

## SRAM型FPGAアーキテクチャに依存したソフトウェアの脆弱性評価

森田 真平 (量子・古典集積回路研究室)  
(指導教員 廖 望 講師)

## 1. はじめに

近年、FPGA (Field Programmable Gate Array) は、高性能な並列計算デバイスとして、宇宙産業および自動車の自動運転技術の分野で注目されている。主流の高性能 FPGA では、回路構成情報をビット情報として SRAM (Static Random Access Memory) である CRAM (Configuration RAM) に格納している。しかし、CRAM は宇宙線などの影響を受けやすく、ソフトウェアと呼ばれるビット反転が比較的高い確率で発生するため、実装回路の対ソフトウェアの信頼性評価が重要である。

先行研究では CRAM ビット全体が回路の信頼性に与える影響を評価することにどまり、CRAM におけるソフトウェアと FPGA アーキテクチャに依存した脆弱性の関係については十分に検討されていない。本研究では、商用 FPGA に実装した回路を対象とし、アーキテクチャに依存した脆弱性の評価手法を提案することを目的とする。

## 2. アーキテクチャに依存した脆弱性評価とその問題点

SRAM 型 FPGA は、論理回路を LUT (Look-Up Table) からなる論理機能ブロックと、ブロック間の配線機能によって回路を構成している。回路構成情報を格納する CRAM の各ビットは論理または配線機能があらかじめ割り当てられている。本研究では、FPGA における CRAM ビットとその構成機能の対応関係は FPGA アーキテクチャとして定義する。

CRAM ビットにおけるソフトウェアが実装回路に与える影響はアーキテクチャによって異なるため、FPGA アーキテクチャに依存したソフトウェア脆弱性の評価は極めて重要である。脆弱性の依存関係の評価するには、CRAM ビットと構成機能の対応関係を特定し、分類した上で脆弱性評価を行う。

旧型の FPGA では、アーキテクチャが先行研究[1]によって解析されており、アーキテクチャを特定できる。しかし、先行研究では、実装した回路に対してビット分類に基づくアーキテクチャに依存した脆弱性の評価は行われていない。一方で、新型の FPGA は公開情報が不足しているため、FPGA アーキテクチャがブラックボックスとなっており、CRAM ビットの分類がまだ確立されていない。さらに評価時には、周辺回路へのエラー注入を避ける必要があり、評価回路の CRAM ビットを抽出する必要もある。先行研究[2]は、評価回路の CRAM ビットの抽出方法のみに着目している。先行研究における抽出手法の制約および分類手法の未確立を解決するため、本研究ではブラックボックス FPGA に対して新たに抽出および分類を行う手法を提案する。

## 3. 脆弱性評価のための CRAM ビットの分類手法

本研究では、エラー注入実験に基づき FPGA の脆弱性を評価する。各 FPGA における注入対象となる CRAM ビットの分類手法は以下に示す。

## 3.1 ホワイトボックス FPGA における CRAM ビット分類

旧型の 7 シリーズ FPGA では Project X-ray[1] で公開されている情報をもとに CRAM ビットの抽出および分類を行う。Project X-ray では 7 シリーズ FPGA アーキテクチャが解析されており、FPGA 上の回路構成要素と CRAM ビットの物理位置の対応関係を特定できる。

## 3.2 ブラックボックス FPGA におけるビット抽出および分類

UltraScale+ FPGA では公開情報が存在しないため、評価回路の CRAM ビットの抽出および分類をする手法を図 1 のように提案する。ダミーモジュールを設計し、2つの EBD ファイル (ビット使用情報) の AND 演算により CRAM ビットを

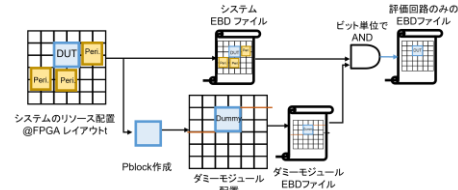


図 1 提案手法のフローチャート

抽出する。分類手法は RBD ファイル (ビット内容情報) に基づく手法を用いる。提案手法をホワイトボックスである 7 シリーズ FPGA で検証し、有用性を確認した後、ブラックボックスである UltraScale+ に適用して脆弱性を評価した。

## 4. アーキテクチャに依存した脆弱性の評価結果

評価回路を 7 シリーズ FPGA、UltraScale+ FPGA に実装し、エラー注入実験を行った。脆弱性評価の指標として、式(1)に示す AVF を用いる。

$$AVF = \frac{N_{critical}}{N_{essential}} \quad (1)$$

AVF は、エラー注入実験により得られる評価回路の故障を誘起するクリティカルビット  $N_{critical}$  と、抽出した CRAM ビット  $N_{essential}$  の比として定義され、評価回路が故障する割合を表す。図 2 に論理ビットおよび配線ビットの AVF と抽出した CRAM ビットの数を示す。

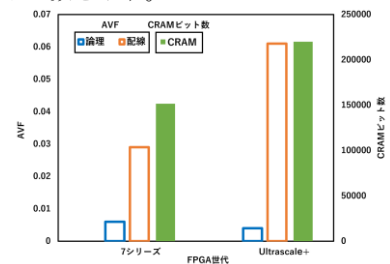


図 2 FPGA 世代間の AVF および CRAM ビット数の比較

図 2 より、CRAM ビット数は、7 シリーズと比較して UltraScale+ が増加していることが分かる。また、配線ビットの AVF も UltraScale+ FPGA の方が高い。これらの結果から、UltraScale+ FPGA は配線機能の高性能化に伴い、配線ビットの割り当てが複雑化し、冗長性が低下していると考えられる。一方で、7 シリーズと UltraScale+ FPGA の両世代において、配線ビットの AVF が最も高い傾向は共通している。この結果は、配線ビットがソフトウェアに対して比較的脆弱であるというアーキテクチャの特徴が世代間で共通していることを示唆している。

## 5. まとめ

商用 FPGA におけるアーキテクチャに依存したソフトウェアの脆弱性評価手法を提案し、脆弱性評価を行った。特に、ブラックボックスの特性を持つ先進 FPGA において、CRAM ビットの抽出およびビット分類と抽出手法の提案し、FPGA 世代間の脆弱性比較を可能にした。

## 参考文献

- [1] F4PGA Authors, "Project X-Ray Documentation," [https://f4pga.readthedocs.io/projects/prjxray/en/latest/db\\_dev\\_process/readme.html](https://f4pga.readthedocs.io/projects/prjxray/en/latest/db_dev_process/readme.html), 2025, accessed: Jun. 9, 2025.  
[2] L. A. Aranda, O. Ruano, F. Garcia-Herrero, and J. A. Maestro, "Acme-2: Improving the extraction of essential bits in xilinx sram-based fpgas," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 69, no. 3, pp. 1577–1581, 2021.