STEP: A Unified Design Methodology for Secure Test and IP Core Protection

P. Yeolekar[1], R.A. Shafik[1], J. Mathew[1], D.K. Pradhan[1] and S.P. Mohanty[2]

[1]Dept of Computer Science, University of Bristol, UK
[2]Dept of Computer Science and Engineering, University of North Texas, USA

Presenter:
Geng Zheng
University of North Texas
Email: gengzheng@my.unt.edu

Outline

- Introduction: Secure Test and IP Core Protection
- Motivations
- Contributions
- STEP: Proposed Unified Design Flow
- Results: AES Case Study
- Conclusions

Introduction

- Current IP core based design technology has two major security threats
  - Reverse engineering or response analyses during normal operation
  - Scan chain based attack during test

- Such design *hacking* is carried out to extract design information
  - For counterfeit product development
  - For inflicting financial and reputation damage

Previous Work

- To secure design during normal operation various approaches have been used
  - Combinational design locking [Roy *et al*]
  - HW obfuscation technique [Chakraborty *et al*]
  - Watermarking technique [Castilo *et al*]

- Also to secure design during test other approaches have been proposed
  - Scan chain scrambling technique [Hely *et al*]
  - Random inverter insertion [Sengar *et al*]

Motivation

- IP core protection does not guarantee secure test
  - As it is possible to use scan chains to identify the response patterns and extract design
- Secure test does not ensure IP core protection
  - Since it is still possible to reverse engineer or carry out response analyses
- For effective IP core protection and secure test, an unified design methodology is much needed.

University of BRISTOL

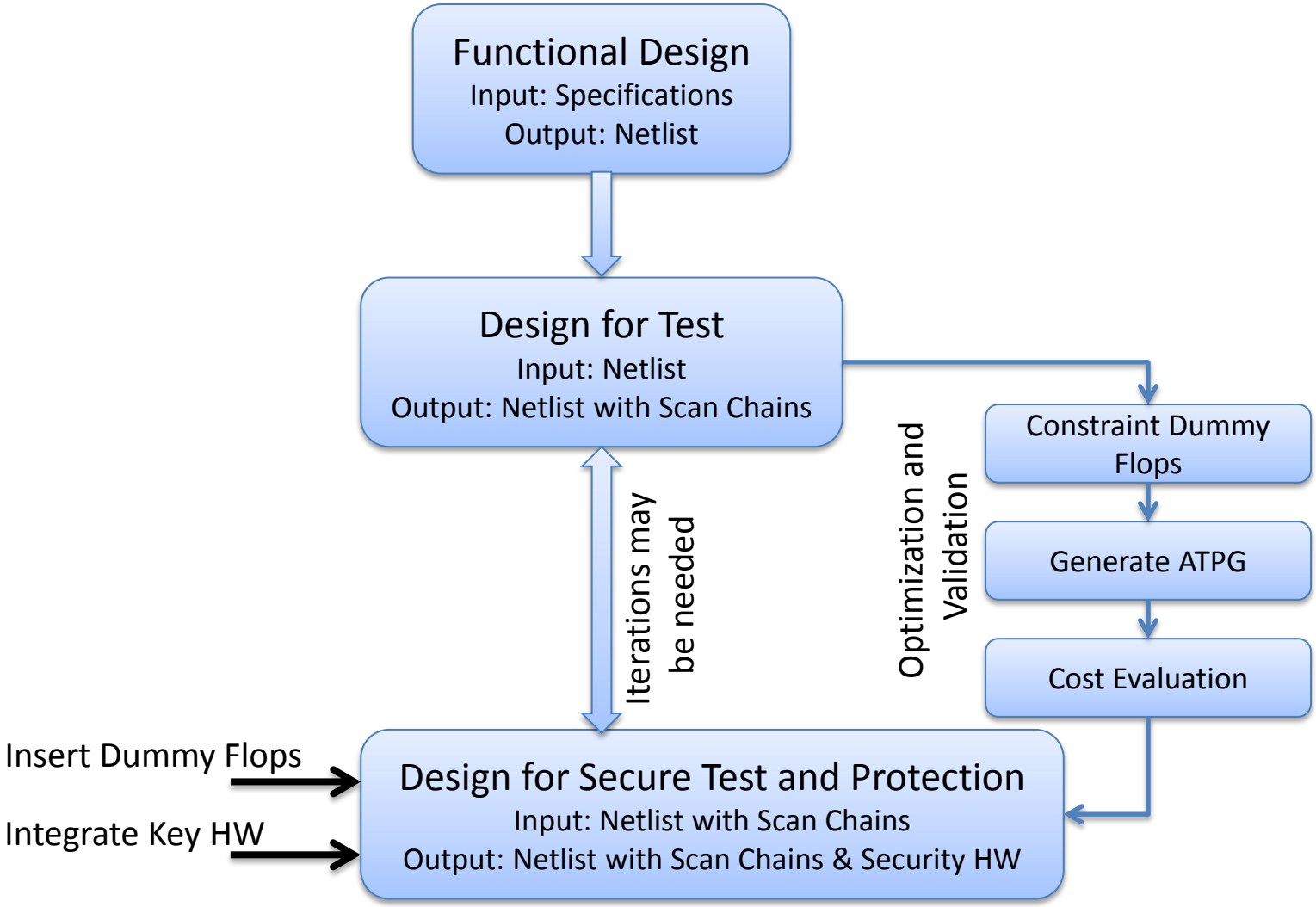
UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas

Contribution

- We propose a novel unified design methodology, STEP (**S**ecure **TE**st and IP Core **P**rotection) for
  - Protecting design information during normal functionality,
  - Securing scan chains during test

- Proposed design methodology STEP uses
  - Common secure key hardware for IP protection and secure test to reduce overall system cost
  - High randomness in the design information requiring extremely high number of combinations to ensure security

STEP: Proposed Design Methodology

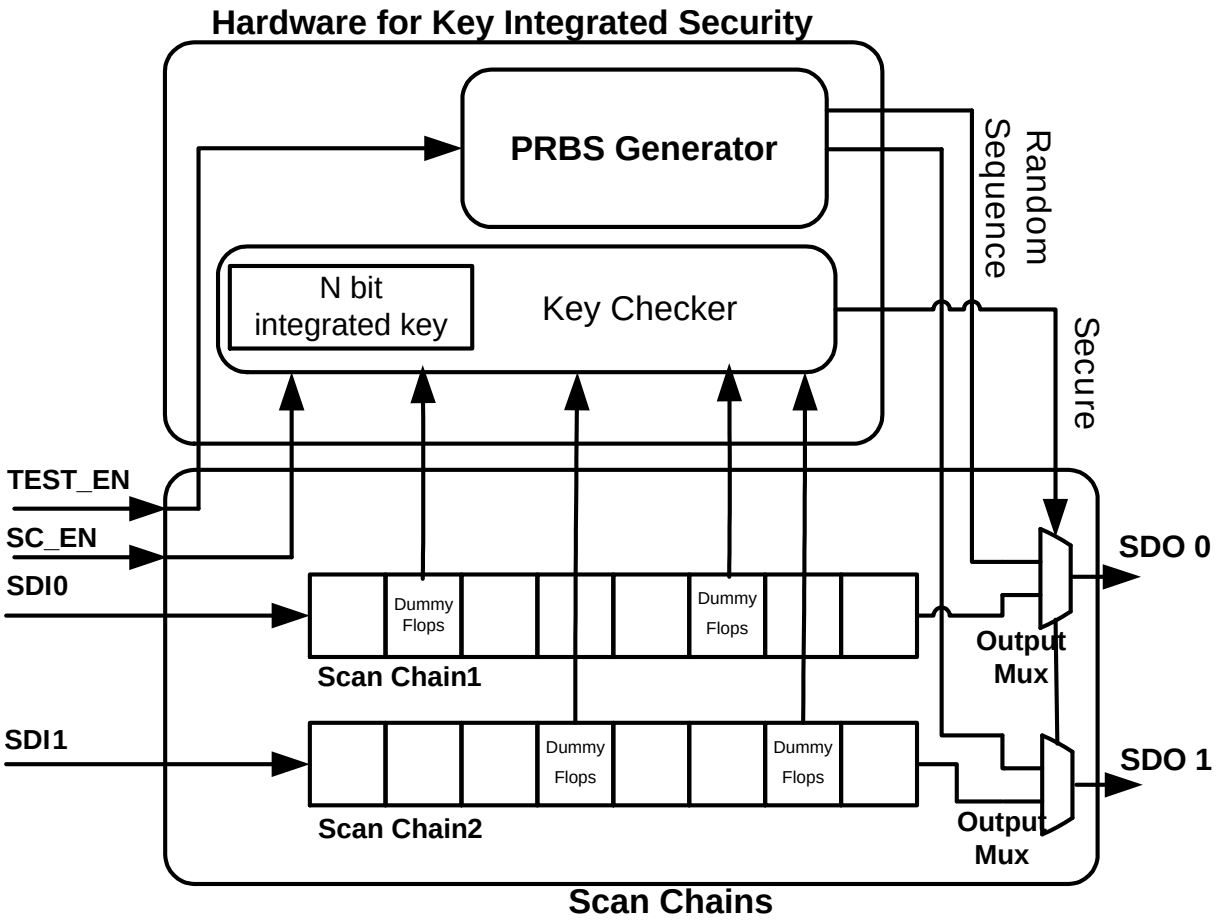


University of BRISTOL

UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas

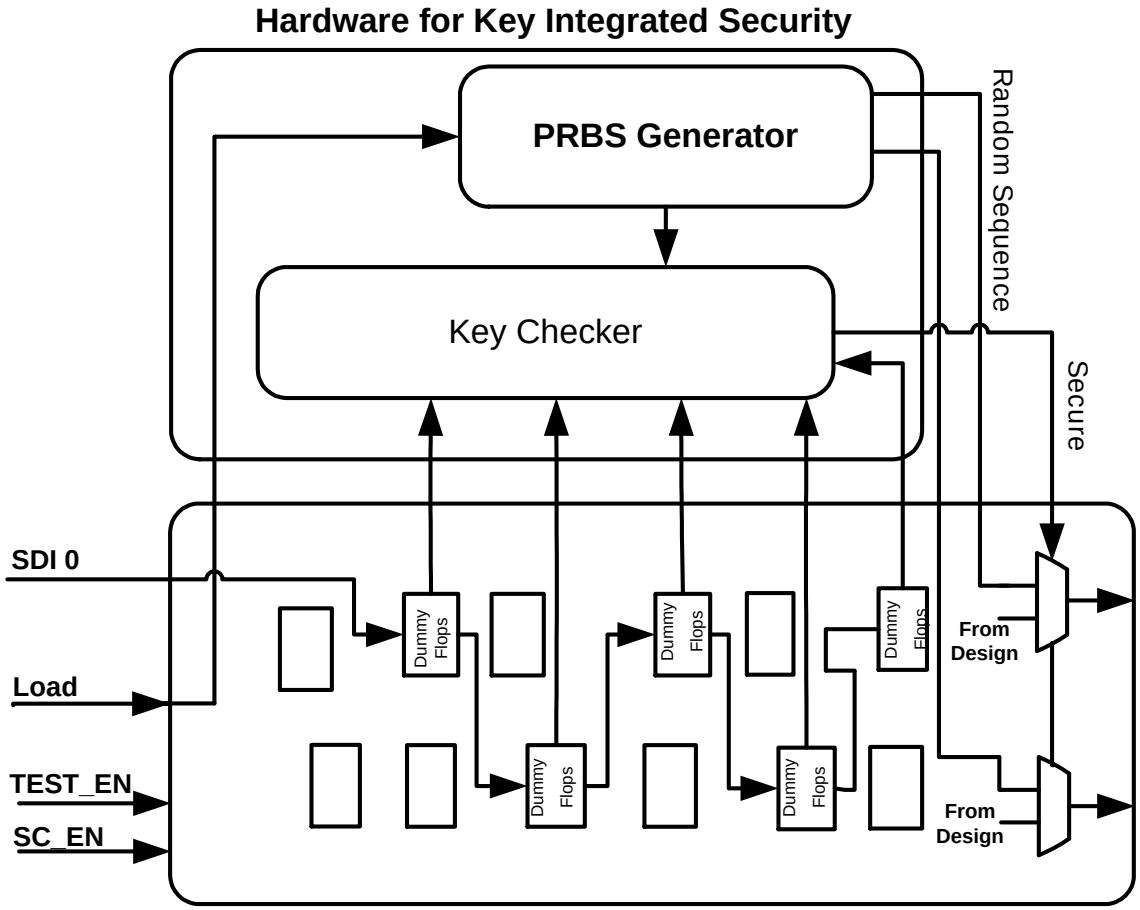
Case Study: AES

Secure Test Architecture



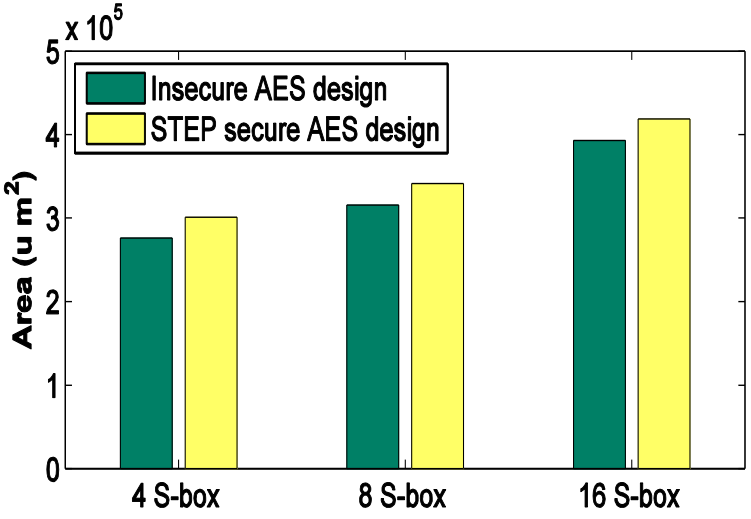
Case Study: AES [contd.]

IP Core Protection Architecture



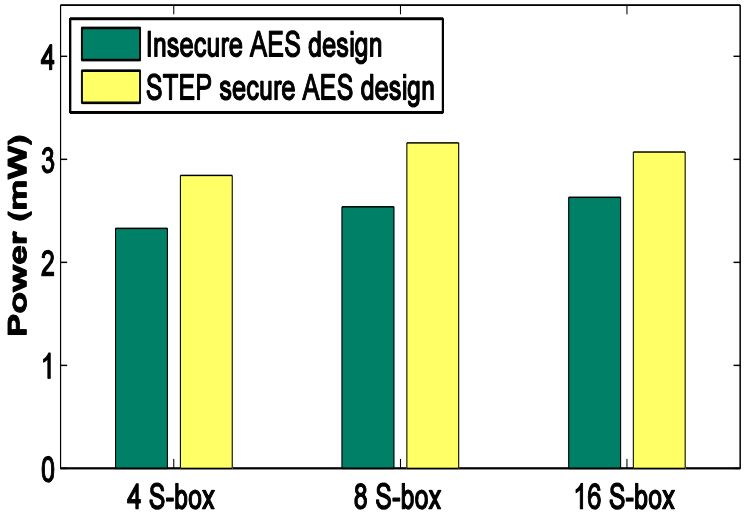
Results: AES Case Study

Area overhead



Up to 9% area overhead

Power overhead



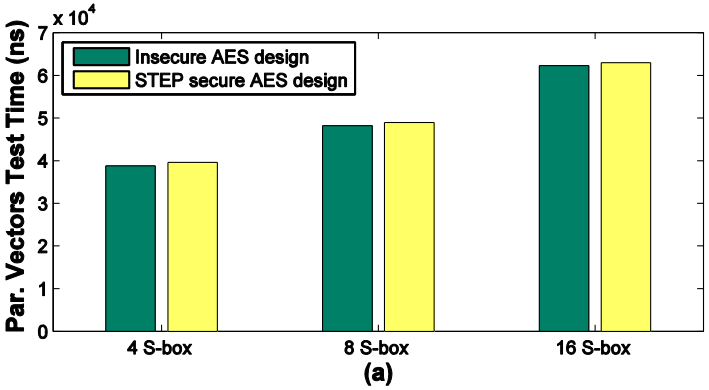
Up to 20% power overhead

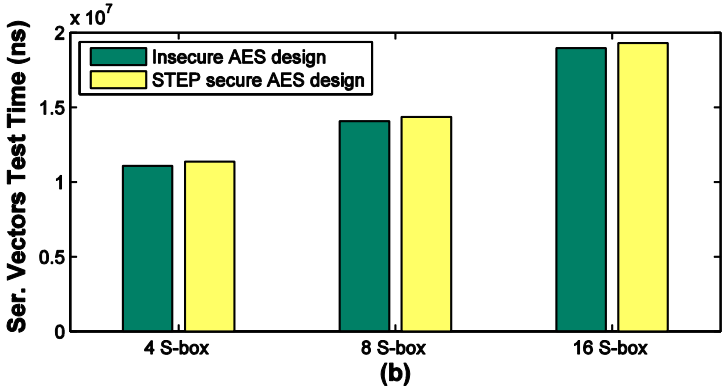
University of BRISTOL

UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas

Results: AES Case Study [contd.]

Test times

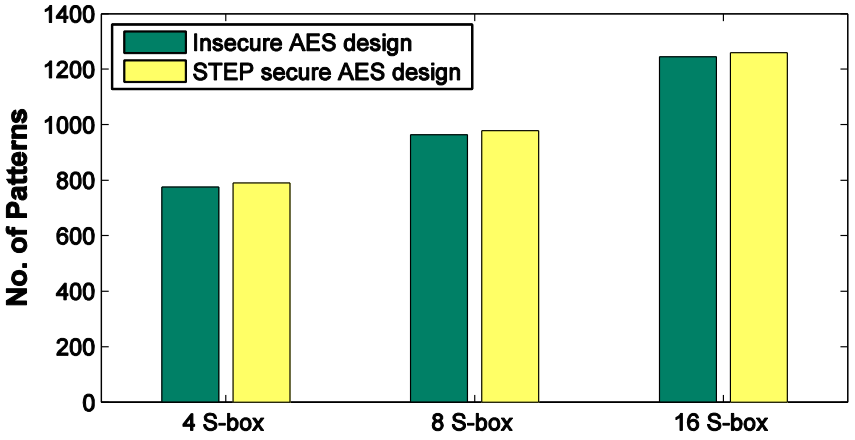




(a) Parallel vectors (b) Serial Vectors

Up to 2% extra delay in STEP AES design

Fault Coverage



Up to 2% higher number of test patterns required
For similar fault coverage in STEP AES design

University of BRISTOL

UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas

Results: AES Case Study [contd.]

Security Analyses

- Combinations required for hacking by scan chain based attack

$$C_{test} = C_N \; C_R \; C_{ff-pos} = 2^{2M} \; G \; \binom{S}{N}$$

- Combinations required for hacking during normal functionality

$$C_{IP} = C_{seq} C_{\mathcal{R}} C_{ff-con} = 2^{M(k+1)} \; G \; N! \; \binom{S}{N}$$

N := number of dummy flops inserted := length of random key
M := hackers guess of number of dummy flops
R := seed of the random number in PRBS
S := length of scan chains and G := number of scan chains
C_N := combinations required for guessing N = 2^M
C_R := combinations required for guessing R = 2^M
C_{seq} := combinations required for guessing correct key sequence with k keys = 2^{kM}
$C_{ff\text{-}pos}$:= combinations required for flip flop positions
$C_{ff\text{-}con}$:= combinations required for guessing correct flip-flop inter-connection

University of BRISTOL

UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas

Conclusions

- Proposed STEP design methodology gives
  - Novel design approach for secure test and IP core protection
  - Unified key integrated hardware to reduce overall cost
- Has been validated using AES benchmark system implementations
  - To illustrate implementation details
  - To observe system costs and
  - Demonstrate the security advantage of the system

Thank you

University of BRISTOL

UNT
UNIVERSITY OF NORTH TEXAS
Discover the power of ideas