トラスト IoT 実現に向けた未知の脅威の On-Chip 検知技術に関する研究

代表研究者　　史　又華　　早稲田大学　基幹理工学部　教授

1 はじめに

近年，情報通信技術の進化と共に，急速に進化している IoT(Internet of Things)は様々な分野での応用が期待されている．IoT につながるものは，個人用情報機器から，医療機器，自動車，交通や金融機関など社会インフラがある．これらの機器は個人情報や，企業などの機密情報を扱うこともあるため，セキュリティ上信頼のおけるものでなくてはならない．しかし，IoT に生じる深刻な脅威に日々さらされるようになった．そのため，未来トラスト IoT 社会の実現には，IoT デバイスにおけるトラスト技術の確立が急務となる．

従来の情報セキュリティ技術は既知の攻撃手段を基にした設計手法であるため，これまで見たこともない「未知の」攻撃や障害が発生したときに，それに対応するのが極めて困難のために，高度なセキュリティは保証できない．もう一方で，IoT デバイスの小型化や低電力化に伴い，回路の臨界電荷量が低下しているため，雑音や電源電圧の変動による一時的な誤作動（＝物理的な一時エラー）が増加している．結果として，環境による故障の発生或いは攻撃を受けやすくなり,信頼性の低下が問題となっている.既存の技術として，面積・電力のオーバーヘッドが大きいため，実用上は一部の回路にしか適用できず，回路全体の信頼性を保証できない問題がある．

IoT におけるトラストの問題点は以下のようにまとめることができる：１）信頼性の低下と２）セキュリティのリスク．特に，トラストの脅威において最も重要な課題は，これまで見たこともない「未知の」攻撃や障害が発生したときに，それを早期検知できることである．そのため，本研究では，トラスト IoT 社会の実現を目指し，IoT デバイスにおける「未知の脅威」の対策手法に関する研究を行った．以下では，提案した（１）エラー回復・検出機能を持つ回路設計手法および（２）遷移頻度を考慮した未知脅威の検出手法についての成果を述べる．

2 エラー回復・検出機能を持つ回路設計手法

集積回路技術の発展は我々の生活を大きく変え，現代のユビキタス・コンピューティング時代を築き上げた．特に微細化・省電力化技術は今後も厳しい設計制約が期待される．これらの進歩は恩恵をもたらす一方で，PVT(Power, Voltage Temperature)ばらつきや経年劣化，そしてソフトエラーといった信頼性を脅かす問題を表面化させた．その中,ソフトエラーとは，α線や中性子線といった放射線が回路に衝突することで発生する一時的なエラーである．微細化に伴い回路がもつしきい値(臨界電荷量)が低下し，ソフトエラーの発生率が上昇した．さらには配線間距離が短縮することで電荷共有が発生し，一度の衝突で複数箇所に影響を与えるようになった．これまで，ソフトエラーは，臨界電荷量の少ない SRAM(Static Random Access Memory) や DRAM(Dynamic Random Access Memory) 等のメモリ回路で問題とされていた．一方，論理回路は前者に比べると，臨界電荷量が多い論理回路では問題とされていなかった．しかし，微細化が進むことで，論理回路の臨界電荷量も放射線の影響を無視できないほど，小さくなっている．つまり，ソフトエラーのような一時的なエラーによる集積回路信頼性の低下は微細化技術の発展の足枷になっているといえる．

これまで，様々なソフトエラー耐性技術の研究がなされてきた．従来耐性手法として，回路の多重化や誤り訂正符号(ECC ：Error Correction Code)メモリを使用することが挙げられる．この２つの技術は回復技術ではなく，エラー値を読み込まないことで影響を無効化する技術である．多くの手法が提案されているものの１つとして ECC を使用したものが挙げられる．これは ECC は 3 つのパートであるエンコード，チャネル，デコーダで成り立ち，ソフトエラーの検出および訂正を行うことができる．ECC を利用したものとして SEC(Single-error Correcting Code)，DEC(Double-error Correcting Code)，Hamming code，Convolutional code が挙げられる．しかし，訂正可能条件に制約があるといった問題を抱える．その他にも多重化回路を使用した TMR(Triple Modular Redundancy)，Intel 社の開発した DICE(Dual Interlocked Storage Cell) ラッチ，ソフトエラーの発生原理を使用して高いソフトエラー耐性を達成する SEH(Soft Error Hardened) ラッチが挙げられる．TMR は多重化回路の 1 つであり，三重化回路は同じ回路を 3 つ重ね，多数決回路に接続し

公益財団法人電気通信普及財団
研究調査助成報告書　第36号　2021年度

た構造である．重ねた回路の 3 つの出力に対して多数決制をとり，正しい出力を得ることができる．ソフトエラーが出力に伝搬することはないが，同じ回路を 3 つ重ねた分の大きな面積オーバーヘッドと電力オーバーヘッドが生じる．DICE ラッチは広く研究が進められており，DICE 自体はセルのため，SRAM に使用できる等，汎用性が高いが，ソフトエラー耐性が低いといった問題が挙げられる．ソフトエラーが発生した際に発生を検出する技術やソフトエラーから回復する技術が多く提案されてきたが，回復・検出機構を付加しているため，面積や消費電力などに問題を抱えている．これらの技術は近年のトレンドである IoT デバイスの小型化・低電力化には適さない．よって，ソフトエラー耐性をもち，かつ小型・低電力を両立した技術が求められているといえる．

本研究は，潜在的な物理故障による信頼性低下の問題に対して，「物理的な脆弱部分」に注目し，設計工程における信頼性向上設計技術の開発を行った．特に，電力遅延積（PD 積）を大幅に改善した ACSC フリップフロップを提案した．提案 ACSC フリップフロップは AC（Adaptive Coupling）素子を利用したマスターラッチと，エラーを回復できるスレイブラッチから構成され，ACSC の回路図を図 1 示す．

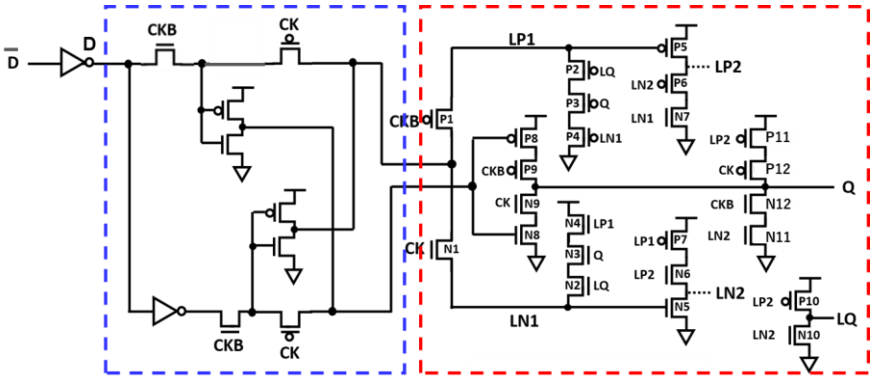


図 1 ：提案 ACSC フリップフロップの回路図

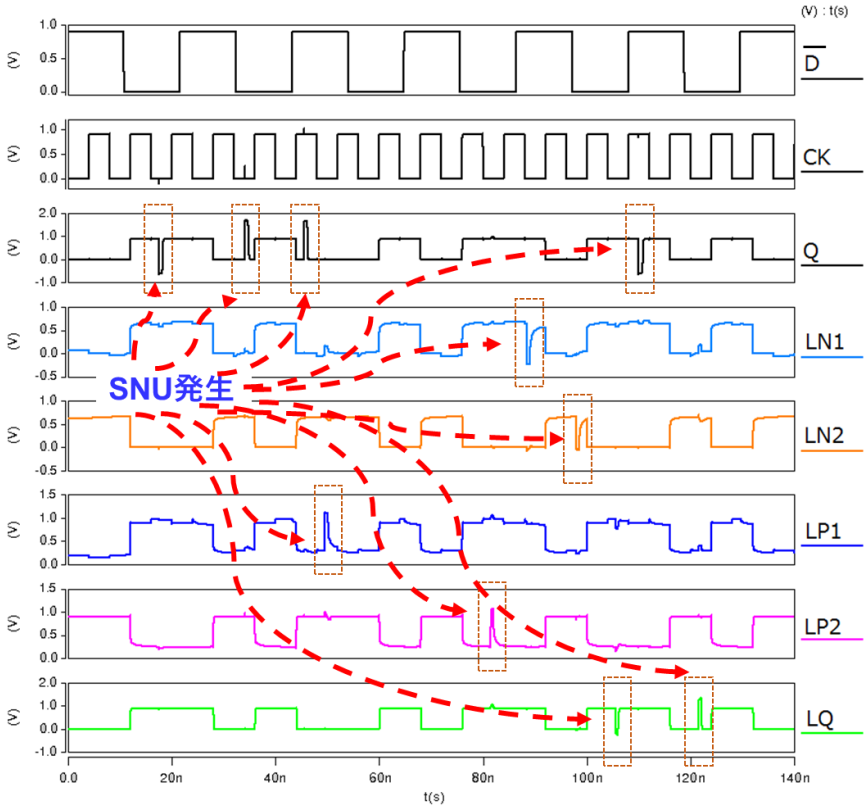
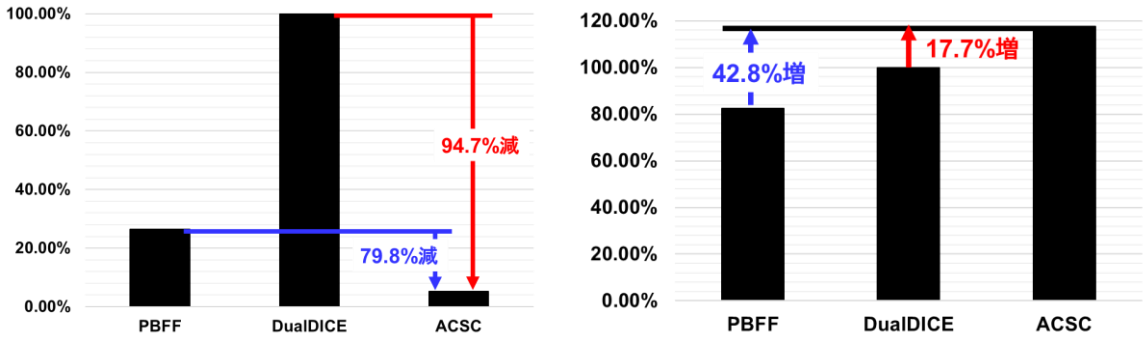


図 2 ：ACSC フリップフロップのエラー発生時波形

ACSC のマスターラッチは，３つ補助インバータと４つパストランジスタで構成される．入力はインバータを通り，上下のパストランジスタによって値の伝播が行われる．マスタ部にある一つ目のパストランジスタを通った後，NMOS だけで値を伝搬すると不安定な値になってしまうため，その先に PMOS が接続される．CK の立ち上がりで，スレイブラッチとつながり，値がスレイブラッチへ出力される．スレイブラッチでは，PMOS，NMOS では一方向にしか反転がおきないという性質を利用し，一部のノードを PMOS，NMOS のみで構成している．LP1，LP2 を PMOS のみ，LN1，LN2 を NMOS のみで構成することで，ソフトエラーの発生を制限している．つまり，LP1，LP2 では 0 → 1 のみ，LN1，LN2 では 1 → 0 への反転しか行われない．

通常動作時，CK=1 であればマスターラッチからの入力は P1，N1 を通り LP1，LN1 へ伝搬する．P5 または N5 がオンになり，LP2 または LN2 を通り，Q へマスターラッチからの入力がラッチされる．また，このとき P12，N12 はオフのため，回復機構からの入力は行われない．CK=0 のときは，P12，N12 がオンとなる．このとき P12 と N12，P11 か N11 のいずれか一つがオンになり Q の値を保持する．P11，P12，N11，N12 は CK=0 のときに Q がフローティングにならないための，キーパーの役割も担う．

SNU 発生時について ACSC の動作を述べる．CK=1 のときに SNU が発生し，いずれかのノードが反転しても，マスターラッチから値が入力され続けるため，すぐに回復できる．CK=0，LP1=0 のときに LP1 が 1 へ反転した場合，P5 がオフになり，他ノードのエラーは伝搬しない．この時，Q，LQ，LN1 は正しい値である 0 を保持し続けているため，P2，P3,P4 がオンとなり LP1 を正しい値の 0 へと回復できる．LN1=1 で 0 へ反転した場合も同様に N2，N3，N4 によって正しい値 1 へと回復できる．LP2，LN2 が反転した場合，LP1，LN1 は正しい値を保持しているため P5 や N5 によって正しい値へと回復できる．Q が反転した場合は P8 または N8，LQ が反転した場合は P9 または N9 によって正しい値へと回復できる．以上のように，提案スレイブラッチはすべてのノードにおいて SNU 耐性をもつ．



(a) (b)

図３：既存研究との比較．(a)PD 積と(b)面積

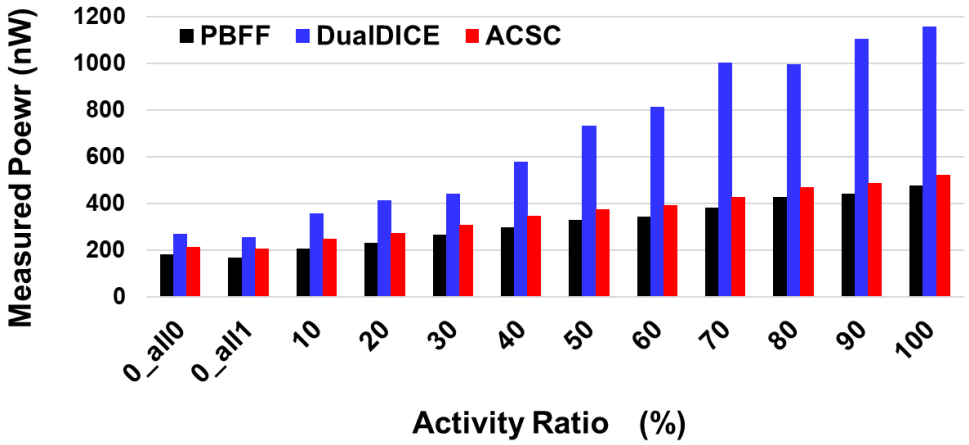


図４：既存研究との消費電力の比較@0.9V，25℃

次に DNU が発生した場合について述べる．CK=0,LP1=0，LP2=1，LQ=0，Q=0 のときに LP1=0→1,Q=0→1 に反転した場合，Q は LN2=1 のため，N8 を参照して 0 へ回復できる．さらに Q が回復したことで P2 がオンとなり，P2，P3，P4 によって LP1 は 0 へ回復できる．LN1，Q が反転した場合も同様である．同条件で LP1=0 → 1，LN2=1 → 0 に反転した場合，LP1 は P2，P3，P4 によって 0 へ回復でき，LN2 は P7，N6 によって 1 へ回復できる．LP1，と LP2，LN1 と LN2 はそれぞれ一方向にしか反転しないため，LP1 と LN1，LP2 と LN2 が同時に反転することはない．また，LP1 と LP2，LN1 と LN2 はそれぞれ逆の値を保持するため，このペアが同時に反転することもない．以上より，提案スレイブラッチはどのノードに対しても SNU と DNU の耐性を持っている．

提案 ACSC FF ソフトエラー発生時の波形を図 2 に示す．図 2 からわかるよう，どのノードにおいてもエラー発生しても次のクロックが入る前に，エラーから迅速に回復できていることが確認できる．また，Q における反転以外は出力 Q に影響を与えていないことがわかる．以上より ACSC のエラー耐性を証明できた．さらに，PD 積・面積と消費電力の比較グラフを図３と図４に示す．既存研究の PBFF[1]と DualDICE[2]と比較して，提案 ACSC 回路は 79.8%と 94.7%の PD 積を削減することに成功している．

3 遷移頻度を考慮した未知脅威の検出手法

近年，半導体設計・製造過程の国際化により IC(Integrated Circuit) チップの信頼性に対する疑念が示唆されている．従来，IC チップは信頼のおける会社や自社内で設計・製造されていたが，現在ではコスト削減のために外部委託されることが増えている．このため，攻撃者が設計内に悪意ある回路を挿入したり，回路の変更を行ったりすることが容易になってきている．このような正規の回路とは異なる不正な機能をもつ回路のことをハードウェアトロイ(Hardware Trojan:HT)と呼び，ハードウェア設計におけるセキュリティが重要な課題となる.ハードウェアトロイの目的はシステムの無効･変更や,IC チップの信頼性や寿命の低下,セキュリティ情報の漏洩と様々である.

これまで情報デバイスのセキュリティ・信頼性を確保するための基幹技術として，暗号技術・耐タンパー技術が開発・実装されてきた．しかし，IoT デバイスの製造コストを削減するために，ハードウェアの一部の設計・製造工程を第三者もしくは第三者のツールで行うようになった．その結果，設計工程では正しく設計しても，第三者によってマルウェア（＝悪意のある機能を持つ回路（例えば：ハードウェア動作の改変，故障注入，機密情報の流出など)）が挿入される危険性が指摘されている．文献 [3] により，プロセッサに 3 つトランジスタ程度のマルウェアを挿入すると,機密情報の盗取が可能であると指摘された.現実的には,数十万個以上のトランジスタのなかからこのような数個で構成されたマルウェアを設計工程での動作検証・テストによって検出することは不可能である．さらに，従来の技術は既知の攻撃手段を基にした設計手法であるため，これまで見たこともない「未知の」攻撃や障害が発生したときに，それに対応するのが極めて困難であり，結果，高度なセキュリティは保証できない.

設計者が想定している機能のみを持つ正規の IC チップであるかどうかを保証するためには，製造工程におけるすべての段階を信頼できるものにすること，あるいは，製造された IC チップの信頼性を検証することが必要である．前者はコスト面の問題からほぼ不可能である．したがって後者の IC チップの信頼性を確保することが現実的であり，ハードウェアトロイのような未知脅威の検出に関する研究が推し進められている．ここ数年では，ハードウェアトロイのベンチマークの公開を行っている Trust-HUB や，検出方法の評価の基準となるハードウェアトロイの新しい分類法の提案といった，この研究分野を支えるための活動や研究も増えてきている．ハードウェアトロイ検出の代表的な方法には，サイドチャネル情報解析や機能テストが挙げられる．この他にも活性化しない信号を特定・除去する方法や，ダミースキャンフリップフロップを挿入することでハードウェアトロイを活性化させる方法，PUF(Physically Unclonable Function) を利用した IC チップ認証，特定の時間内における遷移数に着目した認証方法，パフォーマンスカウンタを用い数値の大きさによってグループ分けして異常な動作パターンを検出するランタイム検出方法，フリップフロップ構造及び組み合わせ回路情報から Trigger の特徴を抽出して検出する方法，難読化により信号活性化を防ぐ耐ハードウェアトロイ設計，と様々なアプローチからハードウェアトロイに対する対策方法が報告されている．

しかしながら，A2[3]はアナログハードウェアトロイと呼ばれる位置に分類され，非常に小規模でステルス性を持ち，攻撃を行う直前まで回路にほぼ影響を与えることなくアナログで動作するという特徴を持つ．そのため，今日までに数多く提案されてきたデジタルなトロイ検出手法ではこの攻撃を検出することは難しい

とされている．膨大な素子数・高い複雑性を持つ IP(Intellectual Property) コアに対してアナログハードウェアトロイ挿入による変化が小さい上，ナノサイズである集積回路に対して物理的な検査やリバースエンジニアリングは困難かつ高コストになってしまう．さらに，リバースエンジニアリングを用いた検出方法では，複数の IC チップの一部にトロイが挿入された場合，検査済の分解された IC チップが正常であったと判断されても，未検査の残りの IC チップが正常であるとは保証されないことに注意しなければならない．また，普段の IC チップの動作には反応せず，特定の条件化のみでしかアクティブ化されない仕組みを持つため，IC チップ検証時にトロイが起動せず正常な動作をしたままテストを通ってしまう可能性もある．

A2 のようなアナログハードウェアトロイの特徴として，トロイ起動の際に特定の信号を複数回遷移させる必要があることが挙げられる．特定の信号とは，普段の動作では使用されないが，攻撃者が送る命令によって 0/1 の指定がしやすい信号のことを指している．アナログハードウェアトロイによる脅威を防ぐためには，全体の回路内で不審に遷移している信号がないか監視できるシステムが 1 つの解決法となる．

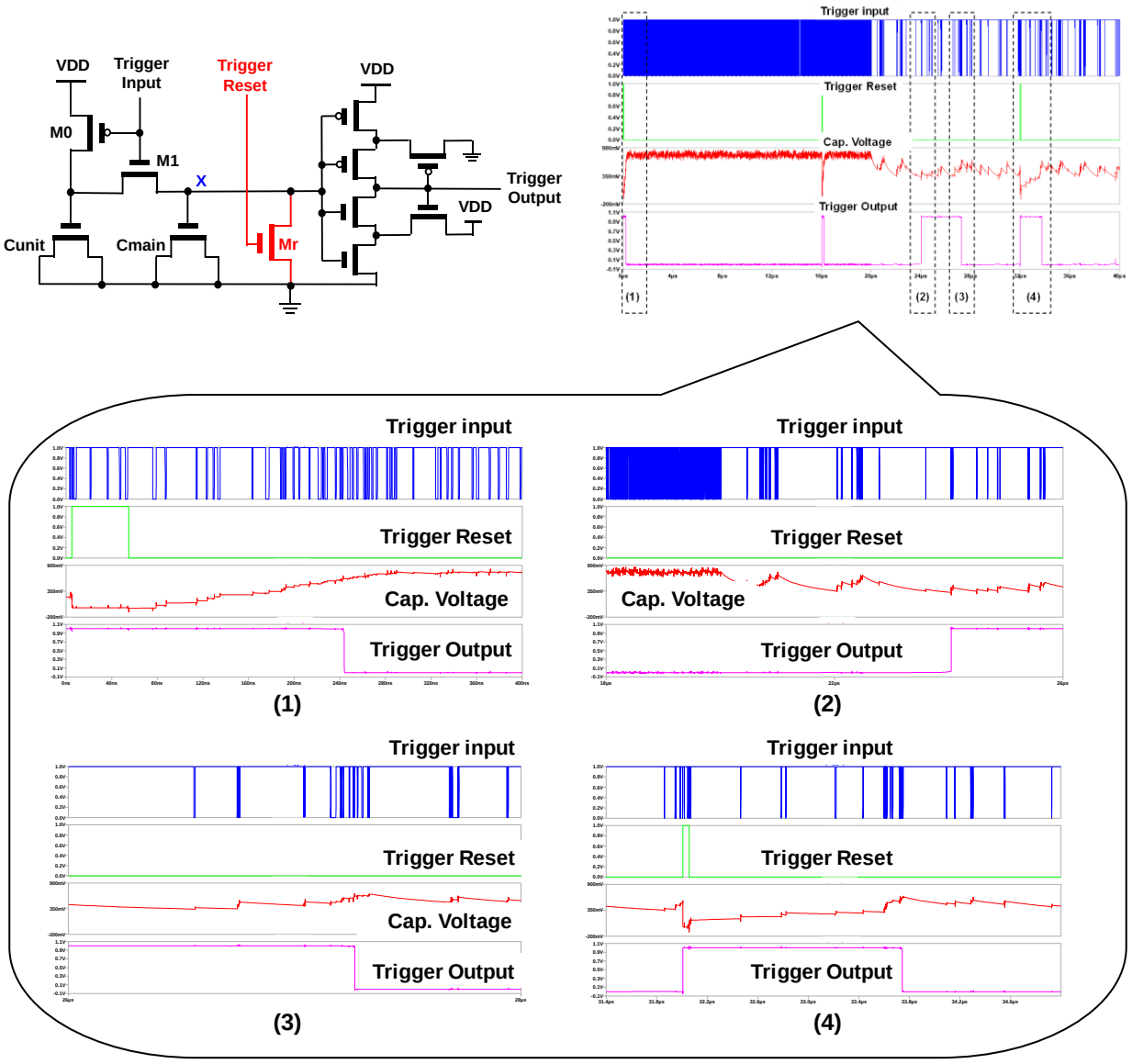
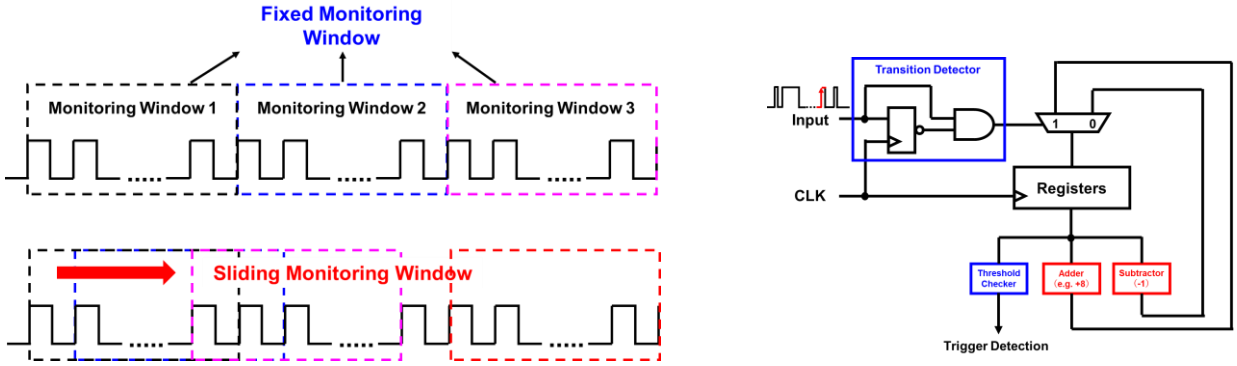


図５：改良した A2 ハードウェアトロイ回路とその SPICE シミュレーション波形



(a) (b)

図６：遷移頻度を考慮した未知脅威の検出回路．(a) 遷移頻度と遷移回数の比較，と(b) 提案回路の一例

そこで，本研究は既存の A2 ハードウェアトロイ回路を改良し（図 5），遷移頻度を考慮した未知脅威の検出手法を提案した（図 6 参照）．提案回路では，監視する信号が遷移する度にカウントを増やしていき，遷移せずに時間が経過する度にカウントを減らしていく仕様にすることで，カウンタ回路が信号の遷移頻度を計測するようにしている．カウンタ回路を用いる利点は 2 つ挙げられる．1 つは，カウンタ回路を用いる場合は RTL(Register Transfer Level)での実装が可能であるため，実装及び検証が容易になる点である．もう 1 つは，カウントの速さ(増減幅）や閾値の設定について，コンデンサはアナログの調整を必要とするのに対し，カウンタ回路はデジタルの調整で行えるため，パラメータ調整が容易になる点である．

この提案検出回路の 1 つの活用例として，オープンソースのプロセッサの機能としてこの検出機能を追加するということができる．まず，設計内で監視したい信号に対して，この検出回路の監視対象(入力）に指定する．次に，この設計から製造されたプロセッサについて，動作検証段階で検出回路が正常に動作するかを確認する．このようにすることで，アナログハードウェアトロイの起動よりも検出信号の送信が早く行われる前提ならば，たとえ設計・製造段階でアナログハードウェアトロイが挿入されていてもプロセッサに被害を出さずに検出することができるようになる．

検出信号送信後の動作はいくつか考えられる．例えば，トロイ起動を阻止する目的でハードウェア割り込みを行う方法や，偽陽性の低下が期待できるネットワークログの診断を行い，攻撃を受けたかどうか判断する方法，機密性の高いデータの漏洩を阻止できるプロセッサ kill，さらには最後にコミットされた命令にロールバックすることで以後の実行時に攻撃回避できるようにログを残す方法が挙げられる．検出回路を挿入する回路のセキュリティ的な重要度や使用環境といった要素を考慮して検出後動作を選択することになる．

増減幅や閾値に関しては，挿入する設計やその回路環境，検出目的とするトロイ等によって最適な値を設定する必要がある．そのため，短期間で連続した遷移が行われる場合に対応するためには，カウンタ回路の入力信号が遷移していた場合の増加数を増やすか，閾値を低く設定する必要がある．また，長期間をかけて遷移し起動する場合に対応するためには，カウンタ回路の入力信号が遷移していなかった場合の減少数を減らすか，閾値を高く設定する必要がある．これらの調整を繰り返し行うことで，攻撃者側は検出の回避が難しくなっていくが,理論的にはハードウェアトロイを微調整することで検出を回避する可能性が残っている．ただし，この競い合いは 2 つの点から検出側が有利であるといえる．1 つは，検出側は間違った検出を行った場合でも通常動作に復帰することができる点である．例えば，特権レベルなどのプロセッサの重要度が高いレジスタの状態が変更されたかどうかを確認し，違反が検出されない場合は通常の動作に戻るといった方法が使える．もう 1 つは，検出側は確実性のあるデジタル調整をしているのに対し，攻撃者側はプロセス変動に対する影響が大きいアナログ回路を介して微調整する必要がある点である．

提案検出回路をオープンソースプロセッサである OR1200 への実装を行った．以下は OpenRISC プロジェクトによるプロセッサ「OpenRISC1200」 [4]をベースに実装した結果について述べる．OpenRISC による命令セットアーキテクチャは OpenRISC1000 アーキテクチャと呼ばれ,それをもとに Verilog ハードウェア記述言語で実装されたプロセッサが OpenRISC1200 である．OR1200 IP core は CPU(Central Processing Unit)/DSP(Digital Signal Processor) や，データ及び命令のキャッシュ・MMU(Memory Management Unit) などのユニットで構成されている．OR1200 の構成を図 7 に示す．

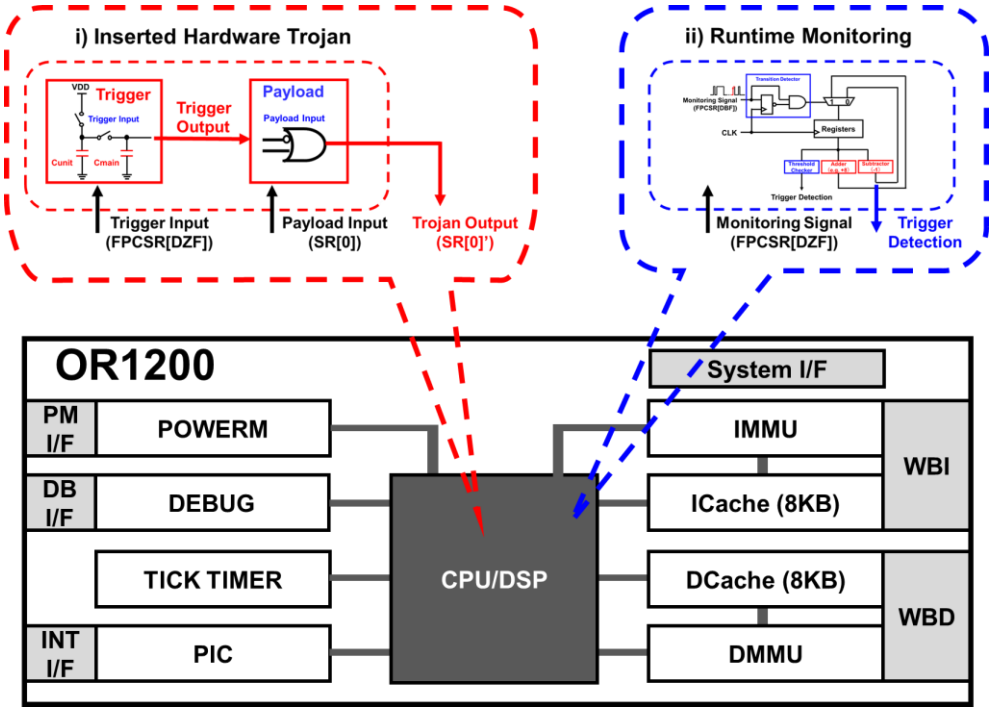


図 7 ：提案検出回路を OR1200 への実装

今回の監視対象としては，プロセッサの状態を管理する 32bit の特権レジスタ(SR)である．特に特権レジスタの最下位 bit である SR[SM] が 0 のときユーザモードに，1 のときスーパバイザモードになることを利用して，トロイ起動時に SR[SM] を 1 に固定するというものである．そのためのトリガとして，低遷移率の傾向を持つ wire の中から，攻撃者が攻撃命令によって操作しやすい wire を選択することができる． 0 除算は浮動小数点状態制御レジスタの 0 除算フラグを立ち上げるため，0 除算命令を繰り返し実行させることで 0 除算フラグを継続的に反転させることができる．この高頻度遷移を以って，攻撃者は意図的にアナログハードウェアトロイを起動することができる．スーパバイザモードに固定することで攻撃者は OS(Operating System) にフルアクセス可能となるため，このトロイはハードウェア版バックドアの役割を果たしているといえる．プロセッサへの実装にあたって，Trigger 回路部への入力信号としていくつか候補となる信号が存在するが，本研究では 0 除算フラグ(FPCSR[DBZ]) が選択された場合を想定する．プロセッサが 0 除算命令を繰り返し実行することで 0 除算フラグは頻繁に切り替わり，内部コンデンサの電圧が上昇していく．提案検出回路を用いて，コンデンサの電圧が閾値を超えたか判断し，通常時は High を，トロイ起動時は Low を Trigger Output へ出力する．Payload 回路部については，トロイ起動時に SR[SM] を 1 に固定することを実現する．このとき Trigger Output は通常時が High で攻撃時が Low であるため，OR 回路に入力する際に反転させている．これらアナログハードウェアトロイ回路はゲートレベルで挿入(記述) することとする．

A2 アナログハードウェアトロイ自体の Trigger 動作確認を行う．入力信号の継続的な遷移を受けてコンデンサの電圧が上昇していき,閾値電圧を超えたところでトロイ起動信号を出力することを確認する.その後，A2 アナログハードウェアトロイ及び提案検出回路が実装された OR1200 に対して攻撃命令を実行させ，トロイが起動する前に検出信号を出力することを確認する．攻撃命令の構成は，何もしない操作である「l.nop」から始め，攻撃を行うタイミングで 2 つの命令「l.movhi」と「l.divu」を繰り返し実行するようにしている．「l.movhi」は 0 以外の数字を作るために使用する命令であり，0 除算における割られる数を用意する役割がある．「l.divu」は除算を行う命令であり，割る数に 0 を指定することで 0 除算を実行させる役割がある．OR1200 に実装された A2 アナログハードウェアトロイの Trigger 動作確認として行ったシミュレーション結果を図 8(a)に示す．入力信号の継続的な遷移を受けてコンデンサ Cmain の電圧が上昇していき，閾値電圧を超えたところでトロイ起動信号を出力(Trigger Output = Low) している様子がわかる．このときの閾値電圧は測定値で約 0.57V であった．

(a) (b)

図８： OR1200 のシミュレーション結果.(a) OR1200 に実装された A2 アナログハードウェアトロイの Trigger 動作と(b) 提案検出回路のシミュレーション結果

提案検出回路のシミュレーション結果を図８(b) に示す．A2 アナログハードウェアトロイと検出回路の両方が FPCSR[DBZ] を入力としてその遷移を監視しており，トロイの起動信号よりも先に検出回路の検出を知らせる信号が出力されていることがわかる．シミュレーション結果から提案検出手法が A2 アナログハードウェアトロイ検出に効果的であることが示された．既存検出手法である R2D2[5] と提案手法では検出が難しいタイプが異なる．これはトロイ検出に用いる情報の違いに依るものである．一定時間毎の遷移数を測る R2D2 は，検証時間の境を跨ぐように異常遷移が発生すると検出が回避される可能性がある．一方，遷移頻度を測る提案手法は，「クロック周波数÷上げ幅」以下の周波数で異常遷移が発生すると検出が回避されてしまう．

OR1200 プロセッサ・既存回路(R2D2) 単体・提案回路単体を実装したときの面積・電力の一覧を表 2 に示す．検出手法実装における信号遅延の影響はない．面積オーバーヘッドに関しては OR1200 プロセッサに対して，既存回路は 0.0096%の増加，提案回路は 0.0064%の増加となる．電力オーバーヘッドに関しても OR1200 プロセッサに対して，既存回路は 0.016%の増加，提案回路は 0.011%の増加となる．結果として，提案回路は既存回路に対して面積・電力オーバーヘッド面で有利であるといえる．単体では少しの差であるが，実際には検出回路を複数個導入するので，その分オーバーヘッドは倍加していき，その差は大きなものとなる．また既存回路・提案回路共に，面積オーバーヘッドは全体に対する割合が小さいため主機能に大きく影響を与えないことが予想される．電力オーバーヘッドは，常にカウンタ回路が動作することになるため電力を消費しやすくなってしまうが，監視する信号が全く遷移しなければ動作しないためその分電力を抑えることできる．

既存検出手法である R2D2 は主にカウンタ回路が 2 つなのに対し，提案手法は主にカウンタ回路を 1 つのみ使用するため，同じ構造を複数導入する際に面積・電力面を比較すると小さく抑えることができる．また，設定が必要なパラメータは，R2D2 が 1 回の検証時間と遷移数閾値の 2 種に対し，提案手法はカウンタの閾値と上げ幅の 2 種となる．課題点として，R2D2 は複数信号監視の有効性の他に，異常遷移が検証時間の境を跨ぐように発生すると検出が回避される恐れがある．提案手法は，「クロック周波数÷上げ幅」以下の周波数で異常遷移が発生した場合に検出が回避される．今後の課題として，プロセスルールの変更における最適化・アナログハードウェアトロイ側の入力が複数の場合の有効性確認・温度及び電源電圧の変化による影響確認が挙げられる．

表２：OR1200 において既存研究との比較

	OR1200 (Baseline)	R2D2	Proposal
Area (μm^2)	9.932×10^6 (100%)	9.583×10^2 (0.0096%)	6.340×10^2 (0.0064%)
Power (μW)	3.533×10^4 (100%)	5.648 (0.016%)	3.715 (0.011%)

4 むすび

情報通信技術の普及に伴い，IoT の信頼性・セキュリティに対する懸念が注目されている．その中，最も重要な課題は，これまで見たこともない「未知の」攻撃や障害が発生したときに，それを如何に検知できることである．本研究は，トラスト IoT 実現に向けた「未知の脅威」に対する On-Chip 検知技術の研究開発を行った．特に，「エラー回復・検出機能を持つ回路設計手法」および「遷移頻度を考慮した未知脅威の検出手法」を提案した．本研究開発の成果は，原理的には，他の攻撃・不正設計へにも適用可能である．今後，ますます重要性が高まる IoT 社会の信頼性確保へと貢献することが期待される．

【参考文献】

[1] K. Yamada, H. Maruoka, J. Furuta and K. Kobayashi, “Radiation-hardened flip-flops with low-delay overhead using pMOS pass-transistors to suppress SET pulses in a 65-nm FDSOI process,” IEEE transactions on nuclear science, vol. 65,no.8, pp.1814-1822, 2018.

[2] J. E. Knudsen, and L. T. Clark, “An area and power efficient radiation hardened by design flip-flop,” IEEE transactions on nuclear science, vol. 53, no. 6, pp. 3392−3399, 2006.

[3] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, “A2: Analog malicious hardware,” in Proc. of International Symposium on Security and Privacy, 2015, pp. 18-37.

[4] D. Lampret et al, OpenRISC 1200 IP Core Specification, 2015.

[5] Y. Hou, H. He, K.Shamsi, Y. Jin, D. Wu, and H. Wu, “R2D2: Runtime reassurance and detection of A2 Trojan,” in Proc. of International Symposium on Hardware Oriented Security and Trust, 2018, pp. 195-200.

〈発 表 資 料〉

題　　名	掲載誌・学会名等	発表年月
特になし		

注: 国際学術論文誌 （IEEE Transactions on Circuits and Systems） 2件投稿中