「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

H23 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. チーム全体の研究の概要
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

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．

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 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本研究のアプローチ

（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．

また，PUF 回路は，個人ごとに異なる指紋パターンのように，個々のデバイスがユニークなIDを安定して生成することが求められている．しかし，デバイスのアナログ的なばらつきを利用するため，動作環境等による変動を少なからず生じる．また，出力されるIDを安定させようとすると，PUF 回路が同じようなIDを出力してしまったり，特定のパターンを生成（偽造）する回路ができてしまうといった問題を生じる．このため，PUF 回路にばらつきを増幅させる非線形変換を施したり，環境による変動をエラーとしてとらえ誤り訂正回路を付加するなど，構成がどんどん複雑化する傾向にある．これに対して，生体認証におけるユニークな ID である指紋パターンは，残留指紋からそのパターンを採取して偽の人口指を作成することが可能であるもかかわらず，広く実用に供されている．これは，パターンマッチングと同時に生体検知によって人工指でないことを確認しているからである．また指紋パターンも取得時に歪み等の変動が生じるため，常に同じデータが得られるわけでもない．そこで，PUF 回路においても，生体認証のようにゆらぎを生じる場合のパターンマッチングやその情報量の算出を行う．それと同時に，PUF 回路動作時の消費電力に着目し，それを生体検知と同じように真贋判定に用いる偽造防止技術の開発を行う．これには，サイドチャネル攻撃の電力計測技術を応用する．このようにして，本来は簡単な回路による認証が特徴であったPUF 回路を複雑化するのではなく，PUF 回路を認証するリーダー側の計測技術によってIDの偽造防止や安定性の確保を図ろうとするものである．

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．さらに発展テーマとして提案する，セキュア SoC のシステムレベルサイドチャネル評価では，三菱電機が論理設計,LSI 実装を立命館大学，ボード設計は産総研が担当予定である．(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. 研究実施体制

(1)立命大グループ

①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)

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研究分担グループ長:佐藤 証 （産業技術総合研究所、チーム長）(主たる共同研究者)

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 研究分担グループ長:鈴木 大輔 (三菱電機株式会社 情報技術総合研究所、主席研究員)(主たる共同研究者)

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)名城大グループ

①研究分担グループ長:吉川 雅弥 (名城大学理工学部、准教授)(主たる共同研究者)

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

§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)

(1)研究の成果と自己評価

(1) 成果1.「ドミノ RSL 方式を用いた耐タンパ暗号回路設計方式」(立命館大グループ)

①内容

消費電力が入力および出力演算データ値に依存しない論理ゲートである「ドミノ RSL(Random Switching Logic)ゲート」を暗号回路のサイドチャネル攻撃対象である非線形回路部に適用する耐タンパ LSI 設計方式である. H22 年度はローム 180nmCMOS プロセスで DES 暗号回路を試作し評価を行った. 試作に使用した設計 CAD フローは, 標準的な ASIC フローに対して, 論理合成したネットリストの非線形回路部のみを, 積和標準形の論理合成ツールで再論理合成する処理と, 自動配置配線用のドミノ RSL ゲートレイアウトライブラリを追加する処理を変更している.

②有用性

上記 DES 暗号回路に対して, 電力を用いた一般的なサイドチャネル攻撃である, ハミングディスタンス型 DPA に対して耐タンパ性の検証を行い, CPA 攻撃により, 未対策回路では 1,000 波形の取得で, 48bit のすべての正解暗号鍵を推定できたが, ドミノ RSL 回路では 100 万波形を取得しても, 6bit 以下の正解鍵を不安定に特定することしかできなかった. ただし, 高度な攻撃手法と, 産総研が新しく開発した攻撃評価ボード SASEBO-RII を使用すると, 図7に示すように高度な波形処理の必要な 2nd Order DPA 攻撃により, 100 万波形で 42bit の正解鍵を特定できた. ドミノ RSL 方式の今後の耐タンパ性向上のためにはマスクビットの多ビット化, Sbox 回路の論理合成方法の最適化などが必須であることが明らかになった.

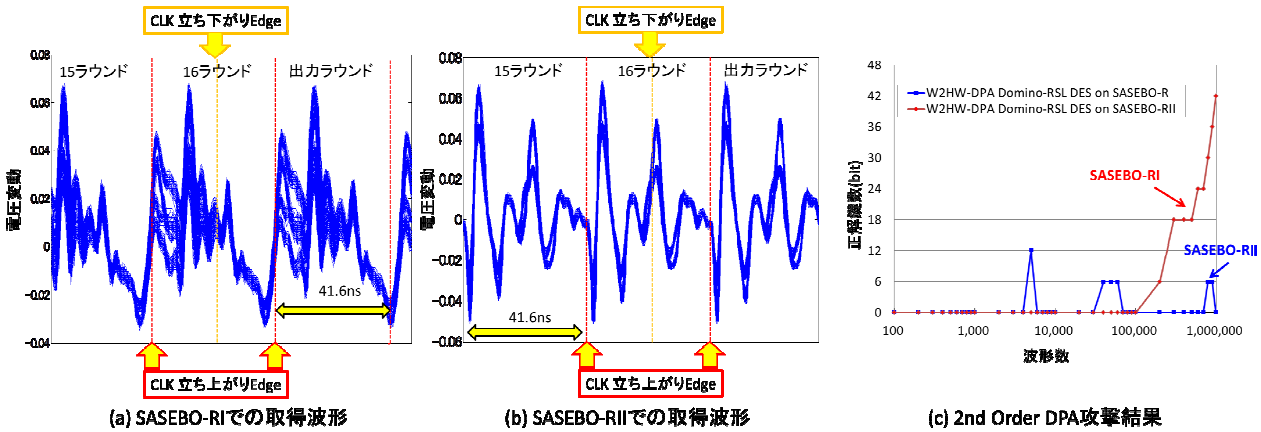


図7. ドミノ RSL 方式耐タンパ DES 暗号回路に対する産総研新型ボード SASEBO-RII による評価結果

③優位比較

従来提案されてきた典型的なプリミティブゲート方式の対策であるWDDL方式と比較すると1st Order攻撃に対する耐タンパ性は高いが，上記脆弱性が問題であり，対策手法を継続検討するとともに，今後は，AES暗号回路に対して検討してきた2線 RSL メモリ方式(次章参照)を DES 暗号回路にも適用することも検討する.

(2) 成果2.「2線 RSL メモリ方式を用いた耐タンパ暗号回路設計方式」(立命館大グループ)

①内容

DES 暗号回路でも，AES 暗号回路でも，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8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 XOR 回路を用いた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，SRAM マクロを使った標準設計 CAD フローで実装可能である.

②有用性

疑似2線 RSL メモリ方式を用いた AES 暗号回路を FPGA に実装して，電力を用いた一般的なサイドチャネル攻撃である CPA(電力相関解析)を用いて耐タンパ性の検証を行った結果を図9に示す. 未対策回路では 1000～数万波形ですべての鍵が導出可能なのに対して，本方式では，100 万波形でも1バイト以下の鍵しか導出できていない. 疑似方式はリークが発生しやすいことが分かっており，ASIC ではより安全性が高いと予想している.

③優位比較

図9に示すように，疑似2線 RSL メモリ方式を用いた FPGA 評価でも，既存の対策手法(WDDL 方式)では，100 万波形で 40%の鍵が導出可能なのに対して，本方式では 6%以下であった. また，ASIC のチップ面積比較では既存の対策手法(WDDL 方式)では，未対策回路の約3倍の面積が必要なのに対して，2線 RSL メモリ方式では，約2倍の面積でレイアウト可能である.

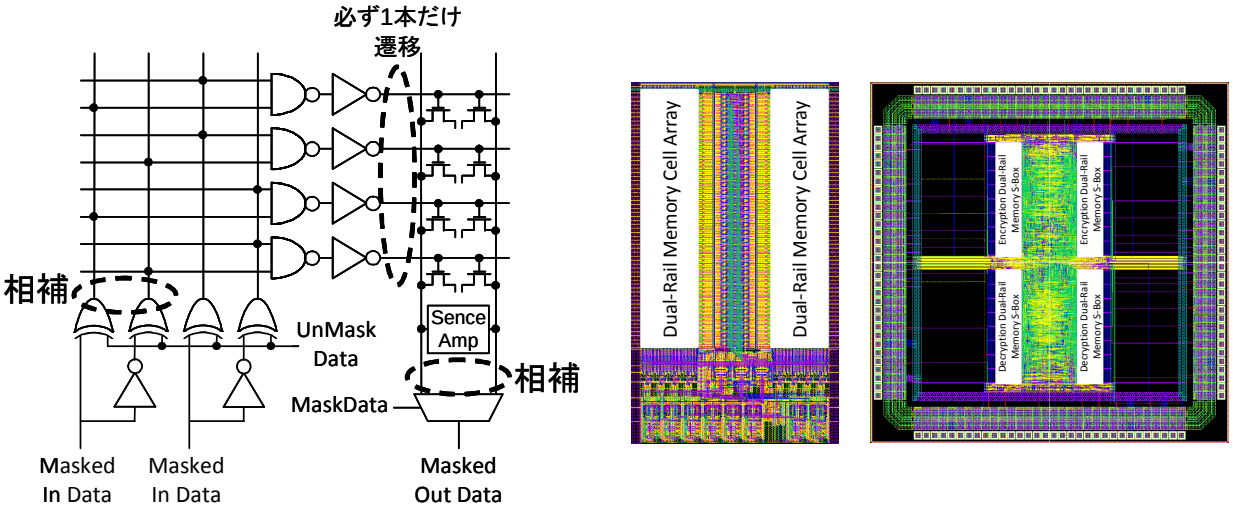


図 8. 2 線 RSL メモリ方式の SBox 部の概念図(左)と 180nmCMOS AES 暗号回路試作チップレイアウト(右)

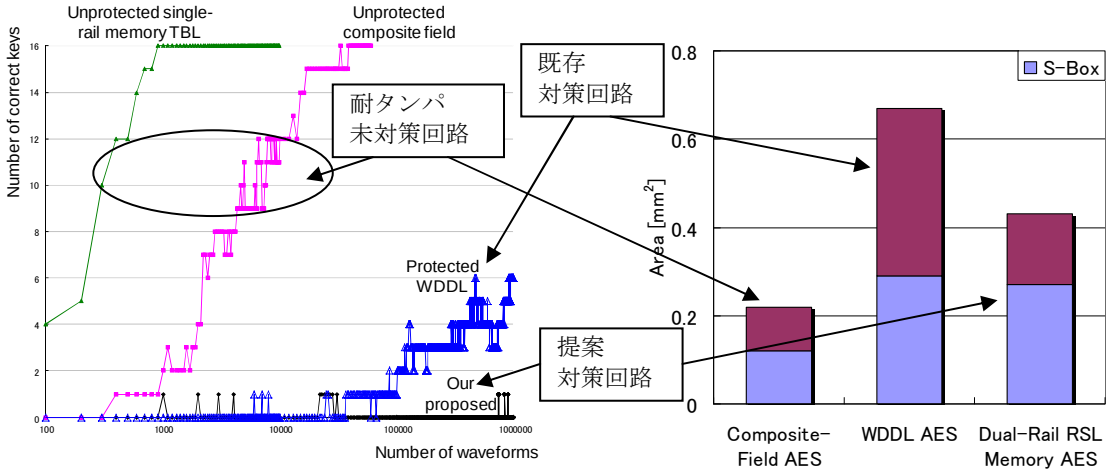


図 9. 既存対策方式(WDDL)との FPGA での耐タンパ性比較結果(左)と ASIC の面積比較結果(右)

(3) 成果3.「DTM 方式アービターPUF 回路」(立命館大グループ)

①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アービター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ている．

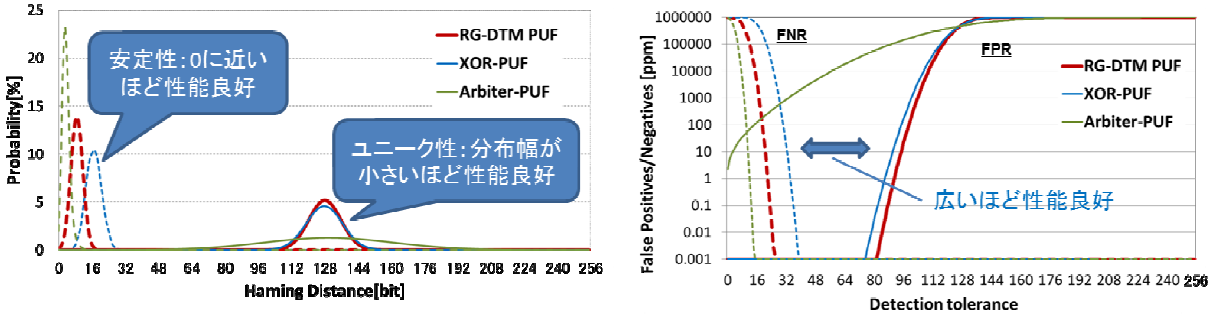
②有用性

デバイス間のユニーク性を示す指標(異なるデバイス間での ID のハミングディスタンス)の分散が理想値より非常に大きくなることを実験的に確認した．これは，アービターPUF 方式の原理的な問題であり，レスポンス ID の出現確率に偏りがあるためである．上記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)型アービターPUF の提案を行った．通常のアービターでは，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，シミュレーションによりユニーク性が向上することを確認できている．

③優位比較

0.18μmCMOS プロセスを用いて，DTM 方式アービターPUF と，従来型アービター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 アービターPUF との比較結果を図 10 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月号に掲載が決定している．



(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 10. 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

(4) 成果4.「暗号モジュールの安全性評価の国際標準化活動」(産総研グループ)

①内容

NIST において FIPS140-3 の制定が予想以上に遅れているため, FIPS140-3(の 2nd ドラフト)をベースに標準化が始まった暗号モジュールの安全性評価の国際規格 ISO/IEC19790 を先行させる活動を始めた. NIST の CMVP(Cryptographic Module Validation Program)のディレクターであり ISO/IEC19790 のエディタでもある Randall Easter 氏が実行委員長, 産総研の佐藤がプログラム委員長となって, 暗号モジュールのサイドチャネル攻撃手法に特化した国際会議 Non-Invasive Attack Testing workshop (NIST2011)を 9 月末に奈良で開催した. さらにそれに引き続き, 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, 国内外の関連企業や研究機関を集めた技術展示会も行った. 300 名を超える参加者の間で活発な議論が行われ, その結果を受けて 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った. 実際にはそのドラフトは Easter 氏と産総研グループの佐藤, 坂根で執筆を行っている. また, ISO/IEC のセキュリティ標準に関する SC27 WG3 国内委員会にも 11 月から佐藤が委員として参加している.

②有用性

IC カードをはじめとする様々な情報機器への暗号実装が進み, 暗号実装の物理的安全性評価手法の標準化, そして評価環境の構築が急務となっている. この上記の取り組みは, 標準化活動を促進し, 暗号製品の安全性向上させる上で大きな成果を上げている.

③優位比較

CHES2012 の技術展示会において, 本事業の成果である SASEBO-RII や小型磁界スキャナーを展示し好評を博している. また, 展示参加 9 団体のうち 8 団体が SASEBO を利用したシステムを構築している. 残り 1 機関は独自の評価ボード開発を行っている韓国の公的研究機関 ETRI であったが, 先方からの要請を受けて産総研との間で共同研究契約を締結した. このように, 産総研の研究成果は国際標準化に伴う評価環境の構築においても高い優位性を有している.

(5) 成果5.「サイドチャネル評価環境の構築」(産総研グループ)

①内容

本事業で開発した暗号 LSI の解析用に, 新規の SASEBO-RII ボードを開発した. プロセスの進歩に伴い電源電圧は低下し, 消費電力に漏洩するサイドチャネル情報の解析が困難となる. 評価試験では可能な限りノイズの少ない環境で解析を行う必要があるため, これまでの実験のノウハウを活用し, ノイズの低減をはかった図11 の SASEBO-RII ボードを開発した. これまでは解析対象毎にボードを開発していたが, 製造期間, 製造コスト, そして動作試験に多くのエフォートを費やしていた. そこで, 市販の SASEBO-W ボード上のドーターカードとして開発を進めることで, これらの問題を解決した. さらに, 設計から部品実装までのすべてをプロジェクトメンバー自身で行うことにより設計データの再利用が容易となり, パッケージ形状や電源電圧が全く異なる立命館大学の LSI 用の評価ボードも短期間で開発することができた.

安価でかつ S/N 性能の高い SASEBO-RII の短期開発に成功したことを受けて, 従来の SASEBO ボードは基本設計を行った後の回路設計やレイアウトは全て外部の企業に委託していたが, 新規の SASEBO-GIII 設計を全て研究チーム自ら行った.

さらに, SASEBO-RII および GIII 用として, 位置精度 100um 以下の 3 軸磁界スキャナーも開発した.

これまで産総研の内製ツールでサイドチャネル攻撃を行っていたが, 市販の IC カード解析ツールとして最もシェアの大きい Riscure 社の INSPECTOR にも SASEBOI ボードを対応させた.

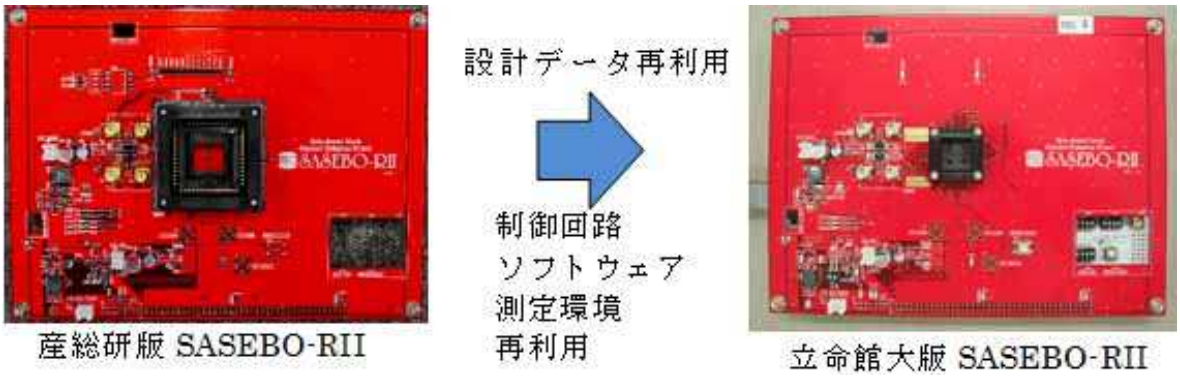


図 11. SASEBO-RII の開発

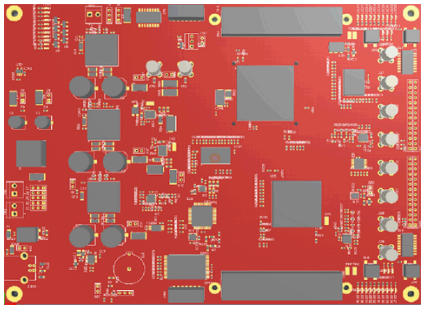


図12.　SASEBO-GIII

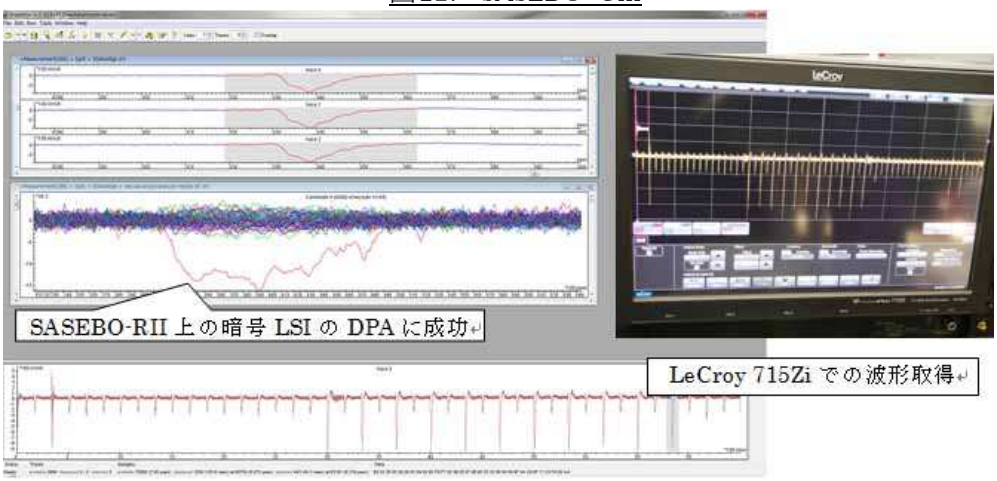


図13. Riscure 社ツール INSPECTOR による SASEBO-RII 上の AES 回路の解析

②有用性

新規開発の SASEBO-RII は図14 に示すように，65nm プロセスによる暗号 LSI の AES 回路の消費電力波形を，既存の SASEBO-R 上および新規開発の RII 上で計測した比較から，RII の振幅が大きく応答性能も早く，明らかに S/N が改善されている．

一般のボードは低電力化や放射電磁波を低減する設計が重視され，サイドチャネル情報の測定・解析に適した設計といったことはまったく行われていない．これに対して，SASEBO-RII や SASEBO-GIII では電源回路やクロック生成部，制御信号へのディファレンシャル線採用などのサイドチャネル攻撃実験のノウハウを集約したノイズ対策の数々の工夫が施されている．

磁界計測は従来，EMC/EMI 対策のためのスペクトルアナライザによる周波数領域での強度解析が中心であった．それに対して，サイドチャネル攻撃では時間波形中の漏洩情報を解析する．今回開発した磁界スキャナーは，暗号回路制御ソフトウェアにより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取得することを可能とし，指定時間中の情報を解析するツールや，INSPECTOR との連動等も目指している．

(a) 全体　　(b) 拡大

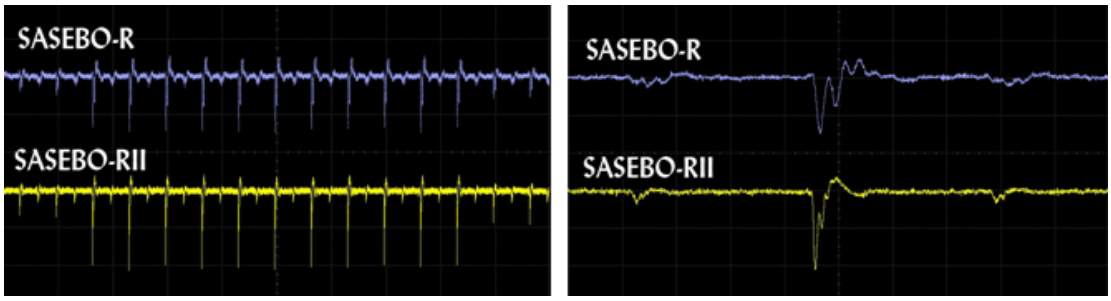


図14. SASEBO-R と RII 上での 65nm プロセスの AES 回路の電力波形比較

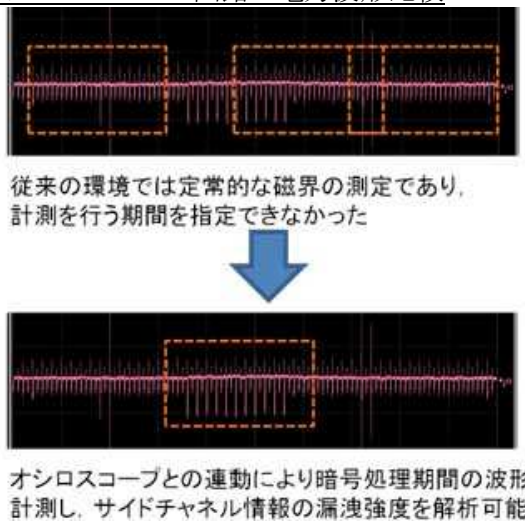


図15. SASEBO-RII を実装した状態の小型磁界スキャナー(左)とオシロスコープ連動による磁界計測(右)

INSPECTOR への SASEBO ボードの接続により，INSPECTOR の解析ルーチンを，本研究グループの暗号 LSIの解析に活用することが可能となった．

③優位比較

SASEBO-GIII はサイドチャネル攻撃評価用としてだけでなく，セキュリティシステムの実装を可能とする大規模 FPGA の利用，高い拡張性を有する FMC 仕様に準拠したコネクタの具備，正式にサポートされた動的再構成機能の適用など様々な改良と性能向上を実現すべく開発を行っている．特に，FPGA には，28nm テクノロジにより製造される販売前の最新の Xilinx Kintex-7 の情報を総代理店である東京エレクトロンデバイス社から入手し，試作においては ES 品を優先的に提供してもらっている．

既に他事業で製品化している SASEBO-GII に対して，性能と機能を大幅に向上させた SASEBO-GIII は，製品としても非常に魅力のあるボードで，サイドチャネル攻撃用途以外にも利用が見込まれている．特に本事業では，PUF と暗号技術を融合したセキュリティシステムの構築として，SASEBO-GIII 上に立命館大学の PUF をドーターカードとして実装するプロトタイプの設計を進めている．現在は PUF の出力を PC 上で識別・認証しているが，ボード上で個体識別と固有鍵の生成を行う．また，プロトタイプではアプリケーションとして動画再生システムの実装・評価を行う予定である．

産総研の内製ツールは 64bit アドレスのマルチコアプロセッサを対象として C#で開発し，十数 GB のメモリ空間と並列処理による高速な解析を行っていたが，以前のINSPECTORでは 32 bit プロセッサ用に開発され，産総研の解析し手法の移植が困難であった．そこで，Riscure 社に 64bit 対応を要請し，これが最新バージョンで実現されたことから，今回の SASEBO-RII の接続と解析が可能となった．今後は SASEBO-GIII や磁界スキャナーのポーティング，そして産総研の解析手法の実装も予定しており，本研究の成果が市販ツールを通じて暗号モジュールの評価に広く活用されることが期待される．

(6) 成果6.「PUF の定量的性能評価ツール」(産総研グループ)

①内容

バイオメトリクスの手法を適用した PUF の定量的性能評価手法を整理し，SASEBO-GII 以外の PUF も評価できるよう汎用ツールを開発し，SASEBO-GII 上の Arbiter PUF のサンプルデータとともに Web での公開を行

った. また, 立命館大グループの PUF チップも同ツールによって評価中である. このツールは PUF が生成する固有データの ID としての識別可能性と安定性を評価するものであり, 数学的にチャレンジ-レスポンスが模擬可能かどうかのクローン耐性を測るものではない. そこで, 立命館大学の PUF にも利用しており, 最もポピュラーな Arbiter 型の実装に対して, 数学的クローンを行う機械学習攻撃ツールの実装を始めている. また, 耐クローン性能に強いと期待される新方式の PUF を開発し SASEBO-GII 上に実装して性能評価を行った[(1)-9][(3)②-3].

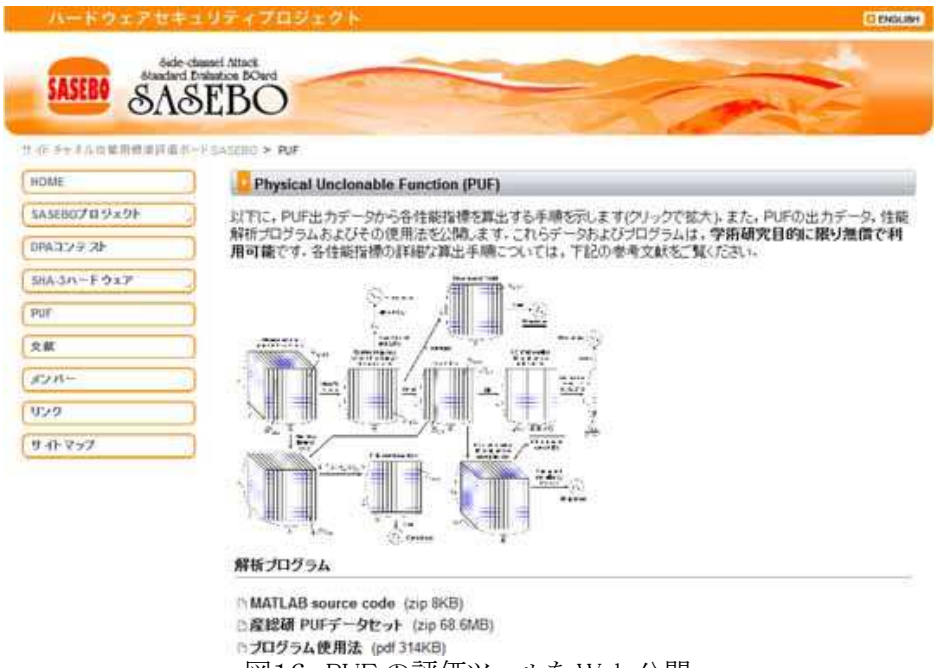


図16. PUF の評価ツールを Web 公開

②有用性

これまでアドホック的に評価を行っていた評価手法を整理し汎用ツールとして公開したことで, 様々な PUF の性能を同じ指標で比較できることになる.

③優位比較

本ツールのように, バイオメトリクスの手法を PUF 評価に取り入れたツールは公開されておらず, SASEBO のアプローチと同様に評価指針の標準化が期待される.

(7) 成果7. 「電力解析攻撃に対する脆弱性評価手法」(名城大グループ)

①内容

本研究で提案する脆弱性評価手法では, 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。さらに, 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。

②有用性

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 通りを対象に行った評価実験では, 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。また, (1)トランジスタレベルのシミュレーションで求めた消費電力データによる解析と, (2)ゲートレベルのシミュレーションで求めた消費電力データによる解析のどちらの場合においても, 電力解析攻撃に対する耐性を高い精度で評価することが可能であることを確認した。

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。

③優位比較

標準暗号 AES を対象に，提案手法と従来の攻撃シミュレーションの処理時間を比較した場合，数十倍の高速化を実現した。これは，提案手法が消費電力データをもとに重回帰分析をベースとした解析を行うだけなのに対し，従来の攻撃シミュレーションでは 8 通りの選択関数（SubBytes 変換の入力 8bit に対応）について，全ての部分鍵の候補(部分鍵が 8bit のため 256 通り)に対して DPA を行う必要があるからである。さらに提案手法では 2000～4000 パターン程度のテストベンチで脆弱な場所を特定する解析を行うことが出来るが，一般的な攻撃シミュレーションでは，数千から数万パターンのテストベンチを使用して，攻撃箇所を変更してシミュレーションを行う必要があるため処理時間の差は大きなものになる。

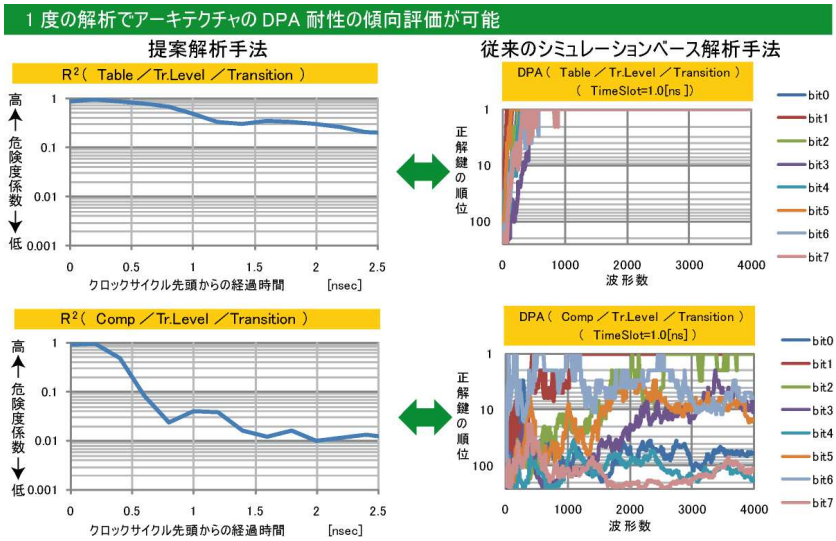


図17. 提案脆弱性評価手法（1 回の解析でアーキテクチャの脆弱性がビット単位で判定可能）

(8) 成果8.「秘密鍵生成回路の開発」（立命館大・三菱電機グループ）

①内容

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を国内で始めて開発した。また、グリッチ PUF の原理に基づいた乱数発生回路もあわせて開発した。本回路を搭載した LSI は e-Shuttle 65nm プロセスで製造され 2012 年 2 月に納品予定。

②有用性

PUF 単体では生成されるデータが不安定なビット列となるため、そのままでは暗号機能との融合が達成できない。本回路によって安定的にビット列が生成可能となり、暗号に用いる鍵情報として PUF のビット列を利用できる。これにより PUF と暗号機能の融合に一歩前進する。また、フロントエンド計段階での性能見積もり、バックエンド設計段階での性能見積もり、および最終的な LSI での PUF の性能比較が可能となり、今後 PUF の設計フローの改善に有用なデータを取得できる。

③優位比較

欧州及び米国では先行してPUFの試作チップが完成している。特に欧州の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は当研究チームで提案している方式と比較して、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。従って、方式としては当研究チームの方式に優位性があると考えており、実績での課題を今後解決していく。

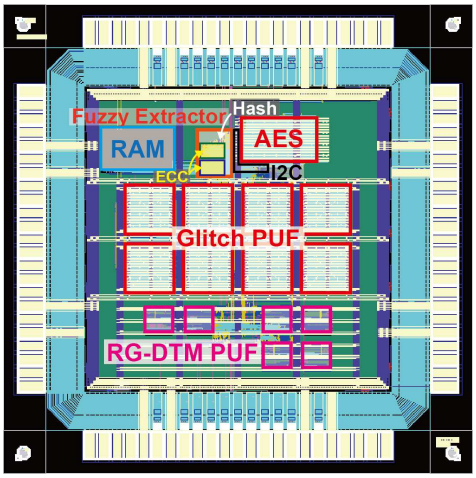


図 18. グリッチ PUF 回路，誤り訂正回路，汎用ハッシュ関数回路による鍵生成回路を搭載したテストチップ

(9) 成果9.「FSA シミュレータの開発」(三菱電機グループ)

①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。

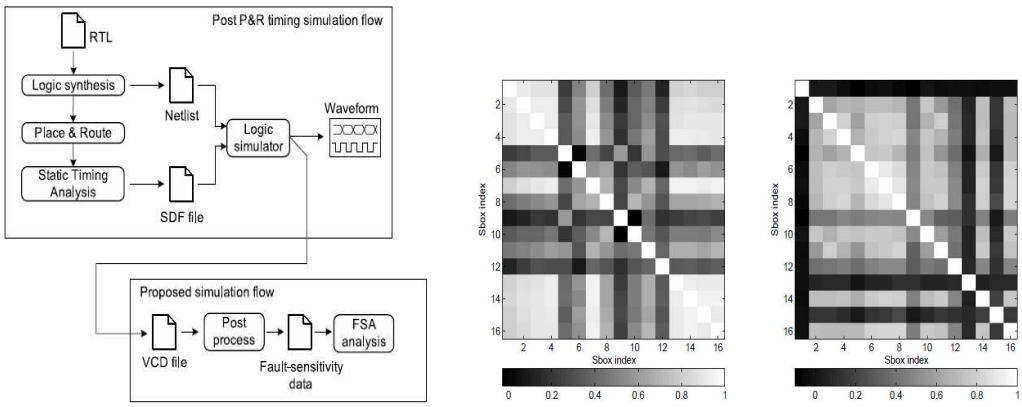


図 19. 開発した FSA シミュレータの動作フローと結果(右図の白色は脆弱性のあるモジュールを意味する)

②有用性

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。

③優位比較

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。

§4. 成果発表等

（4－1)原著論文発表

●論文詳細情報

[1] 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, May 2011.

[2] 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, June 2011.

[3] 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, June 2011.

[4] M.Yoshikawa, K.Sakaue, "Dedicated hardware for RC5 cryptography and its implementation", Proc. of International Conference on Embedded Systems and Applications, pp.135-139,(2011-7)

[5] M.Yoshikawa, M.Sugiyama, "Multi-rounds masking method against DPA attacks", Proc. if IEEE International Conference on Information Reuse and Integration, pp.100-103, (2011-8)

[6] M.Yoshikawa, Y.Kojima, "Efficient random number for the masking method against DPA attacks", Proc. of International Conferences on Systems Engineering, pp.321-324,(2011-8)

[7] 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)

[8] 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, (2011-11)
DOI: 10.1541/ieejeiss.131.1940

[9] 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. December 2011.

[10] 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,(2012-1)

[11] 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), Feb. 2012.

[12] 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,(2012-3)
DOI: 10.1541/ieejeiss.132.364

[13] 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 (2012-3)

[14] 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 (2012-3)

[15] 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 (2012-3)

[16] M.Yoshikawa, T.Asai, "Dedicated Evaluation System for Fault Attacks", Proc. of International Conference on Information and Computer Networks, vol.27, pp.254-257, (2012-2)

[17] 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 (2012-3)

(4－2)知財出願

① 平成22年度特許出願件数(国内 3 件)
② CREST 研究期間累積件数(国内 4 件)