「ディペンダブル VLSI システムの基盤技術」
平成 21 年度採択研究代表者

H24 年度
実績報告

藤野　毅

立命館大学　理工学部・教授

耐タンパディペンダブル VLSI システムの開発・評価

§1. 研究の概要

1.1 チーム全体の研究の概要

(1) 本研究の背景と課題定義

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) 本研究の特徴

(1)耐タンパ性 LSI 設計プラットフォーム

当初計画では，「ドミノ RSL 方式を耐タンパ LSI 設計技術の中心技術」としており，実際に本方式を用いて，H22～23 年度に DES 暗号回路を LSI 実装したが，H23 年以降は攻撃に対する耐性や LSI 設計容易性，小チップ面積という観点で優れる「2線 RSL メモリ方式」を設計プラットフォームの中心技術に変更した．

中間評価時点で当初目標は，達成できた．特に消費電力を用いた攻撃で，未対策回路では 4000 波形で 128bit の暗号鍵をすべて特定できる環境で，100 万波形でも 8bit 以下の暗号鍵しか，特定できなかった．また，他機関で提案されている4方式に対するベンチマークを行い耐タンパ性，面積，消費電力での優位性も確認できた．（詳細は§3 成果1を参照ください）

(2)耐タンパ性能評価プラットフォーム

産総研が開発した，耐タンパ性能評価プラットホームの中心技術である SASEBO ボードは，当初計画通り普及が進み，多くのサイドチャネル攻撃の論文が SASEBO を使用・参照し，学会でのスタンダードとなるに至った．文献検索エンジンで約 240 件（Google Scholar，2012 年 9 月 7 日現在）のヒットがあり，韓国の ETRI による同様の評価環境 SCARF が約 70 件であることと比較して高い優位性を持っている．

SASEBO は CREST プロジェクトにおいて，技術的には，以下 A～C のように発展した．（詳細は§3 成果2を参照ください）

A. SASEBO-RII: 各種対策回路を搭載した多様な ASIC を低ノイズ・低価格で評価できるようにするため，ドーターボード方式を初めて採用した．ドーターボードの基板情報は Web 公開．本ボードを用いて，2線 RSL メモリ方式を含む各種攻撃対策回路 ASIC を高精度に評価をすることが可能になった．

B. 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．28nm という最新のプロセスでも電力解析攻撃が可能であることを実証するとともに，最先端プロセスでは電磁波解析攻撃が有効であることを確認．

C. ZUIHO: Spartan-3FPGA 搭載，教育用サイドチャネル攻撃評価ボードであり，学生などより多くの人に普

及させる.

(3)偽造 LSI を識別する PUF を用いたセキュリティシステム

研究計画当初は, PUF はまだ具体的提案となっていなかったが, 立命館大学では DTM 方式アービターPUF, 三菱電機ではグリッジ PUF を提案し, 180nm および 65nm でチップ試作を行ってユニーク性や環境安定性, 学習攻撃耐性の実チップ評価を行った. 立命館大学の DTM 方式アービターPUF は, 米国 Verayo 社のアービターPUF およびその改良型の XOR アービターPUF との比較実験を行い, チャレンジ―レスポンス方式の簡易認証でも, DTM アービター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. 三菱電機のグリッジ PUF では, SRAM を用いた PUF と誤り訂正技術で, 安定な鍵生成を行う技術で先行していたオランダ 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. (詳細は§3 成果5を参照ください) 産総研では, FPGA を用いて固有 ID を生成する Pseudo-LFSR PUF を提案するとともに, PUF の評価指標提案と評価ツールの作成をおこなった. (詳細は§3 成果6を参照ください)

(3) 本研究の達成目標

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.

①128bitAES 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.

②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.

③LSI 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)

(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.

①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.

②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.

③AES 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)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.

①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.
②PUF により生成された固有 ID を使用した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.

1．2 研究実施方法

(1) 本研究チーム全体の運営と取りまとめ方針

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)に関してはフォールト攻撃等の新しい攻撃手法の開発を三菱電機, 名城大が行う. また評価ボード, EM 評価ステージなどの耐タンパ性能評価プラットフォームの構築を産総研が行い, これらを使用して(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.

(1)耐タンパ性 LSI 設計プラットフォーム
①耐タンパ LSI 設計環境(立命館大, 名城大)
②耐タンパ性能評価プラットフォームを用いた耐タンパ LSI の評価(立命館大, 産総研)
③耐タンパ検証 CAD システム(名城大, 立命館大)
(2)耐タンパ性能評価プラットフォーム
①フォールト攻撃や侵襲攻撃等の新しい攻撃手法の評価実験(三菱電機・名城大)
②輻射電磁波を用いた差分電磁波解析(DEMA)攻撃環境と LSI 評価(産総研, 立命館大)
③セキュア SoC のシステムレベルサイドチャネル評価用 LSI 試作と耐タンパ性評価環境構築
(三菱電機, 立命館大)
(3)偽造 LSI を識別する PUF を用いたセキュリティシステム
①従来型 PUF 回路の問題点の把握と新型 PUF の実装と評価(立命館大, 三菱電機)
②PUF の性能評価手法と評価ツール作成およびセキュア動画再生システムの開発(産総研)
③PUF 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セキュリティーシステム
(三菱電機, 立命館大)

図1－1. 現在の研究実施体制

(2)研究グループの分担

1)「立命館大学」グループ(研究代表者グループ)

①本研究グループの研究課題、ならびに所属する研究チームの課題との関係

§1で述べたように本研究チーム全体としては, IC カード等に搭載される機密情報を保管しているセキュリティーLSI のディペンダビリティーの向上が目標である. 立命館大学Gではこの目的を達成するため, 能動的な攻撃者によるセキュリティーLSI へのサイドチャネル攻撃に対抗できる耐タンパ LSI の設計環境, および実際の暗号回路搭載システムを構築することが第1の研究課題となる. さらに窃取した機密情報を悪用するためのセキュリティーLSI の偽造に関しても対策を講じることが第2の研究課題である.

立命館大学Gは, 上記第1のサイドチャネル攻撃に対するディペンダビリティー問題に対して, 図1－1の研究実施体制中の,「(1)耐タンパ性 LSI 設計プラットフォーム研究」の中心的な役割を果たす. さらに, 上記第2のセキュリティーLSI の偽造に対するディペンダビリティー問題に対して,「(3)偽造 LSI を識別する PUF を用いたセキュリティーシステム研究」の①における, 高性能な PUF の回路設計技術の研究を行う. また,「(2)耐タンパ性能評価プラットフォーム研究」においては, H23 年度までに産総研が開発してきた評価プラットフォームを使用して, (1)で開発したチップの耐タンパ性の検証を行い, 問題点の抽出並びに産総研へのフィードバックを行う.

②本グループの研究の特徴

（1）耐タンパ性LSI設計プラットフォーム研究」を実現するため提案する中心技術として，当初はドミノRSL方式を検討してきた．DES暗号回路で実装を行った結果，標準的な1st Orderの CPA攻撃に対しては100万波形で8bit以下の鍵特定しかできなかったが，高度な2nd Order攻撃に対しては，脆弱性が発見された．また，新しい暗号方式である AES 暗号回路に対してチップ面積が大きくなりすぎるという問題点があった．これに対して，H23年度以降の耐タンパ設計技術としては，小面積でかつ2nd Order攻撃に対しても耐性のある2線RSLメモリ方式を中心技術として研究を進めた．本方式を用いて 0.18μmCMOS で回路設計を行い，評価したところ，電力を用いた1stOrderの攻撃に対しては8bit以下という目標を達成することができた．本性能は既存の提案方式である WDDL 方式，MDPL 方式，MAO方式に対しては非常に高く，TI 方式と比較すると，同等である．またチップ面積，消費電力に関しては他の対策方式と比較して最も面積ペナルティーが小さく，消費電力も小さい．耐タンパ性を有するTI方式と比較すると1/5以下の面積,1/10以下の消費電力である．今後，2ndOrder等のより高度な電力解析攻撃および電磁波を用いた攻撃に対して検討を進めるとともに，最終デモンストレーションに使用する，三菱電機と共同で試作予定のセキュアチップに搭載を予定している．

（2）偽造LSIを識別するPUFを用いたセキュリティーシステム研究においては，立命大で提案するDTM方式アービターPUF を試作し，ユニーク性の評価に加えて環境変化（電圧・温度）再現性を実チップを用いて評価を行ってきた．PUFのベンチャー企業であるVerayo社の提案するアービターPUFおよびXORアービターPUF方式と，実チップを用いての比較を行い，DTM アービター方式が最も認証誤認率が最も低いことを確認した．また，SVM および LR 方式の機械学習攻撃耐性の評価も行い，アービターPUF と比較して，高い機械学習攻撃耐性を持つことを確認できた．また，三菱電機と協力して，立命大の提案するDTMアービターPUFと，三菱電機の提案するグリッジPUFを65nmプロセスで試作した．今後PUFが生成するIDの安定化を目指して回路および誤り訂正回路の研究を行っていく．

③研究実施方法(研究チーム内外の連携関係など)

（1）耐タンパ性LSI設計プラットフォーム研究」においては，LSI設計時に耐タンパ性の評価を行うことのできる耐タンパ検証 CAD システムの研究を名城大学がおこなっており，立命館大で設計した，「2線 RSL メモリ方式」を用いた暗号回路の耐タンパ性の検証を行うとともに，他の研究機関で進められている，耐タンパ対策方式との相対的なタンパ性の比較を行う予定である．また，実際に試作した耐タンパ LSI の実験的な評価に当たっては，産総研が研究を進めている，（2）耐タンパ性能評価プラットフォームの最新の技術を導入して評価を行う．

（3）偽造LSIを識別するPUFを用いたセキュリティーシステム研究」においては，PUFの回路設計・実装において三菱電機Gの提案する新型PUFである，「グリッジPUF」のレイアウト設計・チップ試作を協力して進めていく．さらに， 産総研G，三菱電機 G が中心に進めている，PUFと暗号回路を融合したセキュリティーシステムにおいてPUFに必要とされる要求仕様を議論し，その使用を満足できるPUFの回路設計手法を確立する予定である．

2)「「産総研」グループ

①本研究グループの研究課題、ならびに所属する研究チームの課題との関係

情報の漏洩や改ざんに対抗しディペンダブルなシステムを構築するための基礎技術として，暗号が必要不可欠である．しかし近年，暗号モジュールの実装の不備を突き，消費電力や放射電磁波から情報を盗み出す「サイドチャネル攻撃」が問題となっている．サイドチャネル攻撃の耐性評価では高度なVLSIの知識も必要となってきており，暗号が正しく実装され機能していることをユーザ自身が判断することは難しい．ゆえに，評価手法の標準化と公的な試験認証制度の運用が不可欠である．そこで産総研グループでは，サイドチャネル評価環境SASEBO ボードを開発し，評価試験制度の運用に不可欠な試験環境を整備する．統一された評価環境を国際的に普及させることで，各国の研究成果に基づく安全性評価指針の策定と国際標準化に貢献する．これまでもSASEBOボードを開発し米国NISTと協力して国際標準化を進めてきたが，過去のノウハウを生かした低ノイズで利便性の高いボードを新規開発し，また，攻撃技術の進歩や半導体プロセスの微細化に応じた最先端の評価環境を提供することで，ハードウェアセキュリティの国際標準策定における主導的立場を維持する．

また，LSI の製造が東南アジアへとシフトする中で，粗悪品の流通や不正回路の埋め込みの可能性が指摘されている．このような粗悪・不正LSIの検出・防止技術としてPUFの研究が盛んに行われている．しかし，そのアーキテクチャや実装方法，および性能・安全性評価手法等は未だ確立されているとは言えず，多くの課題が山積している．そこで産総研グループでは，高効率で安全な PUF の開発と，PUF の定量的性能評価手法の開発を行う．また，これら手法を応用したデモ・アプリを SASEBO 上に構築し，提案手法の有効性を評価する．

産総研 G では，立命館大 G が開発する耐タンパ暗号 LSI の安全性を評価するためのボードおよび電磁波取得環境を開発する．また，取得された電力・電磁波データを解析するソフトウェアの開発を行う．さらに，機械学習に対する PUF の安全性を立命館大 G と協力して評価するほか，立命館大 G が開発する PUF チップを搭載したアプリケーションを開発するためのボードを作成する．

②本グループの研究の特徴

サイドチャネル“攻撃”と安全性“評価”で大きく異なるのは，後者は LSI の内部情報まで入手可能なホワイトボックス試験が可能な点である．従って試験者は攻撃者よりも，解析コストの面において圧倒的に有利な立場にある．評価試験は絶対的な安全性を保証するものではなく，守るべき情報の価値と攻撃者のコストのバランスを考えることが重要である．また，また評価試験もビジネスとして実施するものであるため，研究と異なりコストを度外視した時間と労力をかけるわけにもいかない．このような観点から，産総研は攻撃コストに基づいた安全性評価指針の策定を提案し，FIPS 140-3 の 2nd ドラフトに採用されている．本事業では，いかにコスト（設備よりも時間的コストが重要）を下げて高い解析（評価）精度が得られるか，またそれは，ブラックボックス評価である攻撃者にとってどの程度のコストとなるのかといった視点に立って研究を進めている．また，事業展開を常に考慮しながら，実験環境の整備と評価ツールの開発も行っている．

PUF はこれまで，長ビットのチャレンジ入力に対し，1 ビット程度のレスポンスが得られるものがほとんどであり，スループットが極めて低かった．しかし PUF は，同一の回路構成からばらつきを利用してデバイスごとに異なる出力を得ようとするものであり，その特性上，出力のエントロピーがどうしても低くなってしまうという問題がある．そのため，例えば 128 ビットの暗号鍵を得るためにはその 4 倍かそれ以上の PUF 出力が必要になる．ゆえに PUF の実用化のためには，高スループットであることが重要である．本研究は，Linear Feedback Shift Register (LFSR) を模した Pseudo-LFSR という独創的な構造によって，小型でありながら極めて高いスループットを持つ PUF を実現する．この構造は，動作サイクル数によって出力のランダム性が高くなってゆくため，同一の回路構成でありながら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，高性能な PUF の開発のためには，PUF の性質を定量的に評価するための指標が必要である．これまで，性能指標はいくつか提案されているが，例えば指標によって 0 や 1 が最高性能であったり，0.5 が最高性能であったりするため，様々なデバイス上で様々な PUF を比較するには不向きであった．本研究が提案する性能指標は，すべて 0 が最低で 1 が最高となるよう正規化されており，定量的かつ直感的で，様々な PUF の性能の比較評価に適している．

③研究実施方法(研究チーム内外の連携関係など)

産総研 G の内部において最先端の対策済み暗号 LSI を設計するとともにその評価環境を開発する．この評価環境を，立命館大 G の耐タンパ暗号 LSI および PUF チップの評価環境へと転用する．さらにこれを一般的な暗号 ASIC の安全性評価用ボードとして公開することで，チーム内の研究の促進とともに，安全性評価指針の国際標準化とその評価プラットフォームの整備に貢献する．

また，最新のサイドチャネル攻撃手法や防御手法の開発のための FPGA ボードの作成や，高精度な電磁波解析攻撃を実現する磁界プローブや自動磁界スキャナの開発を行い，これらを製品化して国際的に展開してゆく．評価ボードは，これまでも協力して開発を行ってきた東京エレクトロンデバイス株式会社および凸版印刷株式会社から事業化することを検討する．また，米 Cryptographic Research 社およびオランダ Riscure 社と協力し，IC カード評価ツールに産総研の評価手法の実装を進める．電磁波解析用の磁界プローブや磁界ステージは，EMC/EMI 製品において高い開発実績を持つ森田テック株式会社と協力し，高精度な電磁波解析攻撃によって安全性評価指針の策定や国際標準化に貢献するとともに，開発した成果物を製品として展開してゆく．

評価手法の標準化活動については，国内では総務省と経産省による暗号アルゴリズムの評価プロジェクトである CRYPTREC 委員会，米国の NIST，欧州の JHAS といった標準化機関・業界団体と協力して作業を進めている．特に，暗号モジュール評価の国際規格 ISO/IEC 19790 およびそのベースとなる米国連邦標準 FIPS 140-3 の早期制定を目指すための活動に力を入れる．具体的には，NIST と産総研で Non-Invasive Attack Testing workshop NIAT2011 を国内開催し，IC カードを中心とする，企業，試験機関，ツールベンダー，大学・研究機関，そしてユーザ間で議論を行う．また，ISO/IEC において具体的な評価手法を New work item として承認されることを目指すとともに，ISO/IEC のセキュリティに関する国内委員会 SC27 WG3 に委員として参加して国際標準策定に貢献する．また，LSI セキュリティの国際標準 Common Criteria の国内部会である ICSS-JC にも委員として参加し，暗号モジュールの国際標準化動向をもとに安全性評価プラットフォームの整備について検討する．

3)「三菱電機」グループ

①本研究グループの研究課題、ならびに所属する研究チームの課題との関係

安全な暗号鍵管理なくして安全な暗号システムは存在し得ない．しかし，現在の VLSI システムにおける暗号鍵管理は，安全性の低いソフトウェア的なアプローチか，高コストな耐タンパ機構で実現されており，技術的パラダイムシフトが求められている． 特に VLSI システムの開発は分業化が進んでおり、フロントエンド、バックエンドを代表とする設計レイアで掛かる制約はこれまで以上に強くなることが予想される。このとき、技術的には実施可能な耐タンパ機構であっても設計制約やそれを解決するためのコストが問題となり、耐タンパの実現を妥協するケースが発生しうる。

その一方で、安全な暗号システムが必要となるアプリケーションは IC カードのみにとどまらず、組み込み機器や産業機器など様々なアプリケーションに展開されている。この際、設計情報の保護や正規品の認証といった機能は海外へと市場を開拓する上で不可欠である。なぜならば、耐タンパ機能が脆弱であることが要因となり、設計情報が流出して高度な模倣品が製造されるケースが後を絶たないためである。このような問題は安心・安全の面でエンドユーザー側は不利益を被り、ベンダー側もブランドイメージの低下など重大な事態を引き起こすことになる。

そこで、本研究グループでは、IC カードのようなセキュリティ LSI で実現すべきセキュリティレベルを LSI 開発の分業化に伴う制約下であっても実現可能な耐タンパ機構の実現を目指す。

②本グループの研究の特徴

当グループGでは，PUF の「性能」であるランダム性やエラーレートを設計段階で評価可能で，かつ，標準 CMOS のみで構成可能な「グリッチ PUF」と呼ばれる方式を提案している．本方式を応用して，LSI 毎にユニークな秘密情報を生成する回路を開発する．具体的には，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，グリッチ 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回路のフロントエンド設計を行う．また，バックエンド設計は，立命館大学グループに協力頂き，ターゲットプロセス(e-Shuttle 65nm を予定)に適したグリッチ PUF 回路，誤り訂正回路，汎用ハッシュ関数回路のパラメータ設計を行う．

また当グループでは，Random Switching Logic(RSL)と呼ぶ，暗号回路そのものに対するサイドチャネル対策技術と，論理シミュレーションによる評価技術を提案してきた．一方で，SoC全体のサイドチャネル対策では暗号回路への対策だけでは不十分で，CPUそのものの演算処理やメモリーレジスタ間転送に対して包括的な評価と対策を施す必要がある．しかし，脆弱性とそれに対応した対策はCPUの実装形態やバス構成と云った実装アーキテクチャに依存する部分が大きく，統一的な対策や評価方法が確立されていないのが実情である．そこで，ベーシックなCPUの実装形態であるあるMIPSアーキテクチャとWishboneバスを題材として，公開されているオープンソースをベースに包括的に脆弱性と実装アーキテクチャの関係を洗い出し，実装アーキテクチャと論理構造および有効な対策を可視化し，相互の関連付けを明確に行う．これらの結果を論理シミュレーションによるサイドチャネル耐性評価にフィードバックし，暗号回路のみならず，SoC全体のサイドチャネル耐性を設計段階で包括的に評価するプラットフォームを構築する．

③研究実施方法(研究チーム内外の連携関係など)

サイドチャネル対策及び PUF 共に LSI の試作は立命館大学グループと連携して実施する。

サイドチャネル対策については、立命館大学グループで開発されるサイドチャネル対策 AES 回路を取り込み、それ以外のモジュールは当グループで対策し SoC 全体をセキュア化する。AES 回路に関しては、当グループが第三者評価の視点で脆弱性を評価し、立命館大学グループにおける AES 回路の改良へとフィードバックする。評価実施時には産総研 G の SASEBO プラットフォームを活用する。また、シミュレーション評価技術については、名城大グループに要件提示などを行う。

PUF 開発については、当グループが実施するフロントエンド設計における前提の妥当性を、バックエンド設計及びアナログ特性の視点から立命館大学グループで検証し、前提の最適化を実施する。

4)「名城大」グループ

①本研究グループの研究課題、ならびに所属する研究チームの課題との関係

名城大グループでは主として，耐タンパ性を保障するLSI設計プラットフォームに関する総合的なCADシステムを開発する。この CAD システムは，(1)耐タンパ検証 CAD システムと(2)耐タンパドリブン設計 CAD システムと

の 2 つのサブシステムで構成する。

この CAD システムでは，消費電力によるサイドチャネル攻撃，故障利用によるフォールト攻撃を対象とする。(1)に関する研究課題は，検証の高精度化と高速化である。まず，高精度化について，サイドチャネル攻撃では，回路のどの部分が，どの程度脆弱なのかを定量的に評価できることが重要である。また，フォールト攻撃では，トップダウン的なフォールトの拡散のシミュレーションと，ボトムアップ的なフォールト付暗号文からの解析手法の開発が重要である。次に高速化に関して，検証時間の中では，(i)電力波形の取得と，(ii)電力と秘密情報の相関解析の 2 つの処理が支配的である。そのため，この 2 つの処理時間を削減することが重要である。また，(2)に関する研究課題としては，(1)の検証結果を用いて，サイドチャネル攻撃やフォールト攻撃での耐タンパ制約を導入することである。

②本グループの研究の特徴

(i) 耐タンパ検証 CAD システム

消費電力によるサイドチャネル攻撃に対して，これまで発表されている耐タンパ検証手法では，消費電力情報を取得した後に，既知の様々な電力解析攻撃シミュレーションを実施する必要がある。さらに，脆弱な箇所を見落とすことなく検証するためには，種々の選択関数（攻撃箇所）を用いて攻撃シミュレーションを行う必要がある。これに対して，本研究では，従来の攻撃シミュレーションを行う代わりに，電力解析攻撃の対象となる回路が，消費電力に及ぼす影響を分析し，脆弱な場所を特定し，定量的に評価する方法を新たに考案する。
これにより，1 度の解析でアーキテクチャのサイドチャネル攻撃に対する耐性の傾向評価や，クロックサイクル内の時間経過に対するビット単位での脆弱箇所の判定が可能となり，検証の高精度・高速化を実現する。さらに，標準暗号 AES を対象に，WDDL，Maskd-AND，MDPL 等の代表的な対策回路だけでなく，立命大 G の開発したドミノ回路や 2 線 RSL メモリに対しても提案手法の評価実験を行い，その有効性を実証する。

(ii) 耐タンパドリブン設計 CAD システム

これまで理論的な研究が中心であったフォールト攻撃に対して，産総研 G が開発した SASEBO ボードを用いて，クロックにグリッチを発生させて，実機でのフォールト攻撃に対する耐性を評価できる環境を整備する。さらに，従来のフォールト攻撃に関する理論的研究では，暗号化処理中の特定のタイミングで故障が発生した場合を仮定して，その仮定のもとで秘密情報を特定するトップダウン的なアプローチ用いている。これに対して，本研究では実機で生じたエラー（故障）を元に，秘密情報を特定するボトムアップ的な新しい解析手法を導入する。

③研究実施方法(研究チーム内外の連携関係など)

2 つの研究課題（(1)耐タンパ検証 CAD システム，(2)耐タンパドリブン設計 CAD システム）に対して，まず，研究期間の前半で耐タンパ検証システムの開発を重点的に行う。ここでの連携については，消費電力を利用したサイドチャネル攻撃に対しての耐性回路の実機での検証として，立命大 G の試作チップ（DES,ドミノ RSL-DES,AES,ドミノ RSL-AES）のデータを利用する。

また，クロックや供給電圧を利用したフォールト攻撃に対しての実機での検証としては，産総研 G が開発した SASEBO ボードを利用する。

一方，研究期間の後半では，耐タンパドリブン設計 CAD システムの開発を重点的に行う。ここでは，消費電力を利用したサイドチャネル攻撃に対しては，立命大 G が研究・開発を進めてきた対策用の AES の IP を組み込んだセキュアな SoC に対して，耐タンパ性検証結果を踏まえて耐タンパ専用設計 CAD システムを構築する。

さらに，フォールト攻撃に対しては，産総研 G が開発した SASEBO ボードでの評価検証結果を利用するだけでなく，三菱 G でのフォールト攻撃の実験結果を組み込むことで総合的な耐タンパ性を実現する。

（3）領域外部の企業等との連携

耐タンパ性 LSI 設計プラットホームのコア技術である，2線 RSL メモリの設計技術は，設計 IP としてのビジネスの可能性をトッパンテクニカルデザインセンタと議論中である．

耐タンパ性能評価プラットホームのコア技術である SASEBO は，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，H22 年度に正式に製品化を行った． サイドチャネル攻撃評価ツールに関しては，H24 年にオランダ Riscure 本社を訪問し，SASEBO や，森田テック製 EM ステージを使用する環境の構築等での協力可能性を議論している．

PUF に関しては，また RFID・IC カードを商品化している凸版印刷徳田俊彦様，横山喜一様より，9月の国際会議において PUF の評価手法に関して技術交流を行いたいとの申し出があり，ET 展での技術打ち合わせ,および DVLSI ワークショップにおいてポスターを用いた討論を行った．

(4)領域内他研究チームとの連携関係
現状，特になし

1．3　研究グループの今年度の研究の狙い

1)「立命館大学」グループ(研究代表者グループ)

§1に記載した研究チームの達成目標に対して，立命館大学Gでは以下(i)～(iii)の3項目の目標を中心的に達成する．

(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．

⇒H23 年より，未対策回路に対して，消費電力を約2倍以下，回路面積を約3倍という具体的性能目標を追加

(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．

⇒H23 年より，より高い目標として，1stOrder の攻撃に対しては 8bit 以下の鍵特定，2ndOrder 等の高度な攻撃に対しては 64bit 以下と修正した．今後，電磁波を用いた攻撃に対しても 64bit 以下を目標とする．

(iii)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．

⇒H23 年より追加で PUF 回路に対する機械学習攻撃に対する評価を行うことを追加した．また，今後三菱電機と共同して PUF の生成した ID を安定化し，かつ必要があれば誤り訂正を行う手法を追加目標とする．

現在の中間報告時点で，要素技術的にはかなり目標達成に近づいたので，今後，最終年度に向けたデモンストレーションとして，三菱電機とは耐タンパ暗号回路および PUF を搭載するセキュア LSI を使ったワイアレスセキュアシステム，産総研とは PUF を用いた画像データ等のデジタルコンテンツ保護を検討していく．

2)「「産総研」グループ

サイドチャネル攻撃については，FIPS 140-3 の標準化とその評価試験制度 CMVP(Cryptographic Module Validation Program)，およびその日本版である JCMVP の運用を開始(平成 24 年度)するためのイニシャルの評価環境整備を第一の達成目標とする．なお，攻撃手法は日進月歩であるため，評価指針および評価環境も逐次アップデートしていく．また，フォールト攻撃等の研究も進め，国際標準のさらなる改訂にも取り組んでいく．具体的には，サイドチャネル攻撃およびフォールト攻撃の新手法とその防御手法の実験環境である FPGA ボードの開発，立命館大 G 作成の耐タンパ暗号 LSI 等の ASIC 評価用ボードの開発，およびそれらを用いて取得されるデータの解析ツールの開発を行う．また，高精度な電磁波解析攻撃を実現するための高性能磁界プローブや自動磁界計測環境の開発を行う．さらに，これら環境を用いて行った実験結果を基に安全性評価指針を検討し，標準化活動に貢献する．

これまでに，SASEBO-RII，SASEBO-GIII，ZUIHO の 開発，自動 EM ステージの開発，データ解析ソフトウェアの開発を行い，実際に実験を行って結果を安全性評価指標の検討に生かしている．SASEBO-G および GII は，それ自身が JCMVP の認証を受けることで認証制度の運用に貢献している．また，ISO/IEC において安全性評価の具体的な手法が New work item となり，そのドラフトを執筆した．さらに，ISO/IEC の SC27 WG3 の委員や Common Criteria の国内部会 ICSS-JC の委員を務めている．FIPS140-3 およびその国際標準 ISO/IEC 19790 の制定にはまだ至っていないが，目標の 7 割程度が達成されていると言える．

PUF 回路については，ユニークで安定した ID の生成手法や高効率な ID 生成手法の開発に加えて，機械学習によるクローン攻撃に対する安全性確保や，PUF 性能の定量的評価手法の開発を行う．開発した PUF を多くの SASEBO ボードに実装し，その安全性を評価するとともに，定量的指標によってどのように性能を評価することができるか検討する．また，立命館大 G の PUF チップの有効性評価のため，PUF を利用した動画再生システムを SASEBO を用いて開発する．PUF をデバイス認証や暗号鍵生成に利用する動画再生システムを構築し，その安全性や性能を評価する．

これまでに，高効率で安定性・ユニーク性の高い PL-PUF を開発しており，その性能の定量的評価手法を提案している．また，機械学習攻撃に対する安全性評価を行っている．安全性の定量化や PUF を使ったアプリケーションについては開発中であるが，目標の 6 割程度が達成できていると言える．

3)「三菱電機」グループ

同一の回路でありながらデバイス固有の物理特性を抽出することができ，機器のなりすましや不正な模倣品製造を根本的に防止する「PUF」技術と、LSI の処理中に発生する消費電流や電磁波など副次的な情報から LSI に格納された秘密情報の漏洩を防ぐ「サイドチャネル評価・対策」の融合を実現し、不揮発領域を持たない組込み機器向けの低コスト SoC であっても、高度な物理的対策が施されたセキュリティ LSI に匹敵する耐タンパ性を実現することを目指す． この技術ベースにより、現在社会的に問題となっている機器の模倣品製造を防ぎ、エンドユーザーにとって安心・安全な組み込み機器の提供を行う。

PUF 技術については、立命大と共同で，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，グリッチ 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機能を持つ LSI を試作し、0-85℃の温度変化及び+-5%の電圧変化に対応可能とであることを確認した。

・サイドチャネル評価・対策については、教科書的な MIPS アーキテクチャを持つオープンソース CPU を題材とし，CPU に潜在する脆弱性を実施し、脆弱性要因を机上、シミュレーション及び FPGA を用いたプロトタイピングの3つのアプローチで特定した。加えて、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。

・以降は、上記の成果と立命大 G が開発するセキュアな AES 回路と融合を図る。

4)「名城大」グループ

アルゴリズムレベル，論理設計レベル，レイアウト設計レベルの各設計フェーズでの耐タンパ性を指向した設計・検証の CAD システムを構築する。この CAD システムでは，消費電力によるサイドチャネル攻撃，漏洩電磁波によるサイドチャネル攻撃，故障利用によるフォールト攻撃を対象とする。この目標達成により，耐タンパ性を保障する LSI 設計プラットフォーム用総合 CAD システムが完成する。

研究課題(1)の検証の高速化・高精度化を実現するために，消費電力によるサイドチャネル攻撃に対しては，従来の攻撃シミュレーションによりその安全性を評価するのではなく，脆弱な箇所を定量的に評価できるシステムを開発する。さらに，フォールト攻撃に対しても，故障を混入させたこれにより，①の検証 CAD システムの研究課題を解決することが可能になる。

また，研究課題(2)について，サイドチャネル攻撃では，攻撃対象となる部分回路設計だけでなく，回路全体の設計でも提案 CAD システムが適用できるため，耐タンパ性を保証することが可能である。さらに，フォールト攻撃では，理論的なフォールト攻撃に対する解析だけでなく，フォールト攻撃に対する耐性を実機で評価できる環境を整備することで，フォールト攻撃に対する耐タンパ制約を導入することが可能になる。

これまでの進捗として，まず，研究課題(1)では，各設計段階において，電力解析攻撃に対する脆弱性を定量的に評価できるシステムを開発した。また，フォールト攻撃についても，どの程度の情報がフォールトによってリークするかの評価システムを開発した。そのため，研究課題(1)については，これまでに当初計画の 6 割程度の課題を解決し，残る課題としては，設計段階で高精度な消費電力波形を高速に取得できる手法の確立と漏電磁波によるサイドチャネル攻撃への提案手法の拡張である。次に，研究課題(2)では，フォールト攻撃に対する耐性を実機で評価できる攻撃評価システムを開発した。そのため，この攻撃評価システムを用いて，設計段階での耐タンパ制約を導入することが残された課題である。同様に研究課題(2)についても，当初計画の 7 割程度の課題を解決した。

§2. 研究実施体制

①「立命館大学」グループ

ア 研究分担グループ長： 藤野 毅(立命館大学理工学部、教授)（研究代表者）

イ 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

ア 研究分担グループ長： 堀 洋平(産業技術総合研究所、研究員)
イ 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
ア 研究分担グループ長： 鈴木 大輔(三菱電機株式会社、主席研究員)
イ 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
ア 研究分担グループ長： 吉川 雅弥(名城大学理工学部、教授)
イ 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

§3. 研究実施内容
(文中に番号がある場合は(4－1)に対応する)

3. 1 研究の成果と自己評価
次ページ以降に，本研究の大きな3テーマに対する研究成果をまとめた.

(1)耐タンパ性 LSI 設計プラットフォーム
1) 成果 1.「2線 RSL メモリ方式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)
2) 成果2.「電力解析攻撃に対する設計検証システム」(名城大グループ)

(2)耐タンパ性能評価プラットフォーム
3) 成果3.「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) 成果4. 「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
5) 成果5.「新型 PUF および誤り訂正技術を用いた秘密鍵生成回路」(立命館大・三菱電機グループ)
6) 成果6.「高効率な PL-PUF の開発と PUF の定量的性能評価手法」(産総研グループ)

1) 成果 1.「2線 RSL メモリ方式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内容(原著論文[15])

DES/AES 暗号回路などの共通鍵暗号回路では，電力を利用したサイドチャネル攻撃に対する脆弱性はテーブル変換を行う SBox(DES の場合は 6bit 入力 4bit 出力，AES の場合は 8bit 入力 8bit 出力)という非線形回路が，入力または出力データに依存して消費電力が異なることに起因している．この SBox 部を図 4-1 に示すような，どのような入力値に対しても消費電力が一定になる2線 RSL メモリを用いて AES 暗号回路を実装した．SBox 部以外は線形回路で構成されているため，ラウンドごとに乱数マスクを更新することで，入力値に依存した消費電力の偏りを隠ぺいすることが可能である．また，本方式は，SBox 部以外は標準スタンダードセルを用いることができるため，ASIC の標準設計 CAD フローで実装可能である．

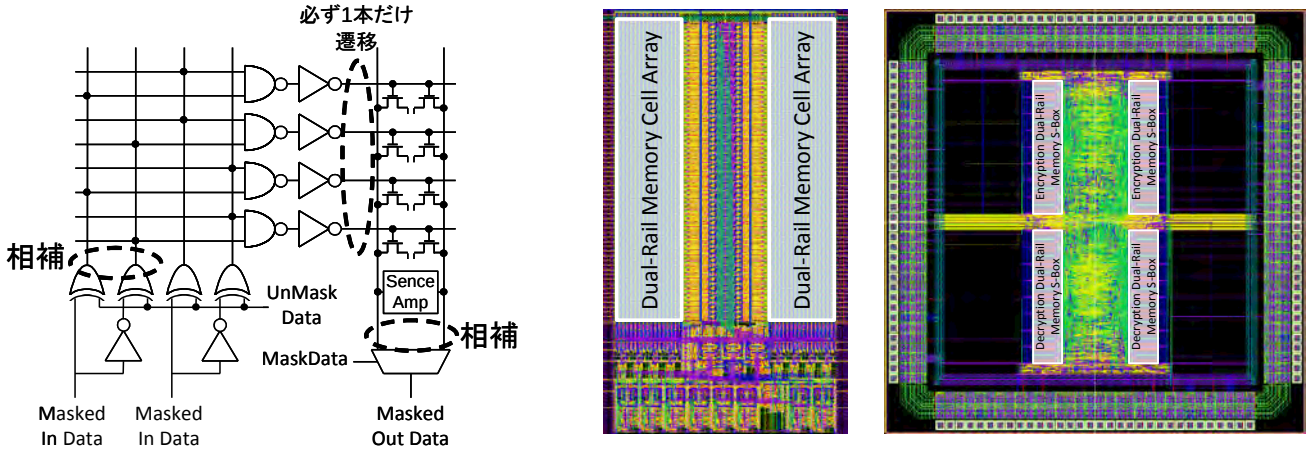


図4-1．2線RSLメモリ方式のSBox部の概念図(左)と180nmCMOS AES暗号回路試作チップレイアウト(右)

②有用性　および　③優位比較

本提案方式と，従来提案されてきた耐タンパ設計方式(WDDL,MDPL,MAO,TI)を通常のASIC設計フローで設計し，0.13/0.18 μ mCMOS で試作したチップを用いて，耐タンパ性の検証およびチップ面積・消費電力を行った結果を図4-2に示す．耐タンパ性の評価は，産総研開発のSASEBO-RIIボードと定評あるオランダ Ricure 社のソフトウエアを使用し各種の攻撃を行った．4000 波形以下ですべての鍵がリークする未対策回路はもちろんのこと，もっとも強いTI方式と同等以上の100万波形でも1バイト以下のリークであることを確認できた． チップ面積・消費電力増加，未対策回路と比較してそれぞれ10%および50%以下であり，他の対策方式と比較して最も面積ペナルティーが小さく，消費電力も小さい．特に同等の耐タンパ性を有するTI方式と比較すると1/5以下の面積,1/10以下の消費電力であることは特筆すべき性能である．

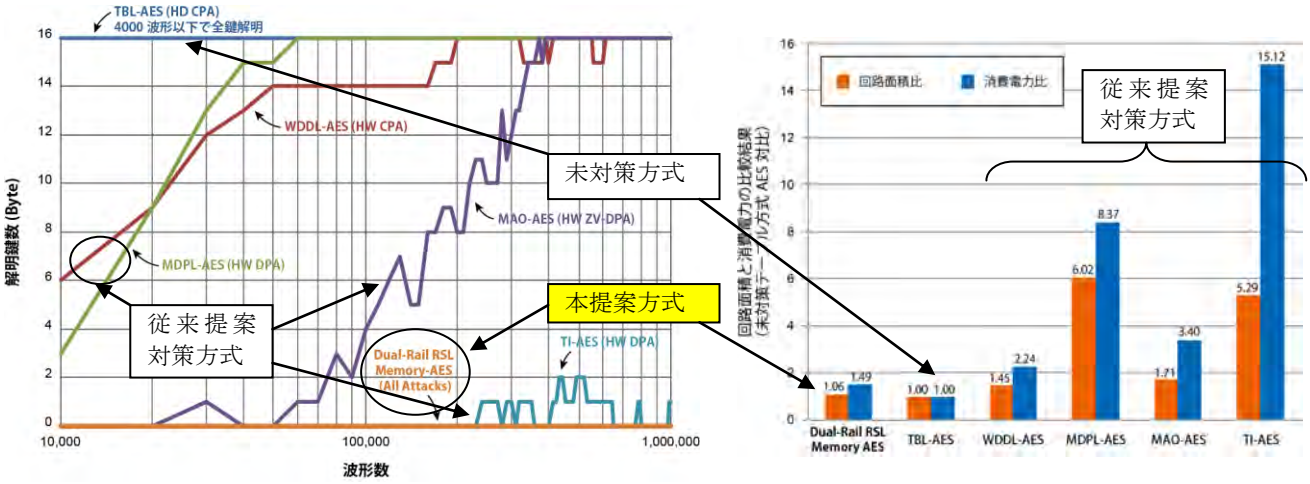


図4-2．未対策および既存対策方式との耐タンパ性比較(左)と消費電力・面積比較結果(右)

2) 成果2．「電力解析攻撃に対する設計検証システム」(名城大グループ)

① 内容(原著論文[19])

本研究で提案する脆弱性評価手法[19]では，従来の電力解析攻撃シミュレーションによって秘密鍵を推定できるか否かで安全性を判定するのではなく，電力解析攻撃の対象となる回路が消費電力に及ぼす影響を分析し，どの箇所からのリーク(秘密鍵に関連する情報)が多いかを定量的に評価する。また，提案手法では，任意のモジュール単位での検証を可能にすることで，全ての回路部の設計が完了する前の段階での耐性評価を可能にする。さらに，LSI と電源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モデル化することで，攻撃検証用の LSI シミュレーション電力波形から攻撃時に観測される波形の予測を可能にする。一方，検証時間について，暗号化で現れる中間値と同じ中間値をスキップしながら再現することで，攻撃に不要なラウンドの消費電力シミュレーションを省略し，攻撃対象ラウンドの消費電力波形のみを再現する攻撃ラウンド型消費電力シミュレーション方式を新たに導入する。これにより，検証に必

要な消費電力波形の取得の大幅な時間短縮を実現する。

② 有用性 および ③優位比較

提案手法の評価実験として，電力解析攻撃未対策回路として真理値表方式，合成体方式，PPRM1 方式，PPRM3 方式の 4 種類を，同対策回路として RSL 方式と MDPL 方式の合計 6 通りを対象に実験結果を図 4-3 に示す．提案手法が，クロックサイクル内の時間経過を考慮して，ビット単位での脆弱性を評価することが可能であることを実証した。さらに，本手法を用いることで，立命大 G が開発したドミノ RSL 回路について，1 ビットの乱数マスクでは攻撃可能なリークがあることを明らかにした．LSI 消費電力波形と比較し，本手法による予測波形と，攻撃検証結果は，図 4-4 に示すように実機での実験結果に近くなっている．また，LSI シミュレーション電力に急峻なピークがあるような場合，積分効果により，むしろ実機上での観測波形を使ったほうが攻撃しやすくなる場合もあるため，提案手法により実際的な検証が可能となる．

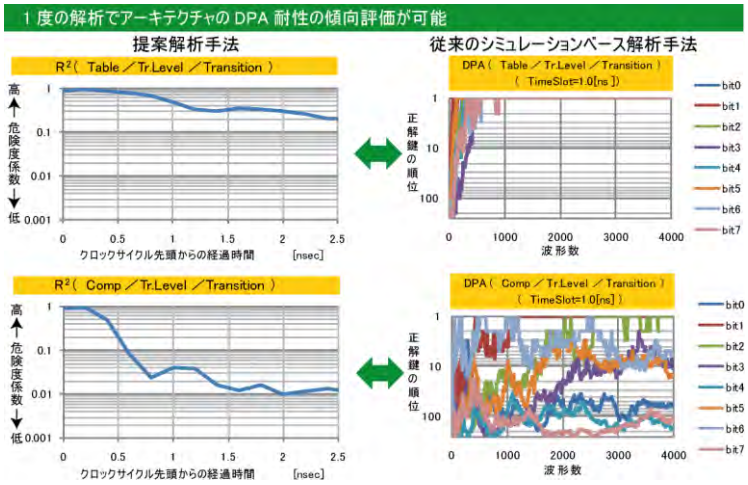
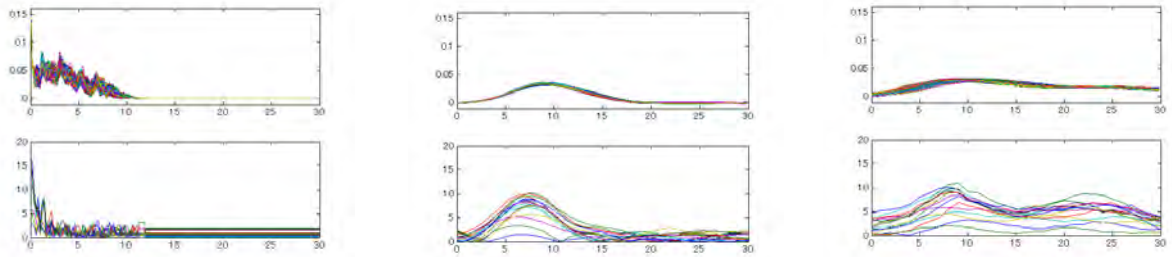


図4-3. 提案脆弱性評価手法(1 回の解析でアーキテクチャの脆弱性がビット単位で判定可能)



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

図4-4. 実機での耐性予測

3) 成果3.「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内容(原著論文[18])

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 評価ボード(図 4-5(左))

(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 4-5(中))

(iii) ZUIHO: Spartan-3FPGA 搭載，教育用サイドチャネル攻撃評価ボード(図 4-5(右))

(iv) 高性能磁界プローブ及び高性能小型磁界スキャナ

(v) サイドチャネルデータ解析ソフトウェア．

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 の制定に協力し，その 2nd ドラフトをベースに国際規格 ISO/IEC19790 の作成を開始した．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 New work item として具体的な評価手法の策定を検討することとなり, そのドラフトを Easter 氏と佐藤, 坂根で執筆した. また, ISO/IEC のセキュリティ標準に関する SC27 WG3 国内委員会に佐藤が 2011 年 11 月から参加し, 2012 年度は坂根が引き継いでいる. また 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.

図4－5. サイドチャネル評価ボード SASEBO-RII(左), SASEBO-GIII(中), ZUIHO(右)

②有用性および③優位性

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(2012 年 9 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 4-6 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. ZUIHO は, サイドチャネル攻撃の教育や評価手法の普及を目指した安価な評価環境であり, 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. ZUIHO のプロトタイプ開発は完了し, 現在, 販路を確保するため企業と交渉中である.

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, 高精度で電磁波データを自動計測することが可能となった. また, オシロスコープと磁界スキャナー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.

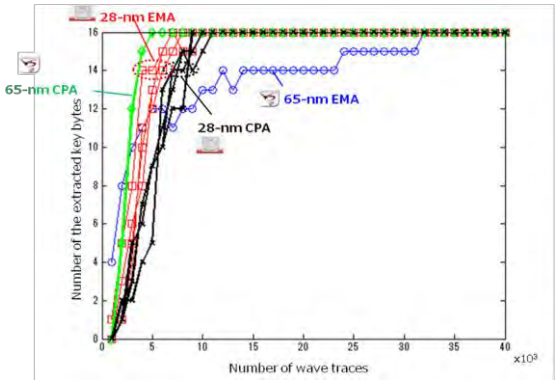


図 4－6 SASEBO-GIII と GII 上の CPA および EMA

4) 成果4. 「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内容(原著論文[9])

(1)フォールト攻撃評価システム: 開発したシステム[14]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。

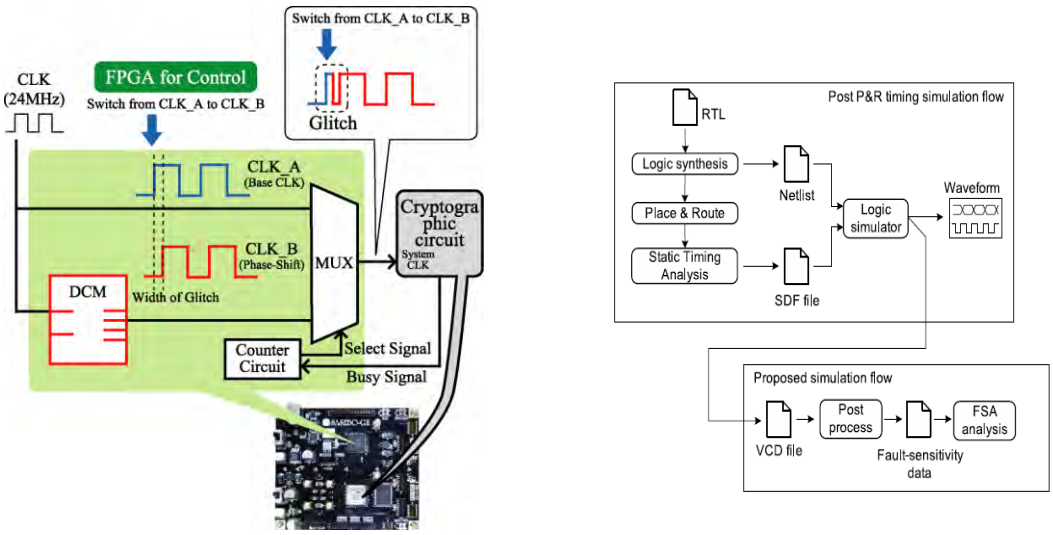


図4－7. 開発したフォールト攻撃評価システム(左:フォールト評価システム、右:FSA シミュレータ)

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。

5) 成果5.「新型 PUF および誤り訂正技術を用いた秘密鍵生成回路」(立命館大・三菱電機グループ)

①内容(原著論文[1])

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アービターPUF を改良した「遅延時間差検出(DTM: Delay Time Measurement)型アービターPUF」を提案しており，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．

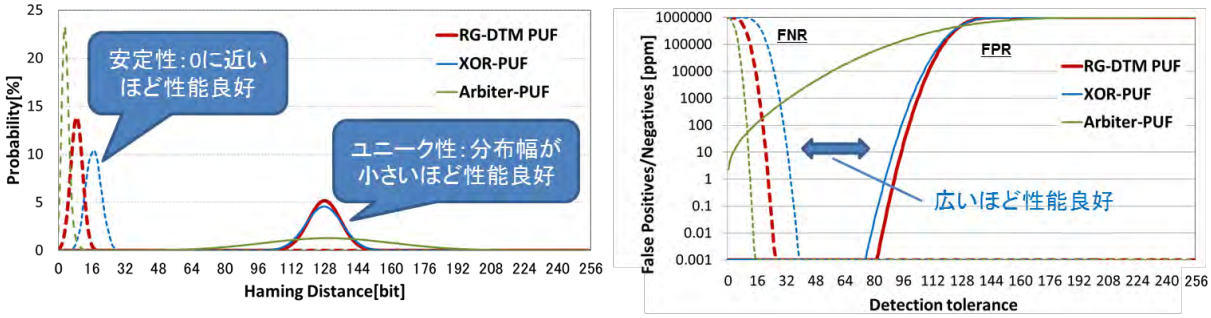
②有用性 および ③優位比較

従来型アービターPUF および従来型の改良案として，米国 Verayo 社が提案している XOR アービター

PUF との比較結果(0.18μmCMOS プロセスチップ)を図 4-8 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 アービター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.

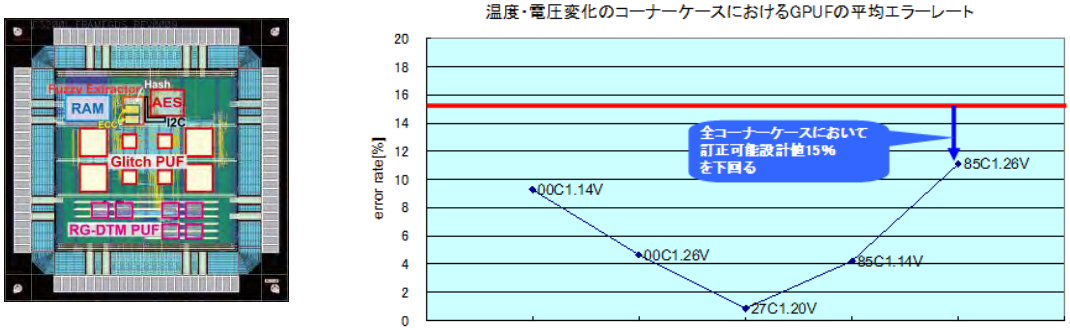
PUF は, 本質的にレスポンスに揺らぎを持つため, そのままでは1ビットの誤りも許されない暗号鍵を生成することはできない. これに対して, グリッチ PUF 回路, 誤り訂正回路, 汎用ハッシュ関数回路を組み合わせることにより, PUF 回路の不安定な出力ビット列を訂正して秘密情報を安定に生成する鍵生成回路を国内で始めて開発した。本回路を搭載した LSI を e-Shuttle 65nm プロセスで製造し評価した結果, 図 4－9に示す通り, 0℃～80℃の温度, ±5%の電圧変動に対しても安定に鍵を生成できることを確認した.

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.



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

図 4-8. DTM(Delay Time Measurement)方式アービターPUF と他のアービターPUF の性能比較評価



(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4-9. 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

6)　成果6.「高効率な PL-PUF の開発と PUF の定量的性能評価手法」(産総研グループ)

①内容(原著論文[10])

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 4-10)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.

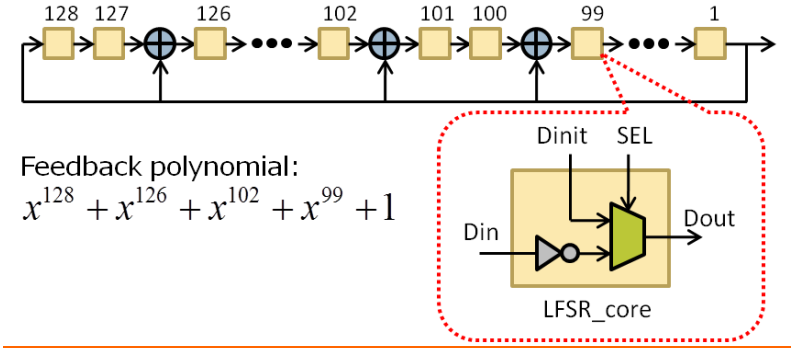


図4－10. Pseudo-LFSR PUF(PL-PUF)の構造

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.

②有用性および③優位性

PUF は認証, 乱数生成, 鍵生成のように暗号システムの重要な構成要素として働くと考えられているが, デバイスのばらつきを利用して同一の回路構成から異なる出力を得ようとする特性上, 出力のエントロピーが低くなってしまうという問題がある. 例えば 128 ビットの鍵を生成するためにはそれ以上の PUF 出力が必要となってしまい, PUF の実用化にはスループットの向上が不可欠である. 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, 従来の PUF の出力は 1bit であるため, 出力に応じてチャレンジ入力を 2 クラスに分類することができ, 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で PUF のクローンを作成できてしまう. PL-PUF の出力は 128 ビットであるため, 機械学習攻撃が極めて困難であると考えられ, クローンの作成は実質的に不可能であると期待される.

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.

3. 2 上記**3. 1**の成果うち、特筆すべきもの

（1） 特に顕著な成果（科学や技術の新しい分野の展望など）

（2） 当初計画で想定外であった重要・新規な展開

§4. 成果発表等

(4－1)原著論文発表

●論文詳細情報

[1] 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)

[2] 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)

[3] 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).

[4] 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).

[5] 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)

[6] K.Ogawa, M.Shiozaki, K.Furuhashi, T.Fujino," Experimental Security Evaluation against Machine Learning Attacks on RG-DTM
PUF", The 27th International Technical Conference on Circuits/Systems, Computers and Communications,C-T1-02,(2012-07)

[7] 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).

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

[9] 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).

[10] Hyunho Kang, Yohei Hori, Akashi Satoh, "Performance Evaluation of the First Commercial PUF-embedded RFID", The 1st International Conference on Consumer Electronics (GCCE2012), pp.5-8, (2012-10).

[11] 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).

[12] 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).

[13] 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)

[14]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)

[15] Anh-Tuan Hoang and Takeshi Fujino, "Hybrid Masking using Intra-Masking Dual-Rail Memory on LUT for SCAResistant AES Implementation on FPGA," 21st ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (FPGA), (2013-02).

[16] Takahiko Murayama, Mitsuru Shiozaki, Takeshi Fujino, “An Arbiter Circuit utilizing Time to Digital Converter Scheme for the RG-DTM PUF”, NCSP 2013 Technical Papers, (2013-03).

[17] Hiroki Ito, Mitsuru Shiozaki, Takeshi Fujino, “Efficient Evaluation Method of Tamper Resistant AES Cryptographic Circuits”, NCSP 2013 Technical Papers, (2013-03).

[18] 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, (2013). 【to be published】

[19] 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, 6 月号掲載予定(2013-6)

[20] 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, 7 月号掲載予定 (2013-6)

(4－2)知財出願

① 平成24年度特許出願件数(国内 1 件)
② CREST 研究期間累積件数(国内 4 件)