07).

[29] M.Yoshikawa, M.Katsube, "Development of an Encryption LSI Resistance Evaluation Platform for Fault Analysis Attacks Against the Key Generation Section and Its Evaluation", Proc. of International Conference on Embedded Systems and Applications, pp.10-14,(2012-07)

[30] Yohei Hori, Toshihiro, Katashita, Akihiko Sasaki, and Akashi Satoh, "Electromagnetic Side-channel Attack against 28-nm FPGA Device", in pre-proceedings of the 13th International Workshop on Information Security Applications (WISA2012), pp.71-72, (2012-08).

[31] M.Yoshikawa, "Multiplexing Aware Arbiter Physical Unclonable Function", Proc. of IEEE International Conference on Information Reuse and Integration, pp.639-644,(2012-08)

[32] Takeshi Sugawara, Daisuke Suzuki and Toshihiro Katashita, “Circuit Simulation for Fault Sensitivity Analysis and its Application to Cryptographic LSI”, The 9th Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC2012), (2012-09).

[33] Toshihiro Katashita, Akihiko Sasaki, Yohei Hori, Mitsuru Shiozaki, and Takeshi Fujino, "Development of Evaluation Environment for Physical Attacks against Embedded Devices", The 1st International Conference on Consumer Electronics (GCCE2012), pp.598-601, (2012-10).

[34] Yohei Hori, Toshihiro Katashita, Akihiko Sasaki, and Asashi Satoh, "SASEBO-GIII: A Hardware Security Evaluation Board Equipped with a 28-nm FPGA", The 1st International Conference on Consumer Electronics (GCCE2012), pp.666-669, (2012-10).

[35] Hyunho Kang, Yohei Hori, Toshihiro Katashita and Akashi Satoh, "Performance of Physical Unclonable Functions with Shift-Resister-Based Post-Processing", International Conference on Security Technology (SecTech 2012), (2012-11)

[36] Yohei Hori, Toshihiro Katashita, Akihiko Sasaki, and Asashi Satoh, "A First Report on Electromagnetic and Power Analysis Attacks against 28-nm FPGA Device", Information-An International Interdisciplinary Journal, Vol.16, No.8(B), pp.5993-6006, (2013-8).

[37] 小野みどり, 勝部真人, 汐崎充, 藤野毅, 吉川雅弥「アーキテクチャを考慮した複数エラーの差分推定に基づくフォールト解析とその評価」, 電気学会論文誌 C, Vol.132, No.12, pp.1888-1896, (2012-12)

[38] 浅井稔也, 汐崎充, 藤野毅, 吉川雅弥「暗号ハードウェアのゲートレベル設計工程における電力解析攻 撃に対する脆弱性評価手法」, 電気学会論文誌C, Vol.133, No.5, pp.947-956, 2013. DOI: 10.1541/ieejeiss.133.947

[39] 佐藤隆亮, 松島大祐, 汐崎充, 藤野毅, 吉川雅弥「周波数領域における部分鍵推定を用いたハイブリッド電力解析攻撃とその評価」, 電気学会論文誌C, Vol.133, No.7, pp.1322-1330, 2013. DOI: 10.1541/ieejeiss.133.1322

[40]M.Yoshikawa, T.Asai, "Platform for Verification of Electromagnetic Analysis Attacks against Cryptographic Circuits", Proc. of International Conference on Information Technology : New Generations., pp.653-658(2013-4)

[41]M.Yoshikawa, "Hybrid Power Analysis Attack in Frequency Domain for Security Modules", Proc. of 4th International Congress on Computational Engineering and Sciences, p.149(2013-5).

[42] Hyunho Kang, Yohei Hori, Toshihiro Katashita, Akashi Satoh, Keiichi Iwamura, "PUF Evaluation with Post-processing and Modified Modeling Attack , " International Journal of Security and Its Applications (IJSIA), Vol.7, No.4, pp.231-241 (2013.7)

[43] Yohei Hori, Toshihiro Katashita, Akihiko Sasaki and Akashi Satoh, "A First Report on Electromagnetic and Power Analysis Attacks against 28-nm FPGA Device," Information - An International Interdisciplinary Journal, Vol.16, No.8(B), pp.5993-6006 (2013.8)

[44] Takeshi Sugawara, Daisuke Suzuki, Minoru Saeki, Mitsuru Shiozaki, Takeshi Fujino: On Measurable Side-Channel Leaks Inside ASIC Design Primitives. CHES 2013: 159-178, (2013.8).

[45] Megumi Shibatani, Mitsuru Shiozaki, Yuki Hashimoto, Takaya Kubota and Takeshi Fujino, "PowerAnalysis Resistant IP Core using IO-Masked Dual-Rail ROM for Easy Implementation into Low-Power Area-Efficient Cryptographic LSIs," Synthesis And System Integration of Mixed Information technologies (SASIMI) (2013-10)

[46] Masato Taniguchi, Mitsuru Shiozaki, Hiroshi Kubo and Takeshi Fujino, "A Stable Key Generation from PUF Responses with a Fuzzy Extractor for Cryptographic

Authentications," In Proc. GCCE2013, pp. 525-527 (2013-10)

[47] Tsunato Nakai, Mitsuru Shiozaki, Takaya Kubota and Takeshi Fujino, "Evaluation of On-Chip Decoupling Capacitor's Effect on AES Cryptographic Circuit," Synthesis And System Integration of Mixed Information Technologies (SASIMI) (2013-10)

[48] K.Sugioka, T.Asai, M.Yoshikawa, "Event Modeling Method for Verification of Power Analysis Attacks" , Proc. of The 18th Workshop on Synthesis And System Integration of Mixed Information Technologies, pp.280-281(2013-10)

[49] Toshihiro Katashita, Akihiko Sasaki, and Yohei Hori, "A Novel Smart Card Development Platform for Evaluating Physical Attacks and PUFs," in Proc. GCCE2013, pp.37-39 (Outstanding Poster Award) (DOI: 10.1109/GCCE.2013.6664860)
(2013.10)

[50] Hyunho Kang, Yohei Hori, Toshihiro Katashita, Manabu Hagiwara, Keiichi Iwamura, "Performance Analysis for PUF Data Using Fuzzy Extractor," in Proc. CUTE 2013, Lecture Note in Electrical Engineering, Vol. 280, pp.277-284 (DOI: 10.1007/978-3-642-41671-2_36)(2013.12)

[51] 浅井稔也, 汐崎充, 久保田貴也, 藤野毅, 吉川雅弥「クロック変動機構を用いた耐タンパアーキテクチャ」電気学会論文誌C, Vol.133, No.12, pp.2134-2142, (2013-12)

[52] Mitsuru Shiozaki, Kousuke Ogawa, Kota Furuhashi, Takahiko Murayama, Masaya Yoshikawa, and Takeshi Fujino, "Security Evaluation of RG-DTM PUF using Machine Learning Attacks", IEICE TRANSACTIONS on Electronics, Vol. E97-A, No.1, pp.275-283, (2014-1)

[53] Koichi Shimizu, Daisuke Suzuki, Toyohiro Tsurumaru, Takeshi Sugawara, Mitsuru Shiozaki, Takeshi Fujino: Unified Coprocessor Architecture for Secure Key Storage and Challenge-Response Authentication. IEICE Transactions 97-A(1): 264-274 (2014-1)

[54] Takeshi Sugawara, Daisuke Suzuki, Minoru Saeki, Mitsuru Shiozaki, Takeshi Fujino: On measurable side-channel leaks inside ASIC design primitives. J. Cryptographic Engineering, Vol. 4(1): 59-73 (2014-1)

[55] Hyunho Kang, Yohei Hori, Toshihiro Katashita, Manabu Hagiwara, Keiichi Iwamura, "Cryptographic Key Generation from PUF Data Using Efficient Fuzzy Extractors," in Proc. ICACT 2014, pp.23-26 (Outstanding Paper Ward) (DOI: 10.1109/ICACT.2014.6778915) (2014.2)

[56] Shintaro Ukai, Tsunato Nakai, Mitsuru Shiozaki, Takaya Kubota and Takeshi Fujino, "Tamper-Resistant AES Cryptographic Circuit utilizing Hybrid Masking Dual-Rail ROM," Nonlinear Circuits, Communications and Signal Processing (NCSP) (2014-3)

[57] M.Yoshikawa, T.Asai, "Tamper Resistance Verification Method for Consumer Security Products", Proc. of Computational Science & Computational Intelligence, pp.30-33 (2014-3)

[58] Yohei Hori, Toshihiro Katashita, Hyunho Kang, Akashi Satoh, Shinichi

Kawamura,and Kazukuni Kobara, “Evaluation of Physical Unclonable Functions for 28-nm Process Field-Programmable Gate Arrays,” Journal of Information Processing, Vol.22, No.2, pp.344-356 (2014-4)

[59] Tsunato Nakai, Megumi Shibatani, Mitsuru Shiozaki, Takaya Kubota and Takeshi Fujino, “Side-Channel Attack Resistant AES Cryptographic Circuits with ROM reducing Address-Dependent EM Leaks”, Digest Paper of The IEEE International Symposium on Circuits and Systems (ISCAS), pp.2547-2550, (2014-06).

[60] Takeshi Sugawara, Daisuke Suzuki, Ryoichi Fujii, Shigeaki Tawa, Ryohei Hori, Mitsuru Shiozaki, Takaya Kubota and Takeshi Fujino, “Reversing Stealthy Dopant-Level Circuits”, CHES 2014, pp.112-126, (2014-9).

[61] 浅井稔也, 旭健作, 汐崎充, 藤野毅, 吉川雅弥「暗号ハードウェア実装回路のサイドチャネル攻撃対策評価」電気学会論文誌C, Vol.134, No.12, pp.1767-1774, (2014-12)

[62] 野崎佑典, 旭健作, 藤野毅, 吉川雅弥「周波数領域における調節平文を用いたテンプレート攻撃とその評価」電気学会論文誌C, Vol.134, No.12, pp.1775-1782, (2014-12)

[63] Tsunato Nakai, Mitsuru Shiozaki, Takaya Kubota and Takeshi Fujino, “Side Channel Attacks on 64-bit Lightweight Block Ciphers—PRESENT, TWINE, and Piccolo,” Nonlinear Circuits, Communications and Signal Processing (NCSP) (2015-3)

[64] Daiki Tsutsumi, Tsunato Nakai, Mitsuru Shiozaki, Takaya Kubota and Takeshi Fujino, “Power Analysis Attacks on AES using RSM Countermeasure,” Nonlinear Circuits, Communications and Signal Processing (NCSP) (2015-3)

[65] M.Yoshikawa, T.Asai, Y.Nozaki, R.Matsuhisa, K.Asahi, "Method of Estimating Side-Channel Waveforms Using Profiling", Proc. of ISCA 30th International Conference on Computers and Their Applications, pp.57-62, (2015-3)

(2)その他の著作物(総説、書籍など)

(3)国際学会発表及び主要な国内学会発表

① 招待講演　　(国内会議　7 件、国際会議　1 件)

〈国内〉

[1] 堀　洋平, “動的再構成システムの最新設計手法とセキュリティ”, 次世代リコンフィギャラブルハードウェア創造研究会 (JACORN), 2010 年 9 月.

[2] 佐藤 証, “IC カードにおけるセキュリティ評価の現状と取組み”, 日銀:第 22 回情報セキュリティ・セミナー, 2010 年 10 月 13 日.

[3] 藤野毅, 汐崎充, 吉川雅弥, “[招待講演]悪意ある攻撃から機密情報を守る耐タンパ LSI 設計手法”, ディペンダブルコンピューティング研究会(DC), 信学技報, Vol.111, No.2, DC2011-4, pp.17-22, 2011 年 4 月.

[4] 藤野毅, 古橋康太, 汐崎充, “[招待講演]耐タンパ LSI 設計技術 ～ 模倣品防止のための

物理複製不可能なデバイス”, 集積回路研究会(ICD), 信学技報, Vol.111, No.352, ICD2011-102, pp.13-18, 2011 年 12 月.

[5] 藤野毅, 汐崎充, 久保田貴也, 吉川雅弥“[招待講演]耐タンパ暗号回路のLSI設計手法”, リコンフィギャラブルシステム研究会(RECONF), 信学技報, Vol.112, No.203, RECONF2012-29, pp.31-36, 2012 年 9 月.

[6] 藤野 毅 “セキュリティーハードウエアの研究”, JASPAR 情報セキュリティ実証 WG 会議 (2013-12)

[7] 藤野 毅 “悪意ある攻撃に耐性のある車載向け認証システム”, 第 36 回 ISS スクエア水平ワークショップ(2014-5)

〈国際〉

[1] Yohei Hori (AIST), Tackling the Security Issues of FPGA Partial Reconfiguration with Physical Unclonable Function, The International Conference on Engineering of Reconfigurable Systems and Algorithms (ERSA 2012), Las Vegas, Nevada, USA, (2012-07)

② 口頭発表 （国内会議 105 件、国際会議 13 件）

〈国内〉

[1] 片下 敏宏, 堀 洋平, 佐藤 証, ”サイドチャネル攻撃対策手法の評価環境の構築”, 信学技報,vol. 109, no. 320, RECONF2009-46, pp. 31-36, 2009 年 12 月.

[2] 佐藤 弘季, 堀 洋平, 今井 秀樹, “SASEBO-GII 上の AES に対する相互情報量解析攻撃”, 暗号と情報セキュリティシンポジウム(SCIS2010), 1B2-1, 2010 年 1 月 19 日.

[3] 奥山 一樹, 小島 憲司, 岩井 克彦, 藤野 毅, “Domino-RSL 方式を用いて FPGA 実装された暗号回路に対する DPA 耐性検証”, 暗号と情報セキュリティシンポジウム(SCIS2010), 1B2-5,2010 年 1 月 19 日.

[4] 野口 正俊, 堀 洋平, 吉田 隆弘, 今井 秀樹, “電力解析攻撃の体系的な分類と比較について”, 暗号と情報セキュリティシンポジウム(SCIS2010), 3B1-1, 2010 年 1 月 21 日.

[5] 関 晃平, 堀 洋平, 今井 秀樹, “SASEBO-GII への PUF の実装及び評価”, 暗号と情報セキュリティシンポジウム(SCIS2010), 4F1-1, 2010 年 1 月 22 日.

[6] 片下 敏宏, 佐藤 証, 永田 真, 藤本 大介, 菊地 克弥, 仲川 博, 青柳 昌宏, “サイドチャネル標準シミュレーションモデル構築に向けた標準評価ボードの DPA 特性測定”,暗号と情報セキュリティシンポジウム(SCIS2010), 4B2-1, 2010 年 1 月 22 日.

[7] 黒川 悠一朗, 中西 愛, 藤野 毅, “共通鍵ブロック暗号回路の FPGA 上での小面積実装手法の検討”, 情報処理学会第 72 回全国大会, 3ZE-3, 2010 年 3 月 10 日.

[8] 山田 翔太, 國生 雄一, 西本 智広, 吉田 直之, 堀 遼平, 松本 直樹, 北森 達也, 藤野毅(立命館大), 吉川 雅弥(名城大), “ビアプログラマブルデバイス VPEX のロジックアレイブロックと配線アーキテクチャの検討”, 信学技報, vol. 109, no. 462, VLD2009-107, pp.

49-54, 2010 年 3 月 11 日.

[9] 堀　遼平, 國生　雄一, 西本　智広, 山田　翔太, 吉田　直之, 藤野　毅(立命館大), 吉川　雅弥(名城大), “ビアプログラマブルデバイスに最適な基本論理ゲートアーキテクチャの検討”, 信学技報, vol. 109, no. 462, VLD2009-108, pp. 55-60,　2010 年 3 月 11 日.

[10] 西本　智広, 北森　達也, 國生　雄一, 山田　翔太, 藤野　毅(立命館大), 吉川　雅弥(名城大), “ビアプログラマブルデバイス VPEX の配線遅延評価”, 信学技報, vol. 109, no. 462, VLD2009-109, pp. 61-66,　2010 年 3 月 11 日.

[11]田口　飛鳥, 堀　洋平, 今井　秀樹, "サイドチャネル攻撃標準評価ボードを用いた CPA と MIA の比較評価",電子情報処理学会　技術報告　Vol.109, No.444, ISEC2009-110,pp.199-204, 2010.

[12] 勝部真人, 吉川雅弥“暗号回路の　FPGA　実装とその評価”, システム制御情報学会研究発表会講演論文集, pp.103-104, 2010 年 5 月

[13] 古橋康太, 汐崎　充, 福島照理, 村山貴彦, 藤野　毅, “物理複製防止デバイスアービター PUF　の設計および測定評価”, 電子情報通信学会, 信学技報, VLD2010-44,　pp.13-18, 2010 年 9 月

[14] 堀洋平, 吉田隆弘, 片下敏宏, 佐藤証, “FPGA 上の Arbiter PUF の定量的評価”, リコンフィギャラブルシステム研究会, 信学技報, vol.110, no.204, RECONF2010-37, pp.115-120, 2010 年 9 月

[15] 岩井克彦, 小島憲司, 佐野真規, 汐崎　充, 藤野　毅, “Domino-RSL　方式を用いた Simplified-DES 暗号回路の試作および DPA 耐性評価”, コンピュータ・セキュリティ・シンポジウム(CSS)論文集, pp.25-30, 2010 年 10 月

[16] 堀　遼平, 北森達也, 上岡泰輔, 藤野　毅, 吉川雅弥,　“ビアプログラマブルストラクチャード ASIC・VPEX　の新アーキテクチャ提案と性能評価”,　信学技報, ICD2010-91,　pp.13-18, 2010 年 11 月

[17] 浅井稔也,　吉川雅弥,　“FPGA　への暗号回路実装方法の検討と電力差分解析に対する耐性評価”,　第 53 回自動制御連合講演会論文集, pp.1124-1127, 2010 年 11 月

[18] 片下敏宏,　堀　洋平, 佐藤　証,　“近磁界測定によるサイドチャネル評価実験”,　デザインガイア 2010 —VLSI 設計の新しい大地—, RECONF-51, 2010 年 12 月

[19] 堀洋平,　吉田隆弘,　片下敏宏, 佐藤証, “確率密度関数の推定法と MIA 成功率に関する一考察”,　デザインガイア 2010 —VLSI 設計の新しい大地—, RECONF-53, 2010 年 12 月

[20] 姜　玄浩,　堀　洋平,　片下敏宏,　佐藤　証, “シフト事後処理を用いた PUF 基盤認証システムの精度評価”,　デザインガイア 2010 —VLSI 設計の新しい大地—, RECONF-54, 2010 年 12 月

[21] 福島照理, 汐崎　充, 古橋康太, 村山貴彦, 藤野　毅, “アービターPUF で生成した固有 ID の環境安定性の実チップ評価”, 暗号と情報セキュリティシンポジウム(SCIS)論文集　2D2-2, 2011 年 1 月

[22] 古橋康太, 汐崎　充, 村山貴彦, 福島照理, 藤野　毅, “生成 ID のユニーク性を高めた遅延時間差検出型アービターPUF の設計と評価”, 暗号と情報セキュリティシンポジウム(SCIS)論文集 2D2-3, 2011 年 1 月

[23] 小島憲司, 岩井克彦, 汐崎　充, 藤野　毅, “ドミノRSL方式を用いたDES暗号回路におけるアーリープロパゲーション効果によるDPAリークの評価”, 暗号と情報セキュリティシンポジウム(SCIS)論文集 2D4-2, 2011 年 1 月.

[24] 岩井克彦, 汐崎　充, 小島憲司, 浅川俊介, 藤野　毅, “Domino-RSL 方式を用いた DES 暗号回路の設計・試作および DPA 耐性評価”, 暗号と情報セキュリティシンポジウム(SCIS)論文集 2D4-3, 2011 年 1 月.

[25] 吉川弘起, 黒川悠一朗, 本田　弘, 熊木武志, 藤野　毅, “超並列 SIMD プロセッサ MX-1 を用いた AES 暗号の高速処理実装”, 暗号と情報セキュリティシンポジウム(SCIS)論文集 3D1-1, 2011 年 1 月

[26] 浅井稔也, 吉川雅弥“上流設計における暗号ハードウェアの電力解析シミュレーション手法”, 暗号と情報セキュリティシンポジウム講演論文集, 1D1-4, pp.1-6, 2011 年 1 月

[27] 佐藤隆亮, 吉川雅弥“AES の S-Box 構成の違いによるサイドチャネル攻撃の耐性評価”, 情報処理学会全国大会講演論文集, No.3, pp.475-476, 2011 年 3 月

[28] 松島大祐, 吉川雅弥“共通鍵暗号の FPGA における CPA・DPA の耐性評価”, 情報処理学会全国大会講演論文集, No.3, pp.477-478, 2011 年 3 月

[29] 浅井稔也, 吉川雅弥“改良リングオシレータPUFのFPGA実装とその評価”, 電子情報通信学会, 信学技報, Vol.110, No.439, CAS2010-131, pp.173-178, 2011 年 3 月

[30] 岩井克彦, 小島憲司, 汐崎　充, 浅川俊介, 藤野　毅, “Domino-RSL 方式を用いた DPA 耐性を持つDES暗号回路の設計試作と安全性評価”, 信学技報, VLD2010-126, pp.57-62, 2011 年 3 月

[31] 村山貴彦, 汐崎　充, 古橋康太, 福島照理, 藤野　毅, “遅延時間差検出型アービターPUF によるセレクタ遅延時間測定評価”, 信学技報, VLD2010-127, pp.63-68, 2011 年 3 月

[32] 熊木武志, 黒川悠一朗, 藤野　毅, “超小型組込みボードを用いた暗号処理の並列化に関する研究”, 信学技報, CPSY2010-79, pp.279-284, 2011 年 3 月

[33] 松島大祐, 吉川雅弥「電力解析攻撃におけるハミング距離と選択関数に関する耐性評価」, 第 55 回システム制御情報学会研究発表講演会論文集, pp.565-566, 2011 年 5 月

[34] 佐藤隆亮, 吉川雅弥「AES 暗号の様々な FPGA 実装に対する評価と検討」, 第 55 回システム制御情報学会研究発表講演会論文集, pp.567-568, 2011 年 5 月

[35] 堀洋平, 姜玄浩, 片下敏宏, 佐藤証, “物理特性を用いた LSI の真贋判定法”, マルチメディア,分散,協調とモバイルシンポジウム (DICOMO2011), pp.1296-1300, 2011 年 7 月

[36] 小野みどり, 吉川雅弥「偶発的なフォールトの解析可能性に関する検討」, 電気関係学会東海支部連合大会講演集, p.F5-3, 2011 年 9 月

[37] 浅井稔也, 吉川雅弥「電力解析攻撃に対する事前評価手法」, 電気関係学会東海支部連合大会講演集, p.F5-4, 2011 年 9 月

[38] 佐藤隆亮, 吉川雅弥「周波数領域での電力解析攻撃に関する一考察」, 電気関係学会東海支部連合大会講演集, p.F5-5, 2011 年 9 月

[39] 松島大祐, 吉川雅弥「FPGA における組込型相関電力解析の一考察」, 電気関係学会東海支部連合大会講演集, p.F5-6,2011 年 9 月

[40] 村山貴彦, 汐崎充, 古橋康太, 藤野毅, “TDC を用いた RG-DTM PUF の検討”, デザインガイア 2011, 信学技報, Vol.111, No.324, VLD2011-52, pp.1-6, 2011 年 11 月

[41] Anh-Tuan Hoang and Takeshi Fujino, “Hybrid Masking AES Using Dual-Rail Memory Against High-Order Side-Channel Attack”, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2012 年 1 月

[42] 岩井克彦, 柴谷恵, 弘田勝則, 汐崎充, 藤野毅, “ドミノ RSL 方式 DES 暗号回路に対する DPA 攻撃脆弱性評価と対策法の提案”, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2012 年 1 月

[43] 古橋康太, 汐崎充, 村山貴彦, 藤野毅, “遅延時間差検出型アービターPUF の設計に関する一考察”, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2012 年 1 月

[44] 伊藤弘樹, 汐崎充, Ahn Tuan Hoang, 藤野毅, “AES 暗号回路における耐タンパ性検証効率化手法の検討”, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2012 年 1 月

[45] 岡本卓朗, 汐崎充, 古橋康太, 藤野毅, “遅延時間差検出型アービターPUF を用いたデバイス固有乱数生成器”, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2012 年 1 月

[46] 小川昂佑, 汐崎充, 古橋康太, 藤野毅, “遅延時間差検出型アービター PUF の機械学習を用いた攻撃耐性評価”, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2012 年 1 月

[47] 橋本祐樹, 岩井克彦, 汐崎充, 浅川俊介, 鵜飼慎太郎, 藤野毅, “Dual-Rail RSL メモリ方式を適用した AES 回路の設計および DPA 耐性評価”, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2012 年 1 月

[48] 片下敏宏, 堀洋平, 佐藤証, “電力測定機能改良の暗号 LSI 用ボード SASEBO-RII とその評価”, 暗号と情報セキュリティシンポジウム(SCIS2012),2012 年 1 月

[49] 佐藤隆亮, 松島大祐, 吉川雅弥「電力解析攻撃に対する供給電源の影響に関する一考察」, システム制御情報学会若手研究発表会講演論文集 2012 年 1 月

[50] 佐藤隆亮, 松島大祐, 吉川雅弥「部分鍵推定を利用したハイブリッド電力解析手法とその評価」, 暗号と情報セキュリティシンポジウム講演論文集, 1D1-4, pp.1-6, 2012 年 1 月

[51] 浅井稔也, 吉川雅弥「ゲートレベル設計工程における電力解析耐性の脆弱性検証手法」, 暗号と情報セキュリティシンポジウム講演論文集, 1D1-4, pp.1-6, 2012 年 1 月

[52] 小野みどり, 吉川雅弥「複数エラーの差分推定に基づくフォールト解析」, 暗号と情報セキュリティシンポジウム講演論文集, 1D1-4, pp.1-6, 2012 年 1 月

[53] 鈴木大輔,清水孝一,鶴丸豊広,菅原健,汐崎充,藤野毅 ``グリッチ PUF を用いた鍵生成", SCIS2012, 暗号と情報セキュリティシンポジウム(SCIS)論文集、2012 年 1 月

[54] 菅原健,鈴木大輔`` Fault Sensitivity Analysis のための回路シミュレーション", SCIS2012, 暗号と情報セキュリティシンポジウム(SCIS)論文集、2012 年 1 月

[55] 佐伯稔, 菅原健,鈴木大輔, ``オープンソース CPU のサイドチャネル評価, 暗号と情報セキュリティシンポジウム(SCIS)論文集 2012 年 1 月

[56] 柴谷恵, 岩井克彦, 橋本祐樹, 汐崎充, 浅川俊介, 藤野毅, "Dual-Rail RSL メモリ方式を用いた耐タンパ DES 暗号回路の設計", VLSI 設計技術研究会(VLD), 2012 年 3 月.

[57] 柴谷恵, 岩井克彦, 汐崎充, 藤野毅, "2線 RSL メモリ方式を用いた耐タンパ暗号回路設計手法～CLEFIA 暗号への適用と面積評価～", 回路とシステムワークショップ, pp.166-171, 2012 年 7 月.

[58] 堀洋平, 片下敏宏, 姜玄浩, 佐藤証「45nm プロセス FPGA 上の Physical Unclonable Function の特性評価」, マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO2012), pp.1928-1933, 2012 年 7 月.

[59] Hyunho Kang, Yohei Hori, Toshihiro Katashita, and Akashi Satoh, "PUF Evaluation against Linear Programming Model on SASEBO-GII", マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO2012), pp.1947-1950, 2012 年 7 月.

[60] 橋本祐樹, 汐崎充, 久保田貴也, 藤野毅, "Dual-Rail RSL メモリ方式を利用したサイドチャネル攻撃耐性を有する AES 暗号回路", デザインガイア 2012, 信学技報, vol. 112, no. 324, ICD2012-84, pp. 43-48, 2012 年 11 月

[61] 望月陽平, 熊木武志, 吉川雅弥, 藤野毅, "トリプル DES 回路に組み込まれたハードウェアトロイの試作とその検知手法の検討", デザインガイア 2012, 信学技報, vol. 112, no. 322, CPSY2012-53, pp.33-38, 2012 年 11 月

[62] 後藤輝, 吉川雅弥「ハイブリッド方式を用いたフォールト解析とその耐性評価」情報学ワークショップ講演論文集, pp.57-60(2012-12)

[63] 谷口雅人, 汐崎充, 村山貴彦, 久保博嗣, 藤野毅, "物理的複製不可能関数(PUF)デバイスにおけるレスポンスの再現性向上のための軟判定 Fuzzy Extractor の検討", 情報理論研究会 (IT), 信学技報, vol. 112, no. 382, IT2012-52, pp. 19-24, 2013 年 1 月.

[64] 鵜飼慎太郎, HOANG Anh-Tuan, 汐崎充, 浅川俊介, 橋本祐樹, 藤野 毅, "耐タンパ性向上のための乗算マスクと Dual-Rail RSL メモリ方式を用いた AES 暗号回路の設計", 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2013 年 1 月

[65] 伊藤弘樹, 汐崎充, 藤野 毅, "AES 暗号回路の設計・評価を効率的に行うサイドチャネル攻撃耐性検証法の一考察", 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2013 年 1 月

[66] 小川昂佑, 汐崎充, 藤野 毅, "機械学習による遅延時間差検出型アービター PUF モデルを用いた認証方式", 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2013 年 1 月

[67] 寺村匡弘, 汐崎 充, 岡本 卓朗, 村山 貴彦, 藤野 毅, “認証と乱数生成利用のための遅延時間差検出型アービターPUF の最適化手法”, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2013 年 1 月

[68] 中井綱人, 汐崎 充, 藤野 毅, “電力・電磁波解析攻撃におけるオンチップ・キャパシタの影響評価”, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2013 年 1 月

[69] Hyunho Kang, Yohei Hori, Toshihiro Katashita, Manabu Hagiwara, “The Implementation of Fuzzy Extractor is Not Hard to Do: An Approach Using PUF Data,” 暗号と情報セキュリティシンポジウム(SCIS2013), 2013 年 1 月

[70] 伊左次 優太, 堀 洋平, 今井 秀樹, “FPGA 上のサイドチャネル攻撃対策済み AES に対する MIA の有効性評価 FPGA 上のサイドチャネル攻撃対策済み AES に対する MIA の有効性評価,” 情報と暗号セキュリティシンポジウム (SCIS2013), 2013 年 1 月

[71] 後藤輝, 吉川雅弥「複数解析手法を用いた故障利用解析に対する耐性評価」, システム制御情報学会若手研究会講演論文集, pp.3-4(2013-1)

[72] 浅井稔也, 吉川雅弥「イベントモデルシミュレーションによるサイドチャネル情報取得の効率化」, 暗号と情報セキュリティシンポジウム講演論文集, 1E1-1, pp.1-6, (2013-1)

[73] 後藤輝, 吉川雅弥「故障確率を考慮した階層型フォールト解析とその実装評価」, 電子情報通信学会, 信学技報, vol.112, no.451, VLD2012-160, pp.135-140(2013-3)

[74] 浅井 稔也, 吉川 雅弥「暗号処理 LSI 内部クロックの周波数及びスキュー可変機構による耐タンパ性改善検討」, LSI とシステムのワークショップ 2013 講演論文集, pp.252-254, (2013-5)

[75] 堀 洋平, 片下 敏宏, 古原 和邦, “Kintex-7 FPGA 上の Physical Unclonable Function の特性評価, ” 信学技報, RECONF2013-17, pp.91-96, 2013. (2013.5)

[76] 浅井稔也, 吉川雅弥「FDTD 法を用いた暗号サイドチャネルリークの設計評価手法」電子情報通信学会, 信学技報, vol.113, no.217, ISEC2013-51, pp.1-7(2013-9)

[77] 鵜飼慎太郎, 中井綱人, 北村俊樹, 久保田貴也, 汐崎充, 藤野毅, “耐タンパ性向上のための Hybrid Masking Dual-Rail ROM を用いた AES 暗号回路の性能評価”, デザインガイア 2013(ICD), 2013 年 11 月

[78] 西村隆志, 菅谷周平, 竹内章浩, 汐崎充, 藤野毅, “サイドチャネル攻撃耐性を持つ IO-Masked Dual-Rail ROM に統合可能な PUF 回路の検討と設計”, デザインガイア 2013(ICD), 2013 年 11 月

[79] 菅谷周平, 西村隆志, 竹内章浩, 汐崎 充, 藤野 毅, “サイドチャネル攻撃耐性を持つ IO-Masked Dual-Rail ROM のデータ読み出し遅延差を用いた PUF の検討と設計”, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2014 年 1 月

[80] 竹内章浩, 谷口雅人, 汐崎 充, 藤野 毅, “PUF の環境変化も考慮した鍵生成システムの実装評価”, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2014 年 1 月

[81] 柴谷恵, 汐崎 充, 中井綱人, 藤野 毅, “IO-masked dual-rail ROM の EM リーク低減手

法", 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2014 年 1 月

[82] 浅井稔也, 吉川雅弥「設計段階での暗号サイドチャネルリークの解析と対策」, 暗号と情報セキュリティシンポジウム講演論文集, 2A3-1, pp.1-8, (2014-1)

[83] 清水孝一, 鈴木大輔, 菅原健, "センサーと PUF の連携について", 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2014 年 1 月

[84] 菅原健, 鈴木大輔, 佐伯稔, "電磁界計測に基づく RSA の内部コリジョン攻撃", 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2014 年 1 月

[85] 野崎佑典, 吉川雅弥「周波数領域におけるテンプレート攻撃とその耐性評価」, 電子情報通信学会, 信学技報, vol.113, no.498, DC2013-107, pp.307-312, 2014 年 3 月.

[86] 中野将志, 鵜飼慎太郎, 柴谷恵, 久保田貴也, 汐﨑充, 藤野毅,「サイドチャネル攻撃対策 AES 暗号と PUF 技術を用いた車載向け耐タンパ認証システムの設計と実装」, 電子情報通信学会, 信学技報, vol.113, no.497, DC2013-93, pp.139-144, 2014 年 3 月.

[87] 野崎佑典, 吉川雅弥「周波数領域におけるテンプレート攻撃とその耐性評価」, 電子情報通信学会, 信学技報, vol.113, no.498, DC2013-107, pp.307-312, 2014 年 3 月.

[88] 野崎佑典, 吉川雅弥,「秘密分散法をベースとした機械学習攻撃耐性のある PUFID の生成手法」, 電子情報通信学会, 信学技報, IEICE-VLD 114(123), pp.225-230, 2014 年 7 月.

[89] 野崎佑典, 吉川雅弥,「PUF の数学的複製可能性について」, 第 37 回東海ファジィ研究会講演論文集, pp.17-20, 2014 年 8 月.

[90] 野崎佑典, 吉川雅弥, "CAN 通信の暗号化に関する検討", 平成 26 年度 電気・電子・情報関係学会東海支部連合大会, O4-5, 2014 年 9 月.

[91] 野崎佑典, 吉川雅弥「軽量暗号の耐タンパ性に関する基本検討」第 12 回情報学ワークショップ WiNF2014 講演論文集, pp.152-157, 2014 年 11 月

[92] 田中将貴, 中井綱人, 汐﨑充, 久保田貴也, 藤野毅,「サイドチャネル攻撃における他の回路が発生するノイズの定量的評価」, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2015 年 1 月.

[93] 堤大樹, 中井綱人, 汐﨑充, 久保田貴也, 藤野毅,「RSM 対策 AES 暗号回路における電力解析攻撃」, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2015 年 1 月.

[94] 中野将志, 汐﨑充, 藤野毅,「レーザフォールト攻撃に耐性のある論理ゲートの基礎検討と実験評価」, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2015 年 1 月.

[95] 中井綱人, 汐﨑充, 久保田貴也, 菅原健, 鈴木大輔, 藤野毅,「レジスタに値を保持しているだけで生じる静的なサイドチャネルリーク」, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2015 年 1 月.

[96] 久保田貴也, 中野将志, 倉地亮, 本田晋也, 汐崎充, 藤野毅,「久保田貴也, 中野将志, 倉地亮, 本田晋也, 汐崎充, 藤野毅,「車載 CAN 通信暗号化デモシステムの構築とサイドチ

ャネル攻撃評価」, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2015 年 1 月.

[97] 竹内章浩, 西村隆志, 汐﨑充, 藤野毅, 「MDR-ROM を用いてサイドチャネル攻撃対策 AES と PUF を実現した鍵生成 LSI の実装評価」, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2015 年 1 月.

[98] 野崎佑典, 吉川雅弥「TWINE に対するエラー値を考慮したフォールト攻撃」暗号と情報セキュリティシンポジウム(SCIS)論文集, 2015 年 1 月

[99] 浅井稔也, 吉川雅弥「ハードウェアのプロファイリングによるサイドチャネル波形の予測」暗号と情報セキュリティシンポジウム(SCIS)論文集, 2015 年 1 月

[100] 野原康平, 吉川雅弥「Piccolo に対する階層的なフォールト攻撃手法 」暗号と情報セキュリティシンポジウム(SCIS)論文集, 2015 年 1 月

[101] 菅原健, 鈴木大輔, 藤井亮一, 田和茂朗, 堀遼平, 汐﨑充, 藤野毅, 「ドーパントを利用した回路カモフラージュのリバースエンジニアリング 」, 暗号と情報セキュリティシンポジウム(SCIS)論文集, 2015 年 1 月.

[102] 野崎佑典, 吉川雅弥「周波数領域での軽量暗号 TWINE に対する電力解析手法」, 電子情報通信学会技術報告, CAS2014-128, pp.49-54, 2015 年 2 月

[103] 松久僚真, 宮本智行, 吉川雅弥「PRESENT に対する統計的なフォールト解析攻撃手法」, 電子情報通信学会技術報告, CAS2014-129, pp.55-60 , 2015 年 2 月

[104] 中野将志, 久保田貴也, 汐﨑充, 藤野毅, 「車載 CAN 通信の暗号化とリプレイ攻撃対策手法の実装評価」, 組込み技術とネットワークに関するワークショップ(ETNET), 2015 年 3 月.

[105] 野崎 佑典, 野原 康平, 松久 僚真, 旭 健作, 吉川 雅弥「PRINCE に対する統計処理を用いた階層的フォールト解析とその評価」, 情報処理学会研究報告, Vol.2015-102, No.13, pp.1-6(2015-3)

〈国際〉

[1] Anh-Tuan Hoang, Masaya Yoshikawa and Takeshi Fujino, “AES Side Channel Attack Using Last to First Rounds Hamming Distance”, IEICE Technical Report, Integrated Circuits and Devices in Vietnam (ICDV), (2010-8).

[2] M.Yoshikawa, T.Asai,"Vulnerability evaluation method considering power supply environment for power analysis attacks", Proc. of International Conference on Advancements in Information Technology(IJFCC), vol.1, no.2, pp.121-123(2012-06)

[3] M.Yoshikawa, T.Asai, "Evaluation technique for cryptography circuits with measures against power analysis attacks", Lecture Notes in Information Engineering, vol.25, pp.76-81, (2012-06)

[4] Yohei Hori, "Side-channel attack evaluation of AES implementations on SASEBO-GIII", Joint Workshop on Cryptographic Algorithm and its Application (JWCAA 2012), Tokyo, (2012-08)

[5] T.Asai, M.Yoshikawa, "Efficient acquisition technique of side-channel information using event-model simulation", Proc. of International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADO), S-5b, (2013-3)

[6] M.Yoshikawa, T.Asai, "Tamper Resistance Verification Method for Consumer Security Products", Proc. of Computational Science & Computational Intelligence, pp.30-33 (2014-3)

[7] M.Yoshikawa, H.Goto, "Analysis of Operation Errors for Fault Injection Attack", International Journal of Signal Processing System, Vol.2, No.1, pp.74-77, 2014-5

[8] M.Yoshikawa, T.Asai, "Tamper-resistance evaluation for cryptographic side channel leakage at design stage", Proc.of International Conference on Emerging Trends in Engineering and Technology (ICETET'2014), pp.45-49, 2014-5.

[9] M.Yoshikawa, H.Goto, K.Asahi, "Error Value Driven Fault Analysis Attack", Proc. of 014 15th IEEE/ACIS SNPD, pp.101-104, 2014-6.

[10] S.Kiryu, K.Asahi, M.Yoshikawa, "Modeling and Attack for 4-MUXs based PUF", Proc. of 2014 World Congress in Computer Science, Computer Engineering & Applied Computing, pp.163-166, 2014-7.

[11] M.Yoshikawa, H.Goto, K.Nohara, K.Asahi, "Countermeasure for fault analysis attack", Proc. of 20th ISSAT International Conference on Reliability & Quality in Design, pp.254-257, 2014-8

[12] S.Kiryu, K.Asahi, M.Yoshikawa, "Vulnerability evaluation of multiplexing PUF for SVM attacks", Progress in Systems Engineering(Proc. of 23rd International Conference oc System Engineering), Vol.1089, pp.205-210, 2014-8.

[13] Y.Nozaki, K.Asahi, M.Yoshikawa, "PUF ID Generation Method for Modeling Attacks", IEEE 3rd Global Conference on Consumer Electronics (GCCE 2014), pp.393-394, 2014-10.

③ ポスター発表　　（国内会議　16 件、国際会議　5 件）

〈国内〉

[1] 片下 敏宏, 堀 洋平, 佐藤 証, ”サイドチャネル攻撃対策手法の評価環境の構築”, デザインガイア 2009, 2009 年 12 月 3 日

[2] 岩井克彦,小島憲司,佐野真規,汐崎　充,藤野　毅, “Domino-RSL 方式を用いた Simplified-DES 暗号回路設計と SPICE シミュレーションによる DPA 耐性の評価”, LSI とシステムのワークショップ 2010　学生部門9番, 2010 年 5 月 17 日

[3] 古橋康太,汐崎　充,藤野　毅(立命館大),
“物理複製防止デバイス PUF の設計とシミュレーションによる性能評価” , LSI とシステムのワークショップ 2010　学生部門 10 番, 2010 年 5 月 17 日

[4] 伊藤弘樹, 汐崎充, 濱崎慎也, 岩井克彦, 藤野毅,
“非接触 IC カードにおける電力転送環境の検討と構築”, LSI とシステムのワークショップ

2011, pp.287-289, 2011 年 5 月

[5] 岡本卓郎, 古橋康太, 福島照理, 村山貴彦, 汐崎充, 藤野毅,
“複製防止デバイス PUF を用いた認証システムの FPGA ボード実装と評価”, LSI とシステムのワークショップ 2011, pp.213-215, 2011 年 5 月

[6] 橋本裕樹, 汐崎充, 岩井克彦, 藤野毅,
“DPA 耐性をもつ AES 暗号回路実装のためのメモリ方式 S-box 回路の設計”, LSI とシステムのワークショップ 2011, pp.207-209, 2011 年 5 月

[7] 小川昂佑, 岩井克彦, 汐崎充, 藤野毅,
“ドミノ RSL 方式を用いた DPA 対策回路におけるフォールト攻撃方法と対策回路の検討”, LSI とシステムのワークショップ 2011, pp.269-271, 2011 年 5 月

[8] 浅井稔也, 吉川雅弥「設計工程における暗号 LSI とその周辺回路へのサイドチャネル攻撃に対する耐性評価手法」, LSI とシステムのワークショップ講演論文集, pp.293-295, 2012 年 5 月

[9] 菅谷 周平,汐崎 充,藤野 毅, “PUF 用途向けグリッチ生成及び抽出回路の検討”, LSI とシステムのワークショップ 2012, pp.177 -179, 2012 年 5 月

[10] 谷口 雅人, “PUF から一意な鍵情報を生成するための Fuzzy Extractor 回路の設計と評価”, LSI とシステムのワークショップ 2012, pp.195-197, 2012 年 5 月

[11] 鵜飼 慎太郎,橋本 祐樹,汐崎 充,藤野 毅, “耐タンパ AES 暗号回路のサイドチャネル攻撃耐性評価”, LSI とシステムのワークショップ 2012, pp.234-236, 2012 年 5 月

[12] 西村隆志, 小川昂佑, 岡本卓朗, 寺村匡弘, 汐崎充, 藤野毅, ”機械学習による遅延時間差検出型アービターPUF モデルを用いたチップ認証”, LSI とシステムのワークショップ 2013, pp.175-177, 2013 年 5 月

[13] 竹内章浩, 久保田貴也, 汐崎充, 藤野毅, ”AES 暗号回路に対するテンプレートを用いたサイドチャネル攻撃評価”, LSI とシステムのワークショップ 2013, pp.178-180, 2013 年 5 月

[14] 堤大樹, 堀遼平, 伊藤弘樹, 汐崎充, 久保田貴也, 藤野毅, ”サイドチャネル攻撃対策回路検証用消費電力シミュレーションツールの検討”, LSI とシステムのワークショップ 2013, pp.187-189, 2013 年 5 月

[15] 久保田貴也, 汐崎充, 藤野毅, ”暗号モジュールにおけるサイドチャネル攻撃耐性の事前評価のための検定(統計的手法)を用いた一手法”, LSI とシステムのワークショップ 2013, pp.258-260, 2013 年 5 月

[16] 中野将志, 久保田貴也, 汐崎充, 藤野毅, ”暗号回路に対するレーザフォールト攻撃の対策手法の検討”, LSI とシステムのワークショップ 2014, PS-3, 2014 年 5 月

〈国際〉

[1] Kota Furuhashi, Mitsuru Shiozaki, Takahiko Murayama, Kosuke Ogawa and Takeshi Fujino, “Uniqueness and Stability Evaluation of RG-DTM PUF”, Workshop on Cryptographic Hardware and Embedded Systems (CHES), September 2011.

[2] Toshihiro Katashita, Yohei Hori, Akihiko Sasaki, and Akashi Satoh, "New SCA Experimental Platform SASEBO-GIII", International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2012), Leuven, Belgium, (2012-09)

[3] Hiroki Ito, Mitsuru Shiozaki, Anh-Tuan Hoang, Takeshi Fujino, "Efficient DPA-Resistance Verification Method with Smaller Number of Power Traces on AES Cryptographic Circuit", Euromicro Conference on Digital System Design (DSD), pp. 735-738, (2012-09)

[4] Mitsuru Shiozaki, Tsunato Nakai, Takaya Kubota and Takeshi Fujino, "Countermeasures against Electromagnetic Leaks on PA-Resistant Dual-Rail RSL Memory AES," Cryptographic Hardware and Embedded Systems (CHES) (2013-8)

[5] Toshihiro Katashita, Akihiko Sasaki, and Yohei Hori, "A Novel Smart Card Development Platform for Evaluating Physical Attacks and PUFs," IEEE GCCE2013 (2013.10)

(4)知財出願

① 国内出願 (9 件)

[1]
発明の名称:認証処理方法及び装置
発明者:独立行政法人産業技術総合研究所
出願人:佐藤 証、片下 敏宏
出願日:2010 年 3 月 24 日
出願番号:特願 2010-067237

[2]
発明の名称:耐タンパ性メモリ集積回路およびそれを利用した暗号回路
発明者:藤野 毅
出願人:学校法人立命館,
出願日:2010 年 7 月 28 日
出願番号:PCT/JP2010/062689

[3]
発明の名称:情報処理装置, 情報処理方法及びそのプログラム
発明者:浅井稔也, 吉川雅弥
出願人:学校法人 名城大学
出願日:2011 年 8 月 18 日
出願番号:特願 2011-178732

[4]
発明の名称:情報セキュリティシステム, ホスト, デバイス, その制御方法及びそのプログラム
発明者:浅井稔也, 吉川雅弥
出願人:学校法人 名城大学
出願日:2011 年 8 月 26 日
出願番号:特願 2011-184503

[5]

発明の名称:デバイス固有情報生成装置及びデバイス固有情報生成方法
発明者:清水孝一,
出願人:三菱電機,
出願日:2012 年 1 月
出願番号:PCT/JP2011/079820,（国内 1 件、海外 7 か国　米、中、韓、台、英、独、仏）
　　海外 7 カ国出願

[6]
発明の名称:耐タンパ性評価方法, そのプログラム及び耐タンパ性評価装置
発明者:浅井稔也, 吉川雅弥
出願人:学校法人名城大学
出願日:2012 年 5 月 25 日
出願番号:特願 2012-119886

[7]
発明の名称:耐タンパメモリ方式
発明者:佐伯　稔
出願人:三菱電機
出願日:2013 年 4 月 22 日
出願番号:特願 2014-026932

[8]
発明の名称:デバイス固有情報生成装置及びデバイス固有情報生
発明者:堀洋平, 萩原学, 姜玄浩, 古原和邦, 片下敏宏
出願人:独立行政法人産業技術総合研究所
出願日:2014 年 2 月 14 日
出願番号:特願 2014-026932

[9]
発明の名称：デバイス固有情報の誤り率制御方法とデバイス固有情報の誤り率制御プログラム
発明者：堀洋平，古原和邦，片下敏宏，松井俊浩
出願人：独立行政法人産業技術総合研究所
出願日：2014 年 8 月 29 日
出願番号：特願 2014-175824

②　　海外出願（10 件）
[1]
発明の名称:デバイス固有情報生成装置及びデバイス固有情報生成方法
発明者:清水孝一,
出願人:三菱電機,
出願日:2012 年 1 月
出願番号:PCT/JP2011/079820（国内 1 件、海外 7 か国　米、中、韓、台、英、独、仏）
　　海外 7 カ国出願

[2]
発明の名称:デバイス固有情報生成装置及びデバイス固有情報生成方法
発明者:鈴木大輔
出願人:三菱電機,
出願日:2012 年 12 月

出願番号:PCT/JP2012/082081,（国内 1 件、海外 7 か国　米、中、韓、台、英、独、仏）
　　海外 7 カ国出願

[3]
発明の名称:Tamper Resistant Memory Integrated Circuit and Encryption Circuit Using Same
発明者:Takeshi Fujino
出願人:学校法人立命館,
出願日:2013 年 1 月 28 日
出願番号:13812628（米国出願）

[4]
発明の名称:統合セキュリティ装置および統合セキュリティ装置に用いられる信号処理方法
発明者:鈴木　大輔
出願人:三菱電機
出願日:2013 年 4 月 9 日
出願番号:102112458（TW）

[5]
発明の名称:機器真贋判定システムおよび機器真贋判定方法
発明者:鈴木　大輔
出願人:三菱電機
出願日:2013 年 5 月 15 日
出願番号:PCT/JP2013/063560

[6]
発明の名称:認証処理装置および認証処理方法
発明者:清水　孝一
出願人:三菱電機
出願日:2013 年 5 月 28 日
出願番号:PCT/JP2013/064747

[7]
発明の名称:半導体装置
発明者:菅原　健
出願人:三菱電機
出願日:2013 年 7 月 16 日
出願番号:PCT/JP2013/069320

[8]
発明の名称:機器真贋判定システムおよび機器真贋判定方法
発明者:鈴木　大輔
出願人:三菱電機
出願日:2013 年 9 月 24 日
出願番号:102134235（TW）

[9]
発明の名称:認証処理装置および認証処理方法
発明者:清水　孝一
出願人:三菱電機

出願日:2013 年 10 月 8 日
出願番号:102136281(TW)

[10]
発明の名称:半導体装置
発明者:菅原　健
出願人:三菱電機
出願日:2013 年 11 月 7 日
出願番号:102140422(TW)

(5)受賞・報道等
①　　受賞

[1] Best Paper Award 受賞
M.Yoshikawa, Y.Kokusyo, T.Fujino, “Placement Tool Dedicated for a Via-programmable Logic Device VPEX”, Proc. of 23rd International Conference on Computer Applications in Industry and Engineering, pp.21-25, 2010 年 11 月 8 日.

[2] Certificate of Merit 受賞
M.Yoshikawa, T.Asai, “High-Level Simulation for Side Channel Attacks”, Proc. of The International MultiConference of Engineers and Computer Scientists, Vol.2, pp.1565-1568, 2011 年 2011 年 3 月 16 日.

[4] IEEE SSCS Japan Chapter VDEC Design Award 受賞
古橋康太, “ユニーク性を改善した RG-DTM PUF”, Proc. of IEEE SSCS Japan Chapter VDEC Design Award, 2011 年 5 月 28 日.

[5] 国際会議 WCECS2011　Best paper award 受賞
M.Yoshikawa, T.Asai, "DPA Attacks Simulator against Cryptography System on Algorithm Design Phase", Proc. of World Congress on Engineering and Computer Science, Vol.1, pp.792-796,(2011-10)

[6] 優秀プレゼンテーション賞受賞
堀洋平, "45nm プロセス FPGA 上の Physical Unclonable Function の特性評価", マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO2012), (2012-07).

[7] 優秀論文賞受賞
堀洋平, 片下敏宏, 姜玄浩, 佐藤証, "45nm プロセス FPGA 上の Physical Unclonable Function の特性評価", マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO2012), (2012-08).

[8] Excellent Paper Award 受賞
Hyunho Kang, Yohei Hori, Akashi Satoh, "Performance Evaluation of the First Commercial PUF-embedded RFID", Proc. of IEEE Global Conference on Consumer Electronics (GCCE2012), (2012-10).

[9]平成 24 年電子情報通信学会論文賞　平成 24 年 1 月号(EA)
K. Shimizu, D. Suzuki, T. Kasuya, "Glitch PUF: Extracting Information from Usually Unwanted Glitches"
本プロジェクトで試作している Glitch PUF の方式提案論文が電子情報通信学会論文賞に

選出された.

[10]Outstanding Poster Award
"A Novel Smart Card Development Platform for Evaluating Physical Attacks and PUFs," Toshihiro Katashita, Akihiko Sasaki, and Yohei Hori, IEEE GCCE2013 (2013.10)

[11] Outstanding Paper Award
"Cryptographic Key Generation from PUF Data Using Efficient Fuzzy Extractors," Hyunho Kang, Yohei Hori, Toshihiro Katashita, Manabu Hagiwara, Keiichi Iwamura, ICACT 2014, (2014.2)

[12] 第 12 回情報学ワークショップ奨励賞 受賞
野崎佑典, 吉川雅弥,「軽量暗号の耐タンパ性に関する基本検討」2014 年 11 月

[13] 電子情報通信学会回路とシステム研究会学生優秀賞 受賞
野崎佑典, 吉川雅弥,「周波数領域での軽量暗号 TWINE に対する電力解析手法」
2015 年 2 月

② マスコミ(新聞・TV等)報道

[1] "暗号モジュールを評価 産総研が手法開発 IC カードの安全性向上" 日刊工業新聞,
2010 年 5 月 21 日.

[2] "三菱電機 IoTにらみ暗号技術 産業機械の悪用防止", 日経産業新聞[日経テレコン21]
2015 年 02 月 06 日 朝刊 6 面 3 段

[3] "三菱電機 立命館大 機器なりすまし防止 LSI個体差でID生成", 化学工業日報
2015 年 02 月 06 日 朝刊 8 面 2 段

[4] "三菱電機 立命館大学 LSI個体差から固有ID生成 IoT時代
に向けたセキュリティ技術", 電経新聞 2015 年 02 月 09 日 朝刊 2 面 4 段

[5] "三菱電機、立命館大学と開発 安全対策技術 IoT普及に備え", 日刊工業新聞
2015 年 02 月 12 日 朝刊 7 面 3 段

[6] "ニュースな科学＝ITはIoT時代に ネットに様々な機器を接続", 日本経済新聞
2015 年 02 月 20 日 朝刊 33 面 6 段 図

＜Web＞
[7] "三菱電機が「IoT」対応のセキュリティー技術を開発 LSIに"指紋"付与"
http://www.sankei.com/economy/news/150205/ecn1502050034-n1.html
産経ニュース(Web) - 2015 年 2 月 5 日

[8] "三菱電機と立命館、LSI ごとに固有 ID を生成して暗号化に利用するセキュリティー技術を開発"
http://www.zaikei.co.jp/article/20150206/234447.html
財経新聞(Web) - 2015 年 2 月 5 日

[9] "「LSI の指紋」を活用、IoT 機器の安全性を向上するセキュリティ技術"
http://eetimes.jp/ee/articles/1502/06/news032.html

EE Times Japan(Web) - 2015 年 2 月 5 日

[10] "三菱電機と立命館大が LSI の個体差を利用したセキュリティ技術を開発"
http://www.rbbtoday.com/article/2015/02/06/128137.html
RBB Today(Web) - 2015 年 2 月 5 日

[11] "三菱電機など、LSI の個体差から固有 ID を生成するセキュリティ技術を開発"
http://news.mynavi.jp/news/2015/02/05/373/
マイナビニュース(Web) - 2015 年 2 月 5 日

[12] "三菱電機、LSI の個体差を鍵として暗号化する技術を開発 - PC Watch"
http://pc.watch.impress.co.jp/docs/news/20150205_687089.html
PC Watch(Web) - 2015 年 2 月 5 日

[13] "LSI の個体差から「指紋」を生成し「IoT 暗号」実現、三菱電機が新技術"
http://cloud.watch.impress.co.jp/docs/news/20150206_687136.html
クラウド Watch(Web) - 2015 年 2 月 5 日

[14] "三菱、IoT 時代に備え、LSI の個体差を利用したセキュリティー技術を開発"
http://kaden.watch.impress.co.jp/docs/news/20150205_687051.html
家電 Watch(Web) - 2015 年 2 月 5 日

[15] "IC チップの「指紋」を IoT のセキュリティ基盤に使う、三菱電機が遅延ベースの PUF 技術を発表"
http://www.nikkeibp.co.jp/article/news/20150206/434605/
nikkei BPnet(Web) - 2015 年 2 月 6 日

[16] "三菱電機が IoT 向けのセキュリティ技術、LSI の個体差で生じる「指紋」を利用"
http://itpro.nikkeibp.co.jp/atcl/news/15/020500444/
ITpro(Web) - 2015 年 2 月 6 日

[17] "半導体製造時のばらつきを IoT セキュリティに生かす"
http://monoist.atmarkit.co.jp/mn/articles/1502/09/news021.html
@IT MONOist(Web) - 2015 年 2 月 8 日

[18] "三菱電機、IoT デバイス向けに LSI 組込型の暗号方式を開発"
http://it.impressbm.co.jp/articles/-/12042
IT Leaders(Web) - 2015 年 2 月 9 日

[19] "三菱電機など、LSI の個体差から個別 ID を生成するセキュリティー技術を開発"
http://ascii.jp/elem/000/000/976/976731/
ASCII.jp(Web) - 2015 年 2 月 9 日

[20] プレス発表
三菱電機、立命館大学、JST 「IoT 時代に向けたセキュリティー技術」を開発
LSI の個体差から指紋のような固有 ID を生成し、組み込み機器の安心・安全に貢献
※[2]～[19]に関連

③ その他

[1] SASEBO を用いたサイドチャネル攻撃の技術展示およびセミナー発表, 組込み総合技術展 Embedded Technology 2009, 2009 年 11 月 18～20 日, SASEBO, http://www.jasa.or.jp/et/

[2] NIST, “FIPS140-3 Security Requirements for Cryptographic Modules 2nd Draft,”, 2009 年 12 月 11 日. http://csrc.nist.gov/groups/ST/FIPS140_3/ (産総研がサイドチャネル攻撃の項目を担当している米国連邦標準の公開)

[3] “サイドチャネル攻撃標準評価ボード SASEBO によるサイドチャネル攻撃実験”, 暗号と情報セキュリティシンポジウム 2010 技術展示セッション, 2010 年 1 月 19 日

(6)成果展開事例、出口活動

①実用化に向けての展開

・産総研が開発した SASEBO-GIII, SASEBO-RII, ZUIHO, MiMICC は、企業に技術移転されて市販化されている。

・ISO/IEC 17825 から派生した、非侵襲撃攻撃に関する試験手法および キャリブレーション手法に関する新しい国際標準規格の策定において、産総研が CREST で開発したボードの利用を提案中

・ISO/IEC JTC 1/SC 27 において、PUF を用いた暗号鍵の生成方法について、フランスと共同で Study Period proposal を行い、標準化に向けた検討を開始。
産総研の坂根が Sylvain Guilley (仏) と共にラポーターを務めている。

§6 研究期間中の活動

6.1 主なワークショップ、シンポジウム、アウトリーチ等の活動

年月日	名称	場所	参加人数	概要
H22. 1.19	暗号と情報セキュリティシンポジウム(SCIS2010) 技術展示	サンポートホール高松	約 600	サイドチャネル攻撃評価環境のデモ展示
H22. 1.21	耐タンパ LSI 研究ミーティング	高松	10	研究グループ内での 2009 年度の研究まとめ
H22.5.14	RCIS Workshop 2010	秋葉原 UDX	約 100	産総研情報セキュリティ研究センター成果発表会. サイドチャネル攻撃評価プラットフォームのデモ展示
H23.9.30	International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2011)	東大寺総合文化ホール	約 300	サイドチャネル攻撃評価環境のデモ展示
H23.11.11	金沢工業大学特別講義	金沢工業大学	約 50	リコンフィギャラブルデバイスの応用とセキュリティ
H23.11.17	トッパン―立命・産総研交流ミーティング	横浜	12	PUF に関する技術討論
H24.1.31	暗号と情報セキュリティシンポジウム(SCIS2012)技術展示	金沢エクセルホテル東急	約 600	IC カードに対するサイドチャネル攻撃標準評価のデモ, 電磁波解析攻撃環境のデモ展示
H24.6.9	市民開放講座	名城大学	161	CREST での研究内容の紹介
H24.9.10	RISEC シンポジウム	日本科学未来館	約 270	産総研セキュアシステム研究部門のシンポジウム. サイドチャネル攻撃評価環境と PUF に関するデモとポスタ展示
H24.10.25-26	産総研オープンラボ	産総研	(約 4,200 (H23 年度実績))	企業・研究機関向け研究公開. "ハードウェアの安全性評価技術と偽造防止技術"を展示.
H25.10.31-11.1	産総研オープンラボ	産総研	約 4,000	企業・研究機関向け研究公開. "ハードウェアの安全性評価技術と偽造防止技術"を展示.
H26.3.13	RISEC シンポジウム	日本科学未来館	約 170	産総研セキュアシステム研究部門のシンポジウム. サイドチャネル攻撃評価環境と PUF に関するデモとポスタ展示