研究共有用資料

村田 絢星

電気通信大学情報理工学研究科 情報学専攻
菅原研究室

2025/10/06

本日の概要

- 目的: 私が今まで試してきた ARM プロセッサーに対するレーザーフォルトインジェクション実験について共有する
  - 明確になっている点や不明点など
- 流れ: 主に２つの実験について説明をする
  - 実験 1: ARM フォルト注入可否に関する実験
  - 実験 2: ARM フォルトの分析に関する実験
- 参考: FPGA 上のベアメタル環境を評価対象にした実験も行ったので、簡単に説明をする

実験1

- 概要：マイコン上で大きな配列を確保し、その中身の整合性を確認しながらレーザーを照射した
- 目的：ARM プロセッサーに対してフォルトを注入可能かどうか調査する
- 照射位置：下記画像の赤い四角に囲われている部分

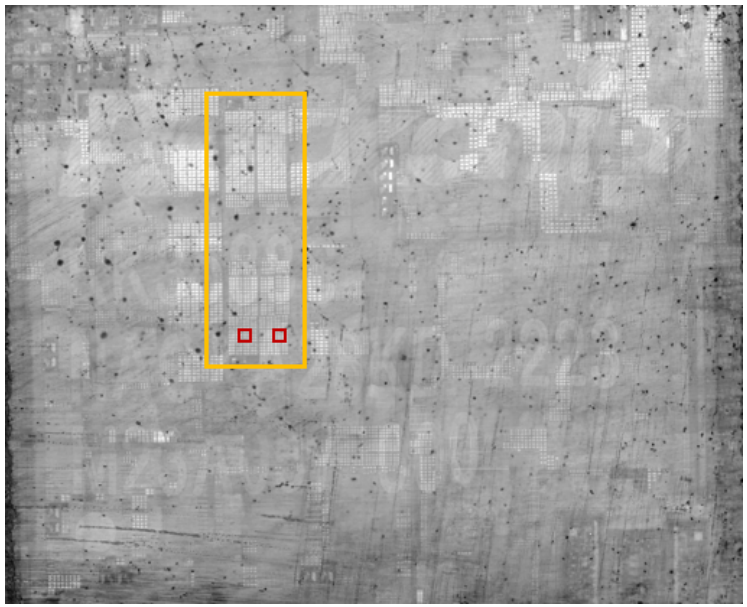

Figure: 照射位置

実験1 セットアップ

- 利用機材：
  - 評価対象: Rock5 model A 8GB
  - 利用レーザー: Maxwave MW ST60x 宝飾加工用レーザー
- 動作プログラム：
  - 大きな配列を確保し、中身を”a”という文字で埋め尽くし、整合性を確認する
  - 配列サイズはL1からL3キャッシュサイズの合計値とする

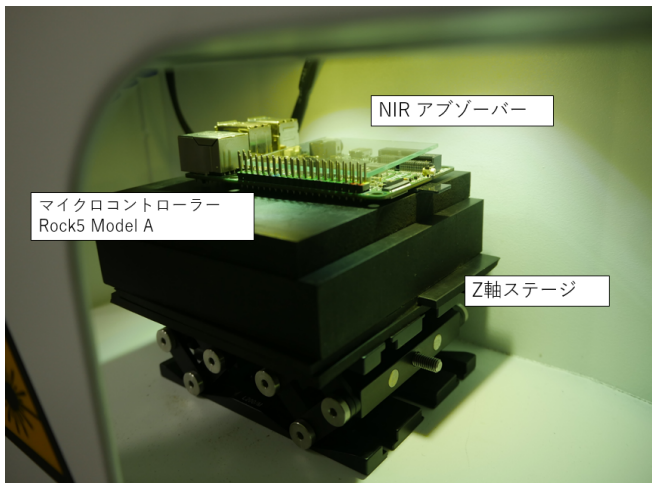

Figure: 実験環境

実験1 結果

- メモリを固定値"a"で埋めレーザー照射の前後でビットの状況を比較し、誤り注入の可否を確認した
- 40回レーザーを照射したところ、5回の誤り注入を確認した
- 1ビット反転が9割以上,2ビット以上の反転が数%確認できた
- 位置を固定して照射した場合でも、誤りの内容が異なった

Table: 変化先文字

文字	ASCII バイナリ	反転ビット数
a	0110 0001	0
q	0111 0001	1
s	0111 0011	2
!	0010 0001	1

実験1 結果

- フォルトが入るたびにCIVAC命令を呼んだ場合の実験も行った
- CIVAC命令： Clean & Invalidate
  - Clean: キャッシュラインをメモリに書き戻す
  - Invalidate： キャッシュラインの無効化
- CIVAC命令を呼ぶ場合: フォルトが次の整合性検証までに消失する
- CIVAC命令を呼ばない場合: フォルトが何度か整合性検証に検出された後消失する

実験 2

- 概要: 使用コアを制限し実験 1 と同様の実験を行う
- 目的: フォルトが L1 から L3 までのどの階層のキャッシュに注入されているか確認する
- 手法: taskset コマンドを用いることでコアの制限を行った
  - フォルトが入る照射位置を確認したのち、位置を固定した状態で使用するコアを変更した。
    それに伴ってフォルトの注入可否が変化するか検証した

実験2 セットアップ

- 利用機材: 実験 1 と同様
- 動作プログラム: 実験 1 と同様に大きな配列内のデータ整合性をチェックする
- チップ仕様: Rock5 は 4 つの Cortex-A76 と 4 つの Cortex-A55 で構成されている RK3588S チップを採用している
  - コア番号 0 から 3 が Cortex-A55
  - コア番号 4 から 7 が Cortex-A76
- big.LITTLE 技術が採用されている
  - 負荷が大きいタスクは優秀なコアが担当し、負荷が小さいタスクは能力の低いコアが担当するという方式

実験2 結果

- 結果: 複数の Cortex-A76 にフォルトが入ることが判明した
  - コア 4 とコア 5 をそれぞれ単独使用した際にフォルトが入るということが判明した
- 考察: 注入できたフォルトは L3 キャッシュにフォルトが注入できていると思っている
  - L1 と L2 はコアそれぞれに専用のキャッシュメモリが実装されている
  - 照射対象が L1 もしくは L2 キャッシュメモリだった場合、同位置で照射した際に別のコアにフォルトが入ることはないと考えられる

ARM チップ関連実験 まとめ

- 出来ている点
  - フォルトをキャッシュメモリに対して注入すること
  - おそらく L3 キャッシュに注入できていると思っている
    - もう少し正確な検証が必要と考えている
- 出来ていない点
  - フォルトに関する再現性: 反転するビットや注入されるアドレスの再現性
  - このフォルトを利用したエクスプロイト

FPGA に関する実験まとめ 1/2

- 概要: FPGA に対してレーザーを照射して実験を行った
  - 実験 1 フォルトの注入可否に関する実験
  - 実験 2 フォルトの操作性に関する実験
  - 実験 3 フォルトを用いて AES の秘密鍵導出をする実験
- 利用機材 :
  - 評価対象: Xilinx Kintex-7 XC7K160T
    - ソフトコアプロセッサ Microblaze を 動作させる
  - 利用レーザー: Maxwave MW ST60x 宝飾加工用レーザー
- 実験手法 :
  - 実験 1,2 大量のメモリを配列で確保し、ビットの反転状況を監視した
  - 実験 3 Microblaze 上に AES を実装し、制御用 PC に平文と暗号文のペアを送信するようにした

FPGA に関する実験まとめ 2/2

- 結果：
  - 実験 1,2: 照射を行う BRAM のタイル位置とフリップするビットの位置に相関があることが分かった
  - 実験 3: フォルトが入りやすいアドレスに対して Sbox を配置した
    その後 PFA[1] という解析手法を利用して、AES のマスターキーの導出が出来た
- 今後：
  - FPGA に関する結果をまとめて一度論文にしたいと思っている
  - SCIS2026 予定

[1] Fan Zhang et al. “Persistent Fault Analysis on Block Ciphers”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2018 (2018), pp. 150–172.

補足資料 1

- 補足資料 1:Rock チップ全体の透過画像

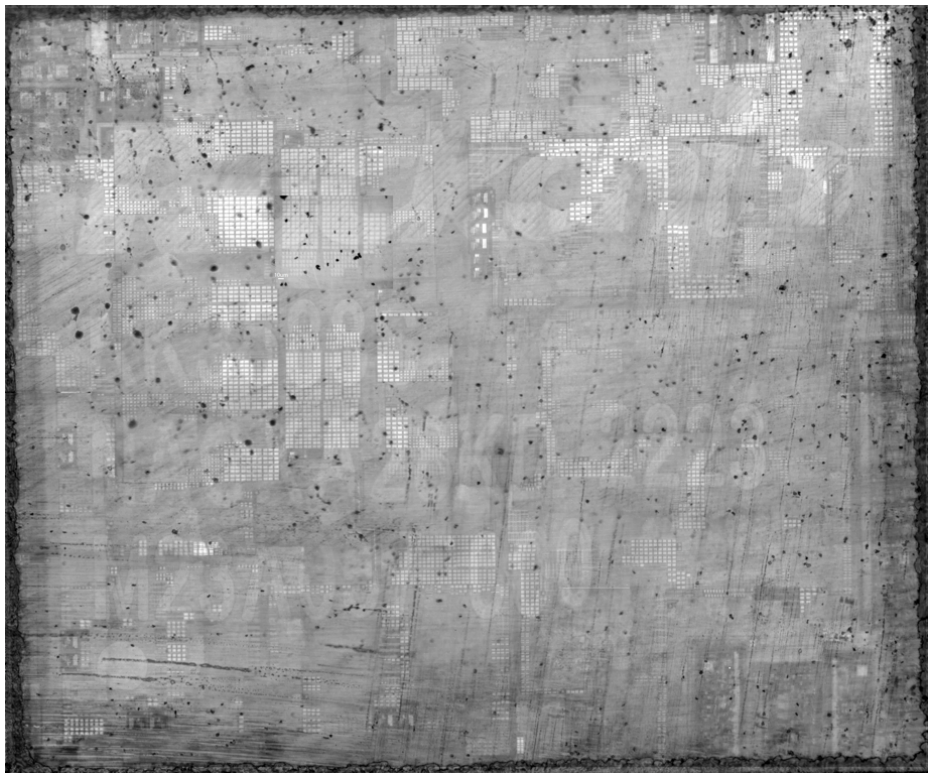

Figure: Rock チップ全体の透過写真

補足資料 2

- 補足資料 2:FPGA 全体の透過画像

Figure: FPGA 全体の透過写真