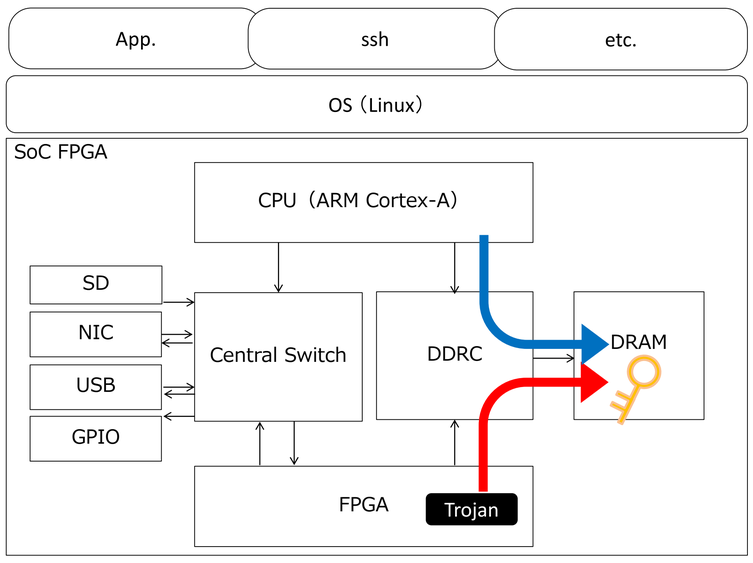
DEMO-14: アプリの暗号鍵を窃取するSoC FPGAの脅威

澤 豊文　　須崎 有康
情報セキュリティ大学院大学

1. 研究背景

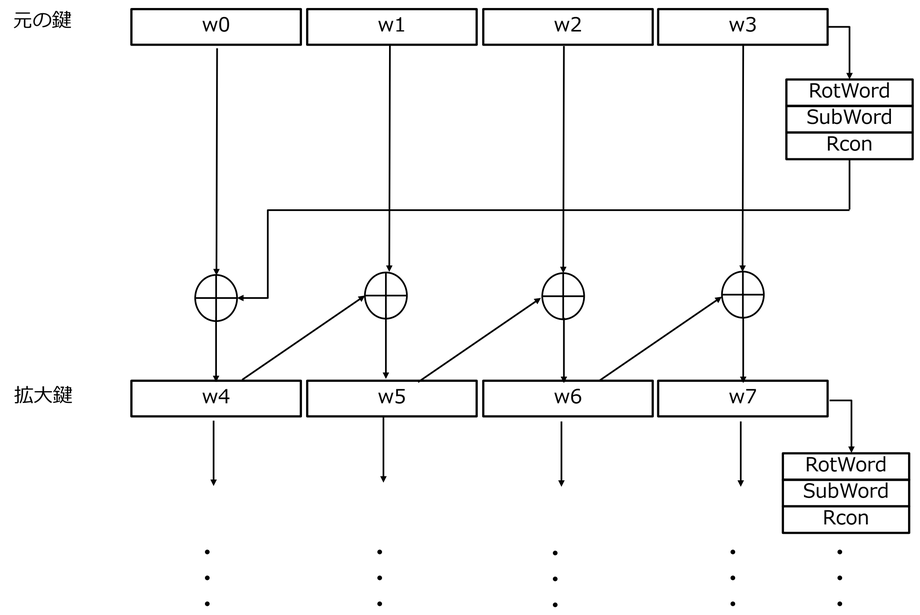
SoC FPGAはCPUとFPGAが1個のチップに収まったアーキテクチャ．CPUとFPGAがメモリや各種コントローラを共有することから，その上で動作するソフトウェアがFPGAによるハードウェアレベルの攻撃を受けるおそれがある．



FPGA上の暗号鍵を窃取する方法として，サイドチャネルや暗号ハードウェアに対するハードウェアトロイなどが研究されているが，新たにDirect Memory Accessとフォレンジック技術を利用したハードウェアトロイの脅威の存在を明らかにする．

2. 提案手法

AESの鍵スケジュールに注目する．鍵スケジュールはメモリ上に配列として並ぶ．これを検索する手法はAESKeyFinderとして知られている．

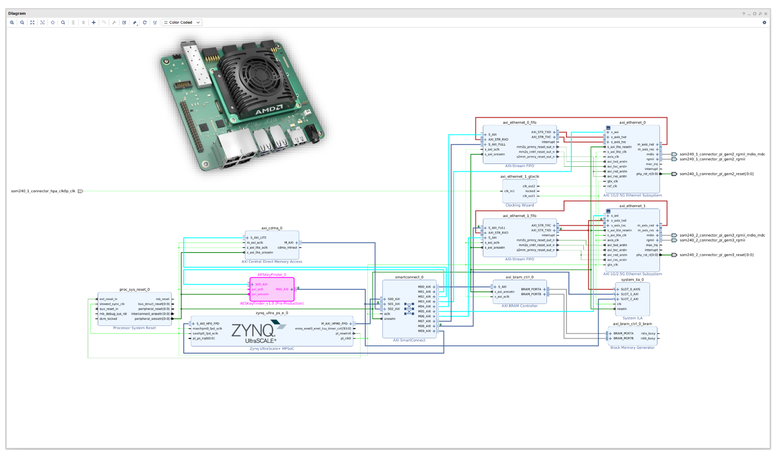


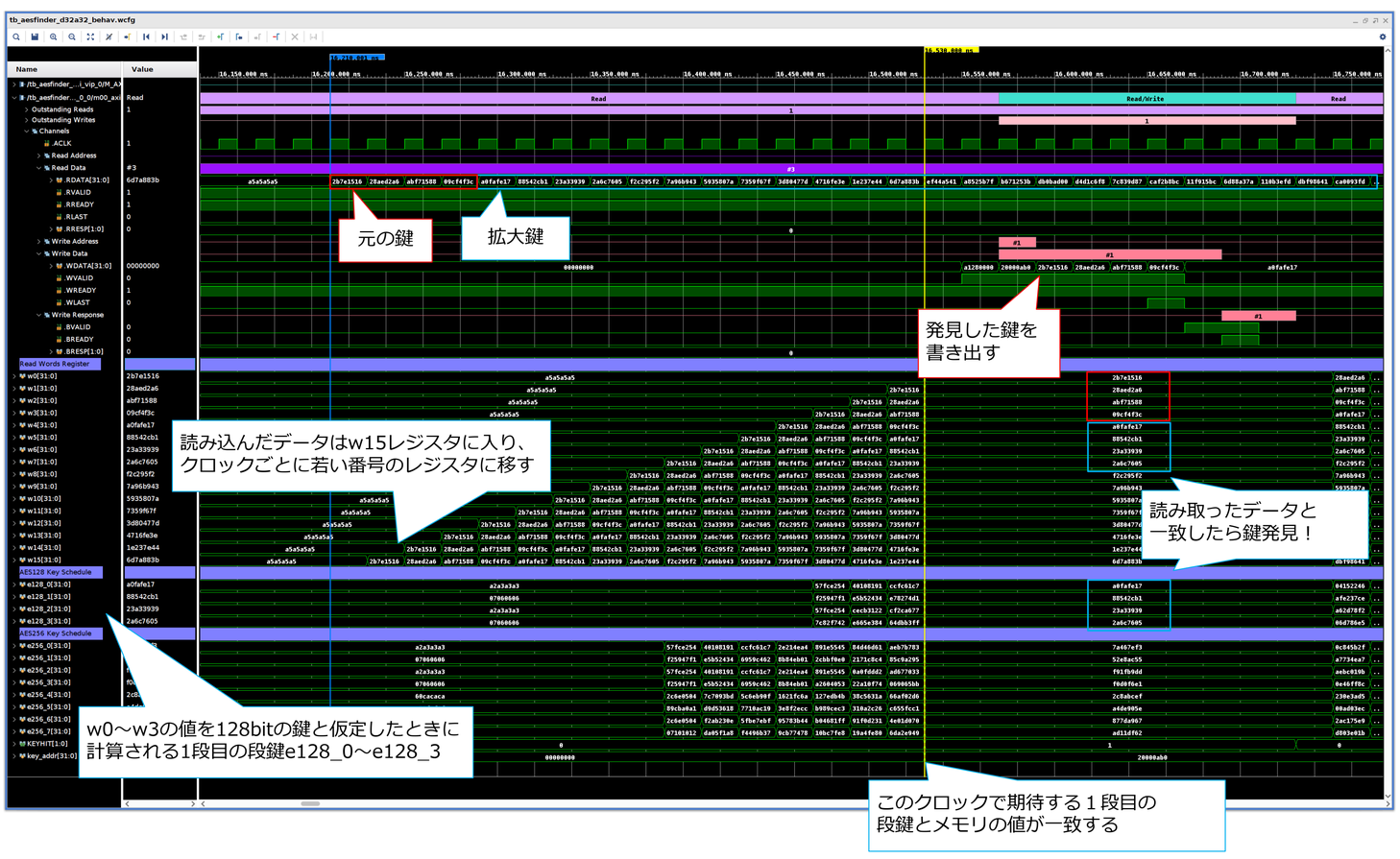
FPGAでDMAを行い，ハードウェア実装したAESKeyFinderにデータを読み込ませることで，メモリからAESの鍵を発見できるはずである．

3. 実装

AESKeyFinderのIPコアを実装した．
FPGAからAXIバスを経由したDMAを行い，メモリをスキャンする． １クロックごとに先に読み込んだデータをAESの鍵と仮定し，後続のデータがAESの鍵スケジュールと一致するか判定する．
128ビットのAESの鍵を32ビットデータ幅アクセスで発見するシミュレーションを右図に示す．

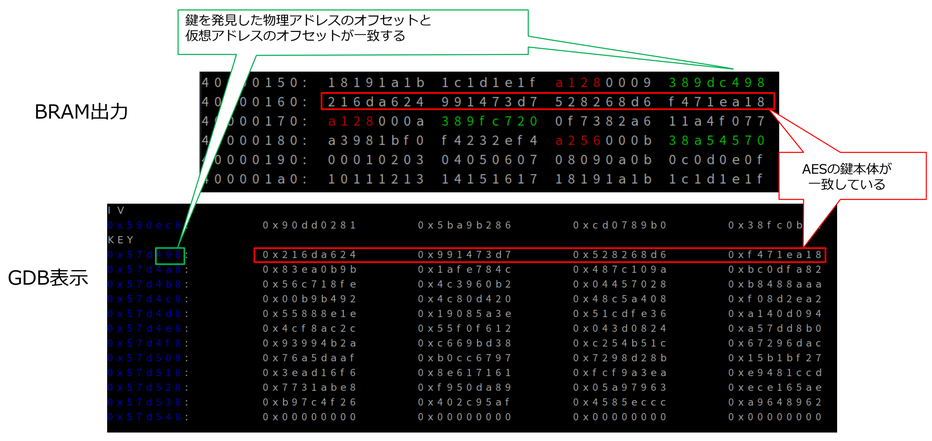
下図はデモンストレーション用のFPGAプログラムのブロックデザインである．
処理結果はBRAMまたはEthernetに出力できる．





4. 実験

評価ボードZC702及びKR260でAESの鍵を発見できるか実験を行った．
GDBでsshdをデバッグし，表示させたAESの鍵とFPGAでBRAMに書き出した結果が一致することを確認した．



結果：メモリに存在するAESの鍵をFPGAから発見できた

5. まとめ

SoC FPGAにおいて、DMAとAESKeyFinderを用いてメモリに存在するAESの鍵をリアルタイムに窃取する攻撃の可能性を明らかにした．
新規性：FPGAのDMAとAESKeyFinderとの組み合わせ
（CPUが利用するメモリを検索するハードウェアトロイ）
強み：リアルタイムに数秒で複数の鍵を発見できる
（評価ボードKR260の4GB RAMを7秒以下でスキャン）

今後の取組み

- AES以外の暗号鍵検索への対応
- リソース使用率、実行時間、ソフトウェアへの影響の評価
- PCI Express接続のFPGAへの適用
- ランサムウェア対抗策としての応用の検討

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY