FPGAを含むシステム用のFPGA回路の部分的難読化について

金沢工業大学 情報工学専攻 中沢研究室 1D1-3 北川裕基

研究概要

背景

SmartNICやFPGA Acceleration Boardといったデータセンタ用のものや、eFPGAといった組み込み向けのものも注目され始めている。FPGAのセキュリティを確保する方法の一つにFPGA設計を難読化し、IP（知的財産）保護や改ざん防止により攻撃の時間とコストを増加させることを目的に研究されている。しかし、高速化や最適化のための利用とセキュリティのトレードオフを考慮する必要がある。

問題

考慮すべき設計上のトレードオフ

- 電力消費
- 回路面積
- パフォーマンス
- Logic Lockなどの最適化との兼合い

難読化によるセキュリティ

- SAT攻撃に対する耐性

提案

1. FPGA内の回路で難読化を行いたい部分と行わなくていい部分を選択的に分けられることを考慮
2. 適切な難読化方法を行えるような仕組みを取り入れられないか検討。
3. FPGA活用のユースケースに沿った難読化

難読化の方法

いくつか方法があり検討する

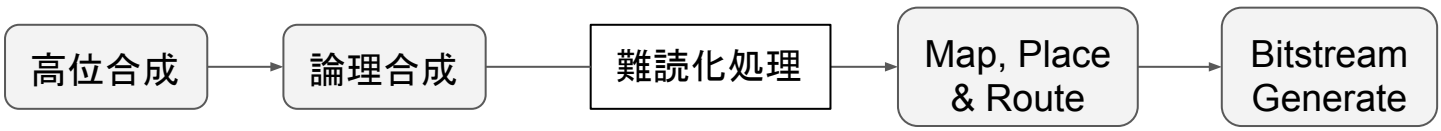
- LUT-Base Obfuscation
- FSM-Base Obfuscation
- Path Obfuscation

など

難読化をするための方法

1. CやC++などで記述し高位合成し、verilog, VHDLに変換
2. verilog, VHDLからRTLへ論理合成
3. 選択部分に部分的に任意の難読化を施す

FPGA設計時難読化フローイメージ図



評価方法

- SAT攻撃への耐性により難読化そのもののセキュリティ的な評価
- 最適化の際と難読化をした場合の設計上のトレードオフとの評価

FPGA活用のユースケースに沿った難読化に関して

難読化手法を示している先行研究にて、評価に使用している回路はベンチマーク用として使用しているに過ぎない。

そのため本研究では、FPGA活用のユースケースも踏まえた検討を行いたいと考えており、その一つの検討例としてネットワークデータプレーンに FPGA活用が進むケースにおいてのセキュリティ保護として活用できないか検討中である。