レーザー故障注入攻撃対策を備えた暗号ICの設計手法

松田 航平[1]　藤井 達哉[2]　庄司 奈津[2]　菅原 健[2]　崎山 一男[2]　林 優一[3]　永田 真[1]　三浦 典之[1]

概要：本稿では, レーザー故障注入攻撃対策を備えた暗号 IC の設計手法を提案する. シリコン基板へのレーザー照射に伴い, 基板内部において異常な過渡電流が発生することが知られている. この過渡電流を検知するための小面積基板電流センサを分散配置した暗号コア回路の設計手法について提案を行う. また, 攻撃検知後の対策手法として, 暗号コアへの電源供給路に挿入しコアへの電源供給路を切り替える電源瞬断回路によって, 内部データ消去を行う手法を提案する. 本稿では, 提案手法の有効性を確認するため, 0.18 µm CMOS プロセスにおいてテストチップを試作し, 無対策暗号コアと比較し+28%の面積オーバヘッドでレーザー故障注入攻撃を無効化可能であることを確認した.

A Design Methodology of Secure Cryptographic Processor against Laser Fault Injection Attack

Kohei Matsuda[1]　Tatsuya Fujii[2]　Natsu Shoji[2]　Takeshi Sugawara[2]　Kazuo Sakiyama[2]
Yu-ichi Hayashi[3]　Makoto Nagata[1]　Noriyuki Miura[1]

Abstract: This paper proposes a design methodology of compact countermeasure against Laser Fault Injection (LFI) attack on cryptographic processors. A compact bulk-current sensor senses abnormal transient bulk current caused by laser irradiation on a silicon substrate. The single sensor size is only $286\,F^2$/Cell and it is distributed across the entire cryptographic core. After attack detection, a flush code eraser switches the core supply path to quickly erase internal data. A test chip mounted 128-bit Advanced Encryption Standard (AES) was designed and fabricated in 0.18 µm standard CMOS. A protected AES processor can disable LFI attack with only +28% layout area penalty compared with an unprotected core.

1. はじめに

近年の情報化社会の発展に伴い, 暗号デバイスが個人情報や機密情報を保護するために身の回りの様々な場面で使用されている. しかし, これらのデバイスにおいて, 実装されたハードウェア由来の脆弱性に着目した物理攻撃により, 内部の秘密情報が容易に解析可能であるということが広く知られている. 典型的な物理攻撃の一つとしてサイドチャネル攻撃 [1, 2] がある. この攻撃は動作中の暗号デバイスから漏洩する消費電力や電磁波, 処理タイミング等を解析することにより, 暗号処理に使用された秘密鍵を解析する攻撃である.

また, より深刻な脅威として, サイドチャネル攻撃と比較し, より強力な物理攻撃である故障解析攻撃 (Fault Attack: FA) がある. この攻撃は動作中の暗号デバイスにおいて意図的に動作不良 (フォールト) を発生させ, そこから得られる誤った処理結果と正常な結果との差分を解析することにより, 処理に使用された秘密情報を解析する. FA は 1997 年に公開鍵暗号への攻撃手法として Boneh らにより提案された [3]. 同年, Biham らにより共通鍵暗号方式に適応可能な攻撃として差分故障解析攻撃 (Differential Fault Analysis: DFA) が提案された [4]. DFA は, フォールト注入による誤り暗号文と正常な暗号文を収集し, 暗号アルゴリズムにおける故障発生モデルに基づき解析を行うことで, 従来の物理攻撃と比較し, 探索する鍵空間を大幅に削減することが可能である. 実際のアプリケーションに対する DFA については, Advanced Encryption Standard(AES) に対する DFA 攻撃が Piret らにより試みられている [5]. この攻撃

[1] 神戸大学
[2] 電気通信大学
[3] 奈良先端科学技術大学院大学

に関して, わずか 2 組の誤り暗号文と正常な暗号文のペアにより, 128bit の秘密鍵鍵のうち 116bit が解析可能であるという解析結果が報告されている [6]. また, 異なる手法の攻撃として, デバイスのフォールトに対する感度に着目した故障感度解析 (Fault Sensitivity Analysis: FSA) が 2010 年に Li らにより提案された [7]. FSA では, 誤り暗号文と正常な暗号文のペアは解析に不要であり, 攻撃に伴うコストを大幅に削減することが可能である. このように, FA の手法は急速な発展を遂げており, 根本的かつ効果的な対策手法の確立が必要とされている.

様々な故障注入手法の中で, レーザーを使用しフォールトを注入するレーザーフォールト注入攻撃 (Laser Fault Injection: LFI) [8] は, 最も強力な攻撃の一つであると考えられている. DFA における解析コストは, デバイスへのフォールト注入の精度に大きく依存する. 高いフォールト注入の制御性は, より正確な故障モデルの構築に寄与し, 結果として DFA/FSA の効率を飛躍的に高めることが出来る. 究極的には, 動作中の暗号デバイスにおいて適切なタイミングで, ある 1 ビットのデータレジスタへフォールトを注入し, 解析を行うことが最も強力な攻撃となる. この点, LFI は高いフォールト注入の時間・空間分解能を持ち, AES 動作中のあるクロックサイクルで動作する特定のデータレジスタに対してフォールトを注入するといったことが可能である.

よく知られている LFI への対策手法としては, まず冗長化した暗号コア・暗号処理を用いる手法が提案されている [9, 10]. 暗号コアを冗長化する手法では, 複数の暗号コアにより同時に暗号処理を行い, 結果を比較し検証することでフォールトの注入を検知する. また, 暗号処理を冗長化する手法では, 暗号化を行った後, その結果を復号し入力平文と比較することでフォールト検知を行う. しかし, これらの手法は必然的に面積や消費電力が 2 倍以上となってしまうことが大きな課題となる. 更に正確にタイミングと照射位置をコントロールされた複数のレーザー照射により, これら対策が無効化されてしまうということが報告されている [11]. これらの対策手法は, 暗号処理の結果というフォールト注入に伴う副次的な現象に着目しているため, 必然的に効果が限られてしまうため, より根本的に, フォールト注入に伴う物理現象を利用する, 低レイヤの対策手法を構築することが必要となっている.

物理レベルの LFI 対策手法の一つとして, まず, IC チップにおけるメタル配線層を利用してチップ上面にメタルシールドを形成し, 表面からの LFI に対して暗号コアを保護するというものが考えられる. しかし, この手法ではシリコン基板を透過する近赤外線のレーザーを用いて, 裏面 LFI を行うことにより攻撃を行うことが可能であるという報告が存在する [12]. また, 別の手法として, 温度センサや光検出センサを用いて暗号コアへのレーザー照射を検知するという手法も考えられる. しかし, 1bit のフォールトを発生させるためにフォーカスされたレーザー照射により発生する光, 温度変化は非常に局所的なものとなり, これをコア全体で検知するためには高密度なセンサ配置が必要となってしまう. また, これらのセンサ出力はアナログ信号となり, デジタルモジュールである暗号コアで使用するためには, 外部にアナログ・デジタル変換器 (Analog-to-Digital Converter: ADC) が必要であることも面積オーバヘッドの増加につながる.

本稿では暗号コア全体において LFI を検知可能で, かつ, 検知後の対策までを統合した暗号プロセッサの設計手法について提案を行う. この対策手法はコア全体に分散配置された LFI 検知用の基板電流センサと, コア内部データ消去用の電源瞬断回路から構成されている. レーザー照射に伴い発生する異常な過渡電流は, 共通基板上の広い範囲へ伝搬するため, スパースに配置した電流センサで容易に検出可能である. また, 攻撃検知信号を受けて暗号コアへの電源供給経路を切り替え, 内部電荷を急速に放電することにより内部データを不定値とし, 秘密鍵解析に必要な誤り暗号文が出力されることを防ぐ. 本稿では, 0.18 µm CMOS プロセスにおいて提案手法を統合した AES コアを試作し, 無対策 AES コアと比較し+28%の面積オーバヘッドで LFI を無効化可能であることを確認した.

本稿の構成は下記のとおりである. 第 2 章では, LFI の物理的なメカニズムと, それを利用した LFI 検知センサの構成について述べる. 第 3 章では, LFI 検知後の対策として暗号コアに統合される, 内部データ消去を目的とした電源瞬断回路について説明を行う. 第 4, 5 章では, 提案手法の有効性確認のため本研究で試作したテストチップと測定系, そして実際にレーザーモジュールを使用し得られた評価結果について述べる. 最後に第 6 章にて本稿の結論を述べる.

2. LFI 検知センサメカニズム

2.1 LFI の物理メカニズム

まず, レーザーによるフォールト注入のメカニズムは, 従来より LSI で問題となっているソフトエラーと同一であることが知られている [13, 14]. ソフトエラーとはメモリ回路等で発生する一時的なデータエラーであり, 主に宇宙線や放射線等の電磁波が原因となる. シリコン基板内部の PN 接合部近傍に電磁波が照射されると, 基板内部で電子正孔対が生成される. 周囲にバイアス領域がない場合, この電子成功対は緩和プロセスを経て瞬時に消滅し, 回路動作に影響を与えることは無い. しかし, CMOS 回路のように周辺にバイアス領域が存在する場合, 電子成功対は消滅せず, NMOS, PMOS においてそれぞれ電源・グラウンド電圧へバイアスされているバックゲート領域へ流入する. その結果, 基板内部で異常な過渡電流が発生し, メモリ回路が充放

電されることにより, 保持しているデータのフリップが発生する.

近年のプロセスの微細化に伴い, ソフトエラーに対しての傾向 [15] と同じく, デバイスはより LFI に対して脆弱になっている. 一方, デバイスサイズの縮小に伴い, 暗号コア内部の特定のレジスタを狙う場合, レーザー照射位置の制御についてはより困難になっている. しかし, 波長の短いのレーザーを用いて集光性を高め, また, より正確な位置制御機構を使用することで依然として LFI は現実的な脅威になると考えられる.

2.2 Bulk Built-In Current Sensor (BBICS)

ソフトエラー検知手法の一つとして, 前節で述べたような, ビットエラーに伴い発生する異常な基板電流を検知する Bulk Built-In Current Sensor (BBICS) が提案されている [16, 17]. これは, MOS トランジスタのバックゲート端子と電源グラウンド端子との間に, 小さな抵抗素子と増幅器を挿入し, 異常な基板電流をセンシングするという手法である. MOS トランジスタのバックゲートで発生する電流は, 通常の動作時においてはごくわずかである. これと比較し, レーザー照射時に発生する過渡電流は mA のオーダーとなるため, このような手法により容易にセンシングすることが可能である. 電圧増幅器の出力は, 0, 1 のデジタル値を保持しているクロスカップルインバータへ接続されており, LFI に伴う過渡電流により, この保持している値が反転することにより, 攻撃検知信号が生成される. 最終的なセンサの出力がデジタル値となるため, 外部 ADC は不要となり, そのまま暗号コアやインタフェース等のデジタル回路で使用することが可能である.

2.3 暗号コアへの BBICS 統合手法

BBICS は低消費電力でレジスタへの LFI を検知することが可能であるが, 暗号プロセッサへの実際の統合手法についての議論はあまりなされていない [16–18]. 本稿では, 2015 年に Champeix らにより提案された改良版 BBICS について, 面積オーバヘッドを抑えつつ暗号コアへ統合するための設計手法を提案する. 本設計手法では, BBICS を基板電流をセンシングするフロントエンド部と, アラーム信号を生成するバックエンド部に分割し実装する. フロントエンド部は PMOS, NMOS の基板電流をセンシングするための抵抗素子と増幅器となる計 4 つのトランジスタのみで構成され, 暗号コアを構成するトランジスタ群の各バックゲートへと接続され異常な基板電流のセンシングを行う. フロントエンドモジュール 1 つあたりのレイアウト面積は $286\,F^2$/Cell（およそ NAND ゲート 2.6 個分）であり, 暗号コア全体を LFI 検知範囲とするため, 格子状に分散配置されている. また, センサ感度を最大化するためには, LFI に伴う過渡電流経路をセンサフロントエンド部へ限定する必要があるため, 基板コンタクトを含むタップセルは全て除去されており, スタンダードセルへの基板バイアス電圧はセンサフロントエンドを通して供給される.

センサ感度と配置間隔の設計については, [19] で報告されている事前の特性評価結果に基づいて決定した. [19] では, 暗号コア中のデータレジスタを構成している DFF へのレーザー照射に伴い基板内で発生する電流について, オンチップモニタ回路を用いて測定された基板電位変動に基づいた解析が行われている. この解析は実測結果に基づいたものとなっており, 半導体中の不純物濃度等の設計者が知りえない情報を使用することなく, シンプルな等価回路をもって過渡電流強度についてモデリングが行われている. センサ感度については, この結果を踏まえた上で, 十分な検知マージンを確保しつつ設計を行った. 合わせて, [19] では過渡電流の基板内伝搬特性についても評価が行われている. 暗号コア中における X 軸方向のセンサ配置間隔については, この結果を踏まえて 60 µm と決定した. また, Y 軸方向の配置間隔については, 各行で分割された n-well において 100%の検知率を保証するため, 5 µm とした.

フロントエンド部の出力は電流となるため, ある一定の数ごとにバックエンド部へワイヤードオア接続することが可能である. このようにすることで, バックエンド部の必要数を削減でき, レイアウト面積オーバヘッドを小さく抑えることが可能となる. ワイヤードオア接続の比率を設定するにあたり, センサ感度, 面積オーバヘッド, 検知範囲の冗長性の 3 つのトレードオフについて考慮する必要がある. 今回の設計では, PVT ばらつきを考慮したシミュレーションを行った上で, 15 個のフロントエンド部毎に 1 個のバックエンド部へのワイヤードオア接続とした. 暗号コア中の各列ごとに 3 個のバックエンド部が割り当てられており, 検知範囲の冗長性を確保したものとなっている.

3. 内部データ消去用電源瞬断回路

暗号コア内部からの秘密情報漏洩を防ぐためには, LFI を検知するだけではなく, 検知後の対策までを統合する必要がある. LFI 検知後の対策として, 本稿ではセンサからのアラーム信号を受けて作動する暗号コアの電源瞬断回路を提案する. これは暗号コアへの電源, グラウンドパス間にスイッチを挿入し, 攻撃検知信号を受けてスイッチを切り替えることにより, 暗号コアをフローティングとする手法である. また本提案手法では加えて, 暗号コアの電源グラウンド間を短絡させる経路にもスイッチを設けることにより, 急速に暗号コア内部の電荷を放電させ, 内部データを不定値にすることが可能となっている. 本提案手法のメリットとしては, まずフリップフロップのリセット信号を用いる手法と比較し高速であることが挙げられる. リセット信号によるデータ消去に必要な時間は, 暗号コア内部のリセット信号から DFF までの配線遅延に依存してしまう.

しかし, 提案手法では暗号コア内部に低インピーダンスでくまなく配線されている電源を根本から遮断することにより, より迅速なデータ消去が可能となる. また提案手法は, 暗号コアをグローバル電源配線よりフローティングにすることにより, データ消去プロセス中に発生するサイドチャネル情報の漏洩を防止することが可能である. リセットによるデータ消去では, グローバル電源配線に内部秘密情報に依存したサイドチャネル漏洩が発生し, 攻撃者が外部からこの情報をプロービングすることにより情報漏洩が発生する可能性が存在する. その点, 提案手法ではグローバル電源配線を通してのサイドチャネル漏洩経路が遮断されているため, より安全であると言える [20].

4. 測定系セットアップ

4.1 評価用試作チップ

本研究では, 提案手法の有効性を確認するため, 0.18 µm 標準 CMOS プロセスにおいて, テストチップ試作を行った. 対策回路を統合する対象としては, 現在広く使用されている 128bit AES 暗号プロセッサを選択した. AES コアはラウンドベース構造となっており, 128bit の鍵レジスタと中間値レジスタを持ち, 各ラウンド処理によりレジスタ値の更新が行われる. また, 本試作チップには比較のため, 無対策のものと対策回路を統合したもの, 2 つの AES コアが搭載されている. それぞれの AES コアは, 一般に用いられている自動設計ツールを用いて設計が行われている. 2.3 節で述べたように, 対策回路搭載 AES コアには, コア全体において LFI を検知するため, X 軸方向では 60 µm, Y 軸方向には 5 µm 間隔でセンサフロントエンドが分散配置されている. 対策回路搭載 AES コアのレイアウトサイズは 570 µm x 280 µm であり, コア中には合計で 336 個のセンサフロントエンドと 16 個のセンサバックエンド, 電源瞬断回路が搭載されている. 対策 AES コアの合計面積オーバヘッドは, 比較のために搭載されている無対策 AES コアと比較すると+28%であった.

4.2 評価システムセットアップ

前節で述べたテストチップは, 表面を露出した状態で評価ボード上に搭載され, ワイヤボンディングで接続されている. 加えて, 評価ボード裏面には, 裏面 LFI を目的とした小さな穴が試作チップの直下に設けられている. 実験で使用するレーザーソースについては, 波長 970 nm の物を選択した. シリコン基板を貫通する近赤外線のレーザーを用いることで, 暗号コア上部のメタル配線層を避けつつレジスタへのフォールト注入が可能であるため, 本実験においてもそれについて考慮したセットアップとした. レーザーの照射スポット径は 50 倍の顕微鏡を通して直径 2 µm まで集光される. また, レーザー照射位置を X, Y, Z 軸方向に 1 µm 刻みで, DC サーボモータにより自動制御可能なシステムを使用して実験を行った. レーザースポット径と照射位置制御については, 0.18 µm CMOS で設計された暗号コアに対して LFI を行うには十分な精度が確保されている. また, 提案 LFI 検知センサは基板上に広がる過渡電流をセンシングするため, このような精密なレーザーシステムによる LFI に対しても, スパースな配置が可能である. 照射するレーザーのパルス幅については, 長くなるほど暗号コアへレーザーが与える影響は強くなり, 一定の強度を超えるとトランジスタの破壊が発生し, 暗号処理においてパーマネントエラーが発生してしまう. 本実験では, これを避けるために, ソフトエラーが発生する最小のパルス幅として 60 ns と設定した.

5. 評価結果

5.1 AES 暗号コアのフォールト感度評価

まず, AES コア中のデータレジスタを構成する DFF のフォールト発生感度について評価を行った. 暗号コア中の DFF を含む範囲でレーザー照射位置を 1 µm 刻みで掃引し, フォールトが発生する照射位置の特定を行った. フォールト注入のタイミングは, 最も効率の良い DFA が可能であるとされる 8 ラウンド目 [5] に対して行うこととした. この評価の結果, 今回試作した AES コアにおいては, ある 1 点におけるレーザー照射において保持しているデータのフリップが確認できた. また, この際フォールトが発生する最小のレーザー強度は 4.2 nJ であり, レーザー強度の上昇に伴いフォールト確率が 0%から 100%まで上昇していくことが確認できた. この結果より, 本プロセスにおいて LFI 検知センサは, 4.2 nJ のレーザー照射を十分な余裕を持って検知する必要があるという結果が得られた.

5.2 LFI センサ感度評価

次に, 暗号コア中に分散配置された LFI 検知センサの攻撃検知感度について評価を行った. 初めに, 評価ボード裏面に設けられた穴からレーザー照射を行った場合のセンサ感度について評価を行った. なおセンサ感度は, レーザーを照射した際にセンサが反応し検知信号が生成される最小のレーザー強度を表しており, 単位は nJ となる. この値が小さいほど, LFI に対して高い感度を持つということが言える. 測定の結果, 裏面穴のエッジ部分においては, はみ出した接着剤によるわずかなセンサ感度の悪化が確認された, しかし, それ以外の場所においてはセンサ感度は攻撃検知に十分な感度を持ち, また領域全体においてフラットであることが確認された. 加えて, AES コア中のある領域において, より詳細な測定を行ったところ, 領域全体において, センサ感度は前節で述べたフォールト注入に必要なレーザー強度である 4.2 nJ を大きく下回り, 攻撃検知に十分な感度を持つことが確認できた. これより, 2.3 節にて述べた設計手法による LFI 検知センサ設計は適切であったこ

とが確認された.

5.3 電源瞬断回路性能評価

最後に, 攻撃検知信号を受けて暗号コアの内部データを消去するに電源瞬断回路の評価結果について述べる. 試作チップには, AES コアの電源, グラウンド配線の電位変動を観測するためのオンチップモニタ回路 (On-Chip Monitor: OCM) [21] が搭載されている. 加えて, AES コアの内部レジスタ値の変化を観測するための, 信号観測回路も搭載されている. また, 本実験では使用する入力平文については固定とした.

AES の 8 ラウンド目の処理中にレーザー照射を行ったところ, 定格の電源電圧である 1.8V から 0.6V 付近までの急速な電圧降下を観測することが出来た. 次に, 提案回路が作動した場合の暗号コアからの出力結果について評価を行った. 正常な暗号化処理を経て出力される出力（128 ビット）と, 電源瞬断回路が作動した場合の出力（128 ビット）について, 各ビットあたりの平均ハミング距離を算出した. この値が 0.5 となると, 各々のデータに相関はないということになる. 電源瞬断回路が作動する時間を外部から制御した上で測定を行ったところ, 2ns 以内で 1 ビットあたりの平均ハミング距離の値は 0.5 となり, 無相関化が達成できていることが確認できた.

6. 結論

本稿では, 暗号コアへの LFI に対する対策回路を搭載した暗号プロセッサの設計手法について提案を行った. この対策手法は, レーザー照射に伴う異常な基板電流を検知する分散配置されたセンサモジュールと, センサからの攻撃検知信号を受けて, 暗号コアへの電源供給経路を遮断する電源瞬断回路により構成されている. LFI に伴い, 避けられない物理現象として基板内に異常な過渡電流が発生する. この過渡電流は基板内を広く伝搬するため, スパースに配置されたセンサアレイで容易に検出可能である. 単一のセンササイズはわずか 286 F^2/Cell であり, 暗号コア全体で LFI を検出するためコア中に分散配置されている. 加えて, 検知後の対策として, 暗号コア内部データを迅速に消去可能な電源瞬断回路を統合した. これは, 攻撃検知信号に伴い暗号コアへの電源供給路をスイッチすることにより, 内部電荷を急速に放電しデータの消去を行う. 本稿では, 提案手法の有効性を確認するために, 0.18 µm CMOS プロセスによりテストチップを試作し, 評価を行った. この結果, センサは LFI の検知に十分な感度を持っていることが確認できた. また, 電源瞬断回路は, センサからの検知信号を受け, 2ns 以内に内部データ消去を達成できていることも確認できた. これより, 本提案手法は+28%のレイアウト面積オーバヘッドで, AES コア全体を LFI から保護することが可能であることを確認した.

謝辞 本研究は JSPS 科学研究費補助事業 (科研費) の基盤研究 A“レーザーフォールト攻撃による情報漏えいを防ぐ耐タンパー技術の総合的研究”(15H01688), 及び基盤研究 S“暗号技術による IoT エコシステムのレジリエンス向上”(18H05289) の助成を受けたものである. また, 本研究の遂行にあたり, 独立行政法人情報処理推進機構（IPA）のレーザーフォールト注入装置を使用し, 同機構の指導の下, 実験を行った.

参考文献

[1] P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis,” *CRYPTO*, *LNCS*, vol. 1666, pp. 388-397, Aug. 1999.

[2] E. Brier, C. Clavier, and F. Oliver, “Correlation Power Analysis with a Leakage Model,” *Conference on Cryptographic Hardware and Embedded Systems (CHES)*, *LNCS*, vol. 3156, pp. 16-29, Aug. 2004.

[3] D. Boneh, R. A. DeMillo, and R. J. Lipton, ”On the Importance of Checking Cryptographic Protocols for Fault,” *EUROCRYPTO*, *LNCS*, vol. 1233, pp. 37-51, May 1997.

[4] E. Biham and A. Shamir, “Differential Fault Analysis of Secret Key Cryptosystems,” *CRYPTO*, *LNCS*, vol. 1294, pp. 513-525, Aug. 1997.

[5] G. Piret and J. J. Quisquater, “A Differential Fault Attack Technique against SPN Structures, with Application to the AES and KHAZAD,” *Conference on Cryptographic Hardware and Embedded Systems (CHES)*, *LNCS*, vol. 2779, pp. 77-88, Aug. 2003.

[6] K. Sakiyama, Y. Li, M. Iwamoto, and K. Ohta, “Information-Theoretic Approach to Optimal Differential Fault Analysis,” *IEEE Trans. Information Forensics and Security*, vol. 7, no. 1, pp. 109-120, Feb. 2012.

[7] Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, ”Fault Sensitivity Analysis,” *Conference on Cryptographic Hardware and Embedded Systems (CHES)*, *LNCS*, vol. 6225, pp. 320-334, Aug. 2010.

[8] S. P. Skorobogatov and R. J. Anderson, “Optical Fault Induction Attacks,” *Conference on Cryptographic Hardware and Embedded Systems (CHES)*, *LNCS*, vol. 2523, pp. 2-12, Aug. 2002.

[9] T. G. Malkin, F. X. Standaert, and M. Yung, “A Comparative Cost/Security Analysis of Fault Attack Countermeasure,” *Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pp. 109-123, Sep. 2005.

[10] M. Doulcier-Verdier, J. Dutertre, J. Fournier, J. Rigaud, B. Robisson, and A. Tria, “A Side-Channel and Fault-Attack Resistant AES Circuit Working on Duplicated Complemented Values,” *IEEE International Solid-State Circuits Conference (ISSCC) Digest of Technical Papers*, pp. 274-275, Feb. 2011.

[11] E. Trichina and R. Korkikyan, “Multi Fault Laser Attacks on Protected CRT-RSA,” *Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pp. 75-86, Aug. 2010.

[12] J. Woudenberg, M. F. Witteman, and F. Menarini, “Practical Optical Fault Injection on Secure Microcontrollers,” *Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pp. 91-99, Aug. 2011.

[13] R. Bauman, “Soft Errors in Commercial Integrated Cir-

cuits," *International Journal of High Speed Electronics and Systems*, vol. 14, no. 2, pp. 299-309, June 2004.

[14] J. L. Wirth, and S. C. Rogers, "The Transient Response of Transistors and Diodes to Ionizing Radiation," *IEEE Transactions on Nuclear Science*, vol. 11, pp. 24-38, Nov. 1964.

[15] R. Baumann, "The Impact of Technology Scaling on Soft Error Rate Performance and Limits to the Efficacy of Error Correction," *Dig. International Electron Devices Meeting*, pp. 329-332, Dec. 2002.

[16] E. H. Neto, I. Ribeiro, G. Wirth, F. Kastensmidt, and M. Vieira, "Using Bulk Built-in Current Sensors to Detect Soft Errors," *IEEE Micro*, vol. 26, no. 4, pp. 10-18, Sep. 2006.

[17] C. Champeix, N. Borrel, J.-M. Dutertre, B. Robisson, M. Lisart, and A. Sarafianos, "Experimental validation of a Bulk Built-In Current Sensor for detecting laser-induces currents," *IEEE International On-Line Testing Symposium (IOLTS)*, pp. 150-155, July 2015.

[18] J.-M. Dutertre, R. P. Bastos, O. Potin, M. L. Flottes, B. Rouzeyre, and G. D. Natale, "Sensitivity tuning of a bulk built-in current sensor for optimaltransient-fault detection," *Microelectronics Reliability*, vol. 53, pp. 1320-1324, Sep. 2013.

[19] K. Matsuda, N. Miura, M. Nagata, Y. Hayashi, T. Fujii, and K. Sakiyama, "On-Chip Substrate-Bounce Monitoring for Laser-Fault Countermeasure," *IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*, pp. 1-6, Dec. 2016.

[20] 郡義弘, 藤本大介, 林優一, 崎山一男, 三浦典之, 永田真, "IC 内部の回路構成変更が秘密鍵の取得性に与える影響の評価", 情報・システムソサエティ特別企画学生ポスターセッション, ISS-P-005, 2018.3.20.

[21] T. Hashida and M. Nagata, "An On-Chip Waveform Capturer and Application to Diagnosis of Power Delivery in SoC Integration," *IEEE Journal of Solid-State Circuits*, vol. 46, no. 4, pp. 789-796, Apr. 2011.