様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月　 ９ 日現在

機関番号：３２６８９
研究種目：基盤研究(C)（一般）
研究期間：2019～2021
課題番号：１９Ｋ１１８８６

研究課題名（和文）侵襲に頑健な集積回路の設計および実装に関する研究

研究課題名（英文）Robust LSI design technology against invasion

研究代表者
柳澤　政生（Yanagisawa, Masao）

早稲田大学・理工学術院・教授

研究者番号：３０１７０７８１

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：本研究では集積回路（LSI）を外部から攻撃することを「侵襲」と呼ぶことにする。侵襲には「人による故意の侵襲」と「自然界に存在する侵襲」の2種類がある。近年、IoTデバイスの普及に伴い、より多くの情報機器がインターネットに接続され、個々のデバイスにおける頑健性が重要となって来ている。本研究では、侵襲を受けても、それを察知し、侵襲に強い集積回路を提案・設計している。

研究成果の学術的意義や社会的意義
近年、IoTデバイスの普及に伴い、より多くの情報機器がインターネットに接続されている現代では、個々のデバイスが誤った動作をしないことが重要である。誤動作をわざと生じさせようとする外敵がいる一方、自然界に存在する放射線が誤動作を起こさせることもある。本研究ではこれらの侵襲に頑健な集積回路の設計するものであり社会的な意義があると考える。また、ここで開発された設計技術は学術的に意義があると考える。

研究成果の概要（英文）：Attacking LSI (Large-scale Integrated circuits) from outside is called “invasion” in this research. There are two kinds of invasions, such as, invasion caused by human being and invasion (soft errors) caused by collisions of radiation particles like alpha particles and high energetic neutrons on an LSI. We have to protect LSIs from those invasions.
Unlike traditional hard-errors caused by permanent physical damage which can’t be recovered in field, soft errors are caused by radiation or voltage/current fluctuations that lead to transient changes on internal node states, thus they can be viewed as temporary errors. Three soft error hardened latch designs were proposed for reliability and energy-efficiency improvements, which can be viewed as i) SNU (single node upset) hardened design, ii) SNU hardened and detection-based design, and iii) MNU (multiple node upset) hardened and detection-based design, respectively.

研究分野：工学

キーワード：侵襲　集積回路　LSI設計　頑健　ソフトエラー耐性

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

(1) 近年、スマートフォンを始め、タブレットやセンサネット並びに健康等のアプリケーションの携帯性を必要とする情報機器（IoT デバイス）の発展拡大に伴い、より多くの情報機器がインターネットに接続され、個々のデバイスにおける頑健性が重要となって来ている。たとえば、情報の暗号化においては、暗号システムをハードウェアで実装する際、サイドチャネル攻撃（人による故意の侵襲）による暗号解読に注意が必要である。

(2) LSI（大規模集積回路）の信頼性における重要な問題の１つとして、放射線起因のソフトエラー（自然界に存在する侵襲）が挙げられる。高エネルギー粒子が回路に衝突すると、エネルギーを失い、電子正孔対が生成する。過剰キャリアである電子は N 拡散領域、正孔は P 拡散領域へと収集される。収集された電荷がノードの臨界電荷量を上回った場合、状態が反転し、ソフトエラーが発生する。つまり、PMOS と NMOS において、データは一方向にしか反転しない。ソフトエラーは一時的な故障のため、回路構造の工夫等で回復することができるが、間違った値をラッチした場合、回路に重大な障害が生じる。従来の耐ソフトエラー技術よりも高い耐性をもち、低消費電力・小面積・高速な LSI 設計技術の開発が求められている。

(3) ディジタルシステムには多くディジタルフィルタが利用されている。ディジタルフィルタでは畳み込み演算が主となる演算である。畳み込み演算は、特定の情報を選択するためのフィルタリングの役割を担っている。畳み込みシステムの主な演算は積和演算（MAC）である。特に高精度なアプリケーションでは、畳み込みシステムの MAC 演算の量は非常に大きくなるため、演算時間が長く、消費電力が高く、そして回路面積も大きくなってしまう。これらの問題を解決するために、高効率な畳み込み演算回路設計技術が求められている。

２．研究の目的

本研究では集積回路（LSI）を外部から攻撃することを「侵襲」と呼ぶことにする。侵襲には「人による故意の侵襲」と「自然界に存在する侵襲」の 2 種類がある。近年、IoT デバイスの普及に伴い、より多くの情報機器がインターネットに接続され、個々のデバイスにおける頑健性が重要となって来ている。たとえば、情報の暗号化においては、暗号システムをハードウェアで実装する際、サイドチャネル攻撃(人による故意の侵襲)による暗号解読に注意が必要である。本研究では、故意の侵襲や自然界の侵襲を受けても、それを察知し、侵襲に強い集積回路を提案・設計することを目的とする。

そのために、故意の侵襲を受けても、それを察知し、正常に稼働する集積回路を提案・設計することを第 1 の目的とする。自然界では放射線が回路に衝突すること（自然界に存在する侵襲）によってソフトエラーと呼ばれる一時的なエラー（信号の反転）が集積回路内に発生する。本研究では、LSI にソフトエラーが生じても回路自身がエラーを修復する機能をもたせた集積回路を提案・設計することを第 2 の目的とする。また、ディジタルシステムに多く利用されているディジタルフィルタの畳み込み演算に焦点を当て研究を行う。畳み込み演算は、特定の情報を選択するためのフィルタリングの役割を担っている。畳み込みシステムの主な演算は積和演算（MAC）である。特に高精度なアプリケーションでは、畳み込みシステムの MAC 演算の量は非常に大きくなるため、演算時間が長く、消費電力が高く、そして回路面積も大きくなってしまう。これらの問題を解決するために、高効率な畳み込み演算回路設計技術が求められている。1 次元／2 次元の畳み込み演算を行う FIR ディジタルフィルタ回路に注目し、高効率な畳み込み演算回路を提案し提案・設計することを第 3 の目的とする。

３．研究の方法

(1) 本研究では第 1 の目的のために、我々が開発した STEP（Suspicious Timing Error Prediction）に注目する。STEP は集積回路中のパス（配線経路）の途中を STEP 挿入位置とし、STEP 挿入位置 D における信号遷移を監視することによって、現在のクロックサイクルにおけるエラーを未然に予測できる回路である。予測後はクロックゲーティングによりエラーを回避することによって、原理的にエラーの起こらない回路が設計可能となる。本研究では、STEP を AES 暗号回路に適用することで遅延変動に対して頑健な AES 暗号回路を提案・設計する。提案する回路は、回路モジュールの分割点を STEP 挿入位置とすることで、遅延が十分に短く、タイミングエラー発生が無視できるパスを除く、すべてのパスを STEP で監視し、回路全体で起こるタイミングエラーの予測とクロックゲーティングを用いたタイミングエラーの回避を実現する。その結果、配線遅延にばらつきが生じた場合でも、正しく暗号化処理を実現できるという利点を併せ持つ。

(2) 第 2 の目的のために、2014 年より耐ソフトエラーラッチに関する研究を行っている。本研究では研究成果をさらに進展させ、さらなる高速化を目指した Fast-SEH ラッチに関して研究し、新しい回路を提案する。また、C-element を活用することにより、高いソフトエラー耐性をもたせた回路を提案する。それぞれの回路をトランジスタ・レベルでシミュレーションを行い、消費電力や遅延時間、面積を求め、比較・検討し、考察する。

(3) 第 3 の目的のために、ディジタルシステムに多く利用されているディジタルフィルタの畳み込み演算に焦点を当て研究を行う。畳み込みシステムの主な演算は積和演算（MAC）である。特に高精度なアプリケーションでは、畳み込みシステムの MAC 演算の量は非常に大きくなるため、演算時間が長く、消費電力が高く、そして回路面積も大きくなってしまう。これらの問題を解決するために、高効率な畳み込み演算回路設計技術に関する研究を行う。1 次元／2 次元の畳み込み演算を行う FIR ディジタルフィルタ回路に注目し、高効率な畳み込み演算回路を提案・設計し、評価・考察する。

４．研究成果

(1) 当研究室で開発した STEP（Suspicious Timing Error Prediction）は、STEP の挿入位置 D における信号遷移を監視することによって、現在のクロックサイクルにおけるエラーを未然に予測する回路である。本研究では、研究計画に記載した通りに、STEP を AES 暗号回路に適用することで遅延変動に対して頑健な AES 暗号回路を提案・設計した。提案する回路は、回路モジュールの分割点を STEP 挿入位置とすることで、遅延が十分に短く、タイミングエラー発生が無視できるパスを除く、すべてのパスを STEP で監視し、回路全体で起こるタイミングエラーの予測とクロックゲーティングを用いたタイミングエラーの回避を実現している。

(2) ソフトエラー耐性をもつ低消費電力・小面積・高速回路設計技術に関して研究を行った。従来、DICE やフリップフロップの多様化といった耐ソフトエラー技術が提案されてきたが、消費電力が増加する、回路面積が増える等の問題点が生じており、低電力で高耐性をもつ LSI 設計技術の開発が急務となっている。本研究では、SEH ラッチを改良することにより、低電力な耐ソフトエラーラッチである New-SEH ラッチを提案し、NCSU15nm の PDK（Process Design Ki）を用い、実装・評価を行った。従来の SEH ラッチと比較し、消費電力を 46%削減、トランジスタを 25%削減可能なことをシミュレーション実験によって示した。ただ、このラッチは遅延オーバーヘッドが大きいものであった。そこで、さらに優れた耐ソフトエラーラッチを検討した。その結果、New-SEH ラッチをさらに改良することにより高速化を目指した Fast-SEH ラッチを提案した。シミュレーション実験によって、Fast-SEH ラッチは SEH ラッチと比較して、最大で 10.91%の電力削減、55.17%の遅延削減することを示した。また、C-element を使用し、低電力化を目指した耐ソフトエラーラッチである SHC ラッチの提案を行った。SHC ラッチと既存の耐ソフトエラーラッチを実装し、spice シミュレーション・評価を行った結果、SHC ラッチ は HiPeR ラッチと比較し、最大で 80.52% の電力削減を達成した。また、改良 SHC ラッチは FERST ラッチと比較し、最大で 66.04% の遅延削減を達成した。また、ソフトエラー耐性に関する既存技術の問題点として出力のノードが弱点であることが挙げられる。既存の耐ソフトエラー技術では出力のノードをソフトエラーから回復させるまでに時間がかかるため、エラーが後続の回路に伝搬してしまう可能性がある。その結果、回路の誤動作を引き起こし、大きな障害に繋がる恐れがある。また、微細化と共に複数ノードにおけるソフトエラーの発生率が高まっている。そのため、SNU（Single Node Upset）だけでなく DNU（Double-node upset）におけるエラー回復機能および検出機能をもつラッチ回路を提案した。さらに、TDRHL 回路は TNU（Triple-node upset）に対して、一定の条件でも検出できることが確認した。既存検出ラッチ(sPGTD)と比較して 82.70%、耐 DNU ラッチ回路（SEID）と比較して 59.44%の PDP を削減できることを示した［①］。

(3) ディジタルシステムに多く利用されているディジタルフィルタの畳み込み演算に焦点を当て研究を行った。畳み込み演算は、特定の情報を選択するためのフィルタリングの役割を担っている。畳み込みシステムの主な演算は積和演算（MAC）である。特に高精度なアプリケーションでは、畳み込みシステムの MAC 演算の量は非常に大きくなるため、演算時間が長く、消費電力が高く、そして回路面積も大きくなってしまう。これらの問題を解決するために、高効率な畳み込み演算回路設計技術が求められている。1 次元／2 次元の畳み込み演算を行う FIR ディジタルフィルタ回路に注目し、高効率な畳み込み演算回路を提案し以下の成果を得た［②］。回路構造レベルでは、電力遅延積で 18%の削減、面積遅延積で 10%の削減、レイテンシーで 33%削減を実現した。ユニットレベルでは、電力遅延積で 35.8%の削減、面積遅延積で 44.5%の削減を実現した。また、ビットレベルでは、面積遅延積で 30.7%の削減、電力遅延積で 22.8%の削減を実現した。以上の３つの階層にわたり、回路全体の面積、遅延、消費電力、面積遅延積および電力遅延積を抑える最適な高効率回路設計方法を提案し、それぞれの有効性を示した。高次元の FIR フィルタの設計において、高効率な回路を設計し、国際会議 APCCAS で学生が発表したところ、Best Student Paper Award を受賞することとなった［③］。深層畳み込みニューラルネットワークのハードウェア設計においては、部分的な加算の再利用をしたデーターフロー技術を用いて、低消費電力の回路を実現し、その成果を論文書で発表した［④］。

＜引用文献＞

① Saki Tajima, Masao Yanagisawa, and Youhua Shi, “Transition Detector-Based Radiation-Hardened Latch for Both Single- and Multiple-Node Upsets,” IEEE Transactions on Circuits and Systems II: Express Briefs, Volume 67, Issue 6, 2020, pp. 1114-1118.

② Jinghao Ye, Masao Yanagisawa, and Youhua Shi, “Faithfully Truncated Adder-based Areapower Efficient FIR Design with Predefined Output Accuracy,” IEICE Transactionson Fundamentals of Electronics, Communications and Computer Sciences, vol. E103-A, no. 9, Sep. 2020, pp. 1063-1070.

③ Jinghao Ye, Masao Yanagisawa, and Youhua Shi, “A High-Performance Symmetric Hybrid Form Design for High-Order FIR Filters (Best Student Paper Award),” 2020 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), 8-10 December 2020, pp. 121-124.

④ Lin Ye, Jinghao Ye, Masao Yanagisawa, and Youhua Shi, “Power-Efficient Deep Convolutional Neural Network Design Through Zero-Gating PEs and Partial-Sum Reuse Centric Dataflow,” IEEE Access, Volume: 9, 21 January 2021, pp. 17411-17420.

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　2件）

１．著者名 Saki Tajima, Masao Yanagisawa, Youhua Shi	４．巻 67
２．論文標題 Transition Detector-Based Radiation-Hardened Latch for Both Single- and Multiple-Node Upsets	５．発行年 2020年
３．雑誌名 IEEE Transactions on Circuits and Systems II: Express Briefs	６．最初と最後の頁 1114 - 1118
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TCSII.2019.2926498	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Lin Ye, Jinghao Ye, Masao Yanagisawa, Youhua Shi	４．巻 9
２．論文標題 Power-Efficient Deep Convolutional Neural Network Design Through Zero-Gating PEs and Partial-Sum Reuse Centric Dataflow	５．発行年 2021年
３．雑誌名 IEEE Access	６．最初と最後の頁 17411 - 17420
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2021.3053259	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Jinghao Ye, Masao Yanagisawa, Youhua Shi	４．巻 E103-A
２．論文標題 Faithfully Truncated Adder-based Areapower Efficient FIR Design with Predefined Output Accuracy	５．発行年 2020年
３．雑誌名 IEICE Transactionson Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1063 - 1070
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2019KEP0010	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 Jinghao Ye, Masao Yanagisawa, Youhua Shi
２．発表標題 A High-Performance Symmetric Hybrid Form Design for High-Order FIR Filters
３．学会等名 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)（国際学会）
４．発表年 2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関