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

H25 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. 研究実施体制

(1)「立命館大学」グループ
① 研究代表者:藤野　毅 （立命館大学理工学部、教授）
② 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
① 主たる共同研究者:堀　洋平 （産業技術総合研究所、研究員）
② 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
① 主たる共同研究者: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）
② 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

① 主たる共同研究者:吉川　雅弥　(名城大学理工学部、教授)

② 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

① 主たる共同研究者:吉田　隆弘　(中央大学 研究開発機構、専任研究員/機構助教)

② 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. 研究実施の概要

2. 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，以下のように「ドミノ RSL 方式を耐タンパ LSI 設計技術の中心技術」と記載しており，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（MDR-ROM：Masked Dual Rail ROM 方式と名称変更した）」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としていた以下の記載は，達成できた．特に下記②に関しては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．

上記方式（MDR-ROM 方式）は，消費電力を用いたサイドチャネル方式には目標性能を大幅に上回る攻撃耐性を有したが，三菱電機にて，電磁波を用いたサイドチャネル攻撃耐性を評価したところ，メモリの規則レイアウトに基づく脆弱性が発見された．この問題に対して，SBox 演算時に乗算マスクを導入する HMDR-ROM(Hybrid MDR-ROM)方式を新たに提案し，上記脆弱性が改善されることを確認した．

HMDR-ROM 方式は上記のように，サイドチャネル攻撃に対する高い耐性を持つことが明らかになったが，より強固な耐性を実現するために，クロックのジッターやスキューを意図的に大きく発生させて，サイドチャネル攻撃を困難にする技術の開発を行った．

耐タンパ AES 暗号回路を設計するためには，電力や電磁波を用いた攻撃に対する耐性を検証するツールが必要である．論理ゲートに使われているセルと消費電力の関係を明らかにすることで，攻撃可能なタイミングにおける脆弱要因を推定することが可能になった．（詳細は§3　成果4）

従来本研究において開発および評価の対象としていた暗号回路は，共通鍵暗号回路であったが，発展的なテーマとして，公開鍵暗号における実装安全性の評価技術も開発した．

(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，以下記載の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～D のように発展した．

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．

D. MiMICC： IC カード型 FPGA ボードを（我々の知る限り）世界で初めて開発した．市販のサイドチャネル攻撃ツールは IC カードを評価対象としている．このようなツールを活用して，耐タンパ暗号実装を検討する際には非常に有効な評価基板である．（詳細は§3 成果7）

公的な立場である産総研の役割としてサイドチャネル攻撃や PUF の標準化に関しても，各種委員会に継続的に参加して，成果を上げた．

(3)偽造 LSI を識別する PUF を用いたセキュリティシステム

研究計画当初の下記記載では，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．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．

耐タンパ AES 暗号回路を車載システムに搭載していく活動のデモンストレーションとして，キーレスエントリーを模擬した認証システムを，PUF を用いて作製した．（詳細は§3 成果2）

また上記のようなシステムに搭載する耐タンパ AES 暗号回路とそれに統合できる新しい MDR-ROM を用いた PUF の開発と，PUF 動作の確認を行った．（詳細は§3 成果3）

さらに，PUF を用いて安定な鍵を生成するためのヘルパーデータの作成方法や，ヘルパーデータの容量削減方法に関して研究を行った．

（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.

2. 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. 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)

■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．

■本研究グループの達成目標

§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．

25 年度で，要素技術的にほぼ目標を達成した，かつ，車載向けの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（自動車のキーレスエントリー模擬システム）を構築した．最終年度においては，車載 ECU 間の通信における認証や，ECU プログラムの改ざん防止を耐タンパ AES 暗号回路と PUF を用いて実現するための検討を行う．

■本グループの研究の特徴

（1）耐タンパ AES 暗号回路のチップ実装

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（MDR-ROM 方式と改称）を中心技術として研究を進めた．本チップは三菱電機の評価で，電磁波攻撃に対する脆弱性が指摘され，それを対策するための HMDR-ROM 方式を提案し，チップ試作を行った結果，脆弱性は大幅に改善された．

（2）PUF 回路のチップ実装

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．さらに，25 年度は耐タンパ AES 暗号回路として提案している MDR-ROM を用いた新たな PUF の試作と評価を行った．

■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，「MDR-ROM 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．

（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，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

■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．

■本研究グループの達成目標

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.

■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.

■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

■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.

■本研究グループの達成目標

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.

■本グループの研究の特徴

当グループでは, 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．

■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 「名城大学」グループ

■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．

■本研究グループの達成目標

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，平成 25 年度には，設計段階でのサイドチャネルリーク部分の特定手法を開発した．本手法では，設計段階において，脆弱な箇所のセルまで特定することが可能である．さらに，脆弱と判定した部分に対する対策手法を用いた評価実験によって，提案手法の有効性を実装した．このように，平成 24 年度までに開発した脆弱性を定量的に評価できるシステムと合わせて，総合的な脆弱性の判定が可能になった．次に研究課題(2)に対する進捗としては，平成 25 年度ではフォールトのエラー値に着目した新しい解析手法を考案した．さらに，フォールト攻撃に対する対策手法についても検討した．以上のように，平成 25 年度までに，研究課題(1)と(2)共に，当初計画の 9 割程度の課題を解決した．

■本グループの研究の特徴

(1)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．さらに，設計段階において，チップレベル検証とボードレベル検証とを別々に行うことができ，検証の高精度を実現する．

また，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 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．

(2)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）の値に着目して，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した．さらに，フォールト攻撃に対する対策手法を考案した．

■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(1)に関して，チップレベル検証を実現する CAD の開発を行った．ここでは，電力情報として，昨年度に開発したイベントモデルシミュレーションを使用し，解析手法としては新たにクラスタリングを導入する．これにより，セル単位で脆弱な場所を特定することが可能になる．

一方，研究期間の後半では，(2)に関して，産総研 G が開発した SASEBO ボードを利用して，どのような対策がフォールトに対して有効かについて検証した．ここでは，実際に発生するエラー値を解析することで，効率的な対策手法を考案した．

（3） 領域外部の企業等との連携

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．

2．3　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）

「耐タンパ性 LSI 設計プラットフォーム開発と検証」の研究項目に関しては，前年度まで IO-Masked Dual-Rail ROM（MDR-ROM：前年度まで 2 線 RSL メモリと記載）方式を適用した AES 暗号回路を試作して電力解析攻撃に対して十分な耐性があることを示してきた．しかし，電磁波解析攻撃にも耐性を持つか評価を進めた結果，ROM や RAM といったメモリアーキテクチャにはアクセス・アドレスに基づいた電磁波特有のサイドチャネルリークが存在することを発見した．25 年度はこの新たな電磁波特有のリークに対処すべく対策手法の確立と評価実験を重点的に行う．「PUF セキュリティシステムの研究」の項目に関しては，環境変化によって出力が変わってしまう PUF から安定した鍵生成を実現するための技術開発を行っていく．また，最終的な耐タンパ認証

システムにはサイドチャネル攻撃対策暗号回路と PUF の融合が必要不可欠なので，我々が提案してきた MDR-ROM が PUF としても機能するような新たな PUF 回路を提案していく．

「発展テーマ」として，我々の研究グループが進めてきた耐タンパ LSI 技術がどのような応用が利き，どれ程有効であるのか，広く多くの人に知って貰うため，キーレスエントリーを模した耐タンパ認証システムを開発し，デモンストレーションを行った．

② 「産総研」グループ

24年度までに開発した評価環境を用いて，暗号モジュールのサイドチャネル攻撃評価を行う．特に，前年度の研究において，先端プロセスでは電力より電磁波を利用する攻撃の方が有効であることが分ってきたため，電磁波解析の環境整備や攻撃実験を重点的に行う．また，やや古いプロセスの教育用ボードを用いて防御手法の評価も行ってゆく．PUFにおいては，先端プロセス上の回路の性能評価やクローン攻撃態勢評価を行うとともに，多数のFPGAを用いて統計的な性質を明らかにすることで，PUFの有効性を実証する．また，PUFを用いた動画再生アプリケーションを完成させる．

A. 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

ISO/IEC 7816 準拠の接触型 IC カード上の暗号モジュールの安全性評価を行うため，IC カード型 FPGA ボードを開発する．本ボードを用いて，キャッシュカードや入退室カード等の IC カードアプリケーションの動作時のサイドチャネル攻撃耐性評価を行う．これに加え，立命館大学の耐タンパ性検証用 180nm LSI の評価用 IC ソケット搭載ボードを開発する．本ボードは，24 年度に開発した ZUIHO に接続して使用し，回路の制御は ZUIHO 側で行う．そのため，低コストで他の LSI ソケットに変更することが容易である．

B. 防御手法・解析手法の開発および有効性検証

24 年度に開発した SASEBO-GIII を用いて，28nm の先端プロセス上の様々な実装の AES 暗号回路に対するサイドチャネル攻撃評価を行うとともに，その防御手法について検討する．また，教育用評価ボード ZUIHO 上に同様に AES 回路を実装し，そのサイドチャネル攻撃評価を行う．さらに，今年度新規に開発するソケット搭載評価ボードを用いて，立命館大学の耐タンパ検証用 LSI に対するサイドチャネル攻撃実験を行い，提案防御手法の有効性評価を行う．

C. PUFの実装および測定

28nm の先端プロセス FPGA 上に独自開発の Pseudo-LFSR PUF を実装し，そのユニーク性や再現性等の性能評価を行う．また，24 年度に開発を行っていた機械学習攻撃ツールを用いて，その安全性検証も行う．さらに，ソケット搭載評価ボードに多数の FPGA を搭載し，PUF を実装してその統計的性質を明らかにすることで，PUF の有用性・実用性を検証する．これら PUF の性能評価には，基本的に 22 年度に開発した定量的評価指標を用いるが，その改良が可能であるについても検討する．

D. PUFと暗号技術を融合したセキュリティシステムの構築

24 年度に改良した SASEBO-GIII ボードの上で，PUF を用いたセキュリティシステムのプロトタイプを構築する．バイオメトリクスのように出力の分布統計から個体識別する方式のほか，誤り訂正技術を利用した Fuzzy Extractor によって鍵を生成し暗号技術によって個体識別する方式の実装も行う．既存方式より高効率（小型・高速）な手法を検討し，その性能評価を行う．これらの認識手法や暗号鍵生成手法を用いて，安全に動画再生を行うアプリケーションのデモを完成させる．

③ 「三菱電機」グループ

本年度以降は，H24 年度に発見されたサイドチャネルセキュリティにおける脆弱性の要因評価を継続すると共に，これまでに立命大と議論したセキュリティシステムへの応用に関するプロトタイプ開発を行う．

A. SoC に対する包括的なサイドチャネル評価・対策技術開発

（A-1） 電磁波攻撃におけるリークの機序と攻撃可能レベルの検証を評価する目的で H24 年度にスタンダードセルや SRAM 単体のリークを評価するための TEG を開発し，従来信じられていた対策技術の前提条件が不十分であるという知見が得られた．この結果に加え，さらなる解析を行うことで，電磁波攻撃で必要な安全性の前提条件を明確化する[継続]．

（A-2） H25 年度までに開発した技術をカーセキュリティをターゲットとした場合に重要となる公開鍵暗号方式についても H25 年度までに開発した解析技術を展開する．

B. PUF を用いた SoC のセキュア化技術開発

既存のリバースエンジニアリングツールの能力を解析し，リバース・エンジニアリングに対抗するために必要な安全性条件について検討する[継続]．

C． セキュア SoC の構築とセキュリティシステムへの応用

今年度の立命大Gとの議論に基づき、セキュア無線通信システム構築および車内ネットワークへの応用を想定したデモ開発を支援する．

④ 「名城大学」グループ

今年度の研究の狙いは，「耐タンパ検証 CAD システム」の課題に対して，検証システムを構成するそれぞれの要素技術を開発することである．具体的には，チップレベル検証とボードレベルの検証において，前者では，さらに(a)IP ベース設計と(b)セミカスタム設計のそれぞれにおいて①電力情報，②解析手法，③評価手法を開発する．(a)IP ベース設計では，①電力情報については EDA ベンダーのツールをもちいて消費電 力シミュレーションを行い，②解析手法と③評価手法としては，昨年度までに開発完了している多重線形分析手法を用いて，脆弱性の判定を行う． また，(b)セミカスタム設計では，①電力情報については，SPICE と論理シミュレーションを組み合わせた新しいイベントモデルシミュレー ションを導入する．②解析手法と③評価手法は，新しく考案したクラスタリング手法を導入し，セル単位での脆弱性の評価を実現する．一方，後者 のボードレベル検証では，(a)電力と(b)電磁波に対して，それぞれ①モデリング，②応答波形生成，③観測波形予

測, ④攻撃評価を行う. (a)電力では, ①～④について, まず①では電源系 SPICE モデルを作成し, ②で LSI から観測点までのインパルス応答波形を生成し, ③で LSI の電流波形から畳み込みを行い, ④で予測観測波形を使った CPA による耐性評価を行う. (b)電磁波では, 同様に①～④について, まず ①では EM プローブを含む基板の EM モデル作成し, ②で EM 応答波形を生成するために, FDTD シミュレーションを行い, 電力と同様に LSI から観測点までのインパルス応答波形を求める. そして③では EM 応答波形を使った畳み込みによるプローブ観測波形算出し, ④で予測観測波形を 使った CEMA による耐性評価を行う.
もう1つの「耐タンパドリブン設計 CAD システム」の課題に対しては, フォールト攻撃を対象に要素技術を開発する. 特に, 産総研が開発した SASEBO ボードを利用して, 不正クロックによるフォールトの特性を実験により明らかにして, フォールト解析と対策に利用する.

§3. 成果発表等

(3－1) 原著論文発表

論文詳細情報(国内)

1
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)
(DOI: 10.1541/ieejeiss.133.2134)
2
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
3
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

論文詳細情報(国際)

4[Proceedings]
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)
[Proceedings]
5
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).

6
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)
7
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)
8
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).
9[Proceedings]
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)
[Proceedings]
10
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)
11[Proceedings]
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)
12[Proceedings]
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)
13[Proceedings]
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 (2013.10)
(Outstanding Poster Award) (DOI: 10.1109/GCCE.2013.6664860)
14[Proceedings]
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 (2013.12)
(DOI: 10.1007/978-3-642-41671-2_36)
15
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)
16
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)
17
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)
18[Proceedings]
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 (2014.2) (Outstanding Paper Ward)
(DOI: 10.1109/ICACT.2014.6778915)
19[Proceedings]
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)
[Proceedings]
20
M.Yoshikawa, T.Asai, "Tamper Resistance Verification Method for Consumer Security Products", Proc. of Computational Science & Computational Intelligence, pp.30-33 (2014-3)
21
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,” IPSJ Journal, Vol.55, No.3 (2014.3) (Pre-print 版. 正式版は Journal of Information Processing Vol.22, No.2, 2014.4 に掲載予定.)

（3－2） 知財出願

特許出願件数 （平成 25 年度）

合計	国内	2	件

CREST 研究期間累積件数

合計	国内	6	件