A Comprehensive Netlist Trust Analysis Toolset for IC/IP Trust

Yier Jin
Department of Electrical Engineering and Computer Science
University of Central Florida
yier.jin@eecs.ucf.edu

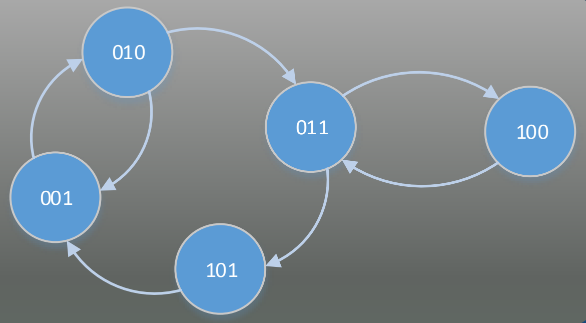
Security in Silicon Lab (SSL)

Netlist Trust Analysis

- Purpose of Netlist Trust Analysis
  - Malicious nodes detection
  - Full functionality reconstruction

```
...
   N5 = DFF(N4)
   N6 = AND(N1, N3, N5, N11)
   N7 = DFF(N6)
   N8 = AND(I1, I2, I3, N7)
   N9 = OR(N7, N8)
   N10 = DFF(N9)
...
```

```
if (indata[31:0] == 0xAAAAAAAA
 and count[30:0] == 0x0
 and sqrrdy and reset == 0 and
 multgo == 0 and ...
  cypher[31:0] <= inExp[31:0];
  root[31:0] <= 0xAAAAAAAA;
...
```

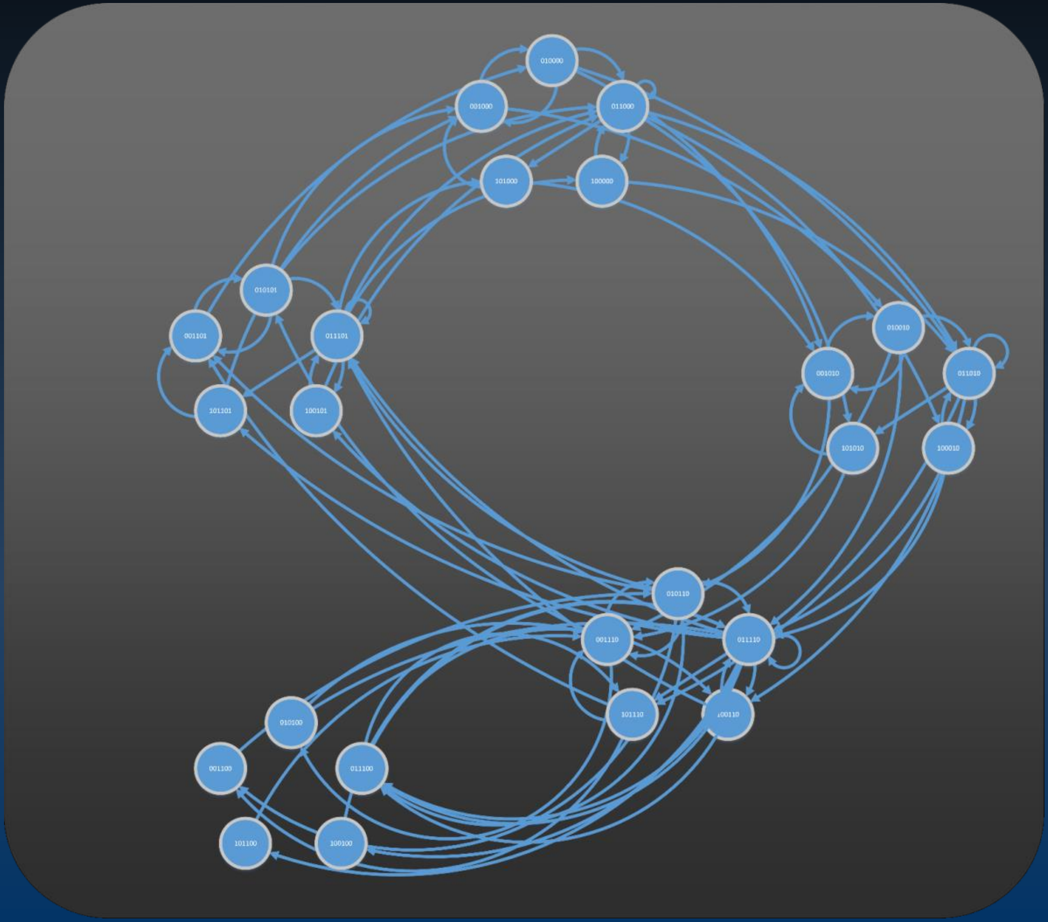


Developed Tools

- REbuilding Logic: Identification and Classification (RELIC)
  - Function: Differentiate state register and data register
  - Input: Netlist
  - Output: Gate list
- REconstructing Finite State Machine (REFSM)
  - Function: Reconstruct the control logic
  - Input: Netlist
  - Output: FSM
- Recovering Datapath and Signal Buses (REBUS)
  - Function: Reconstruct the datapath
  - Input: Netlist
  - Output: Datapath
- REHOP
  - Function: Obfuscate the netlist
  - Input: netlist
  - Output: obfuscated netlist

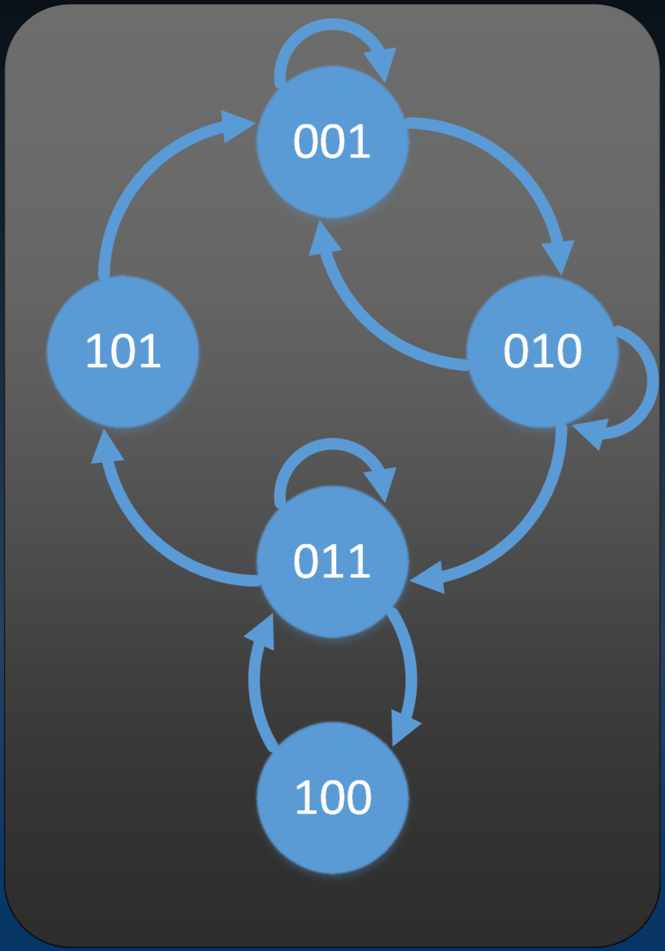
Demo for REFSM

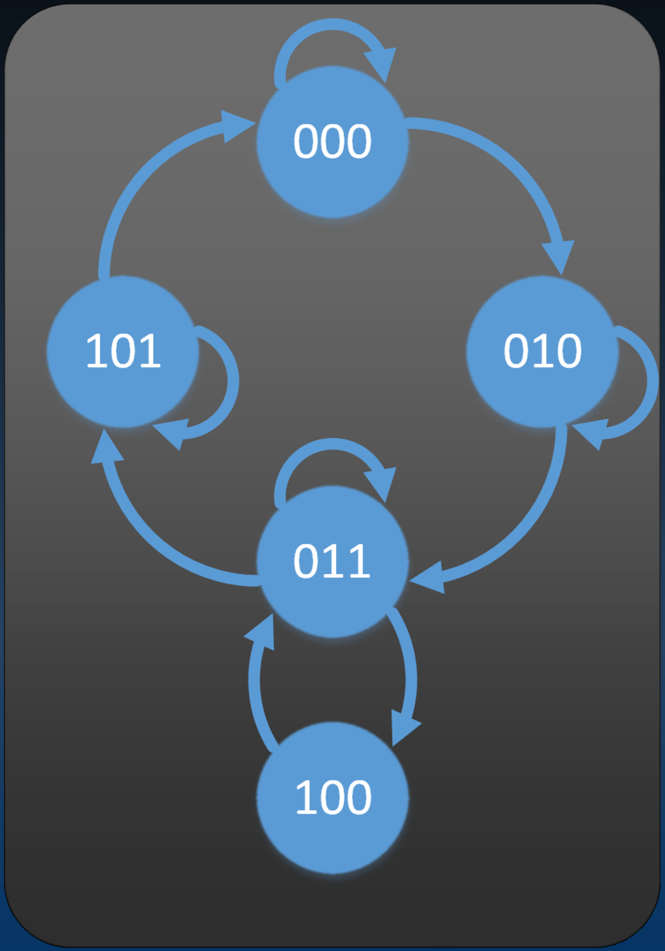
- RS232 Netlist Analysis
  - Two submodules: transmission and receiver
  - Each submodule has its own FSMs



FSM Isolation

- FSM States Independence Analysis
  - Two FSMs are separated

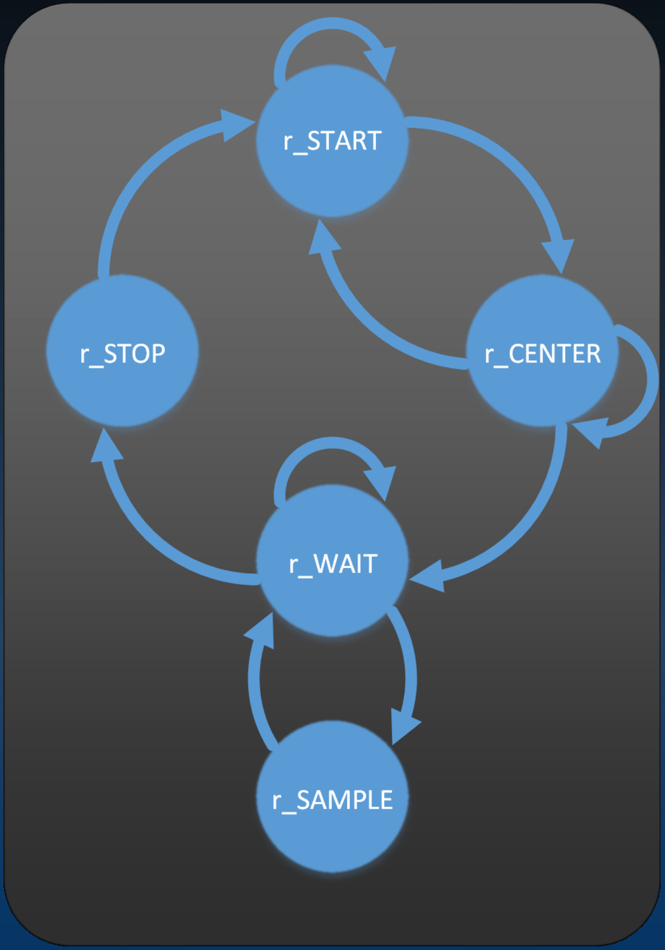




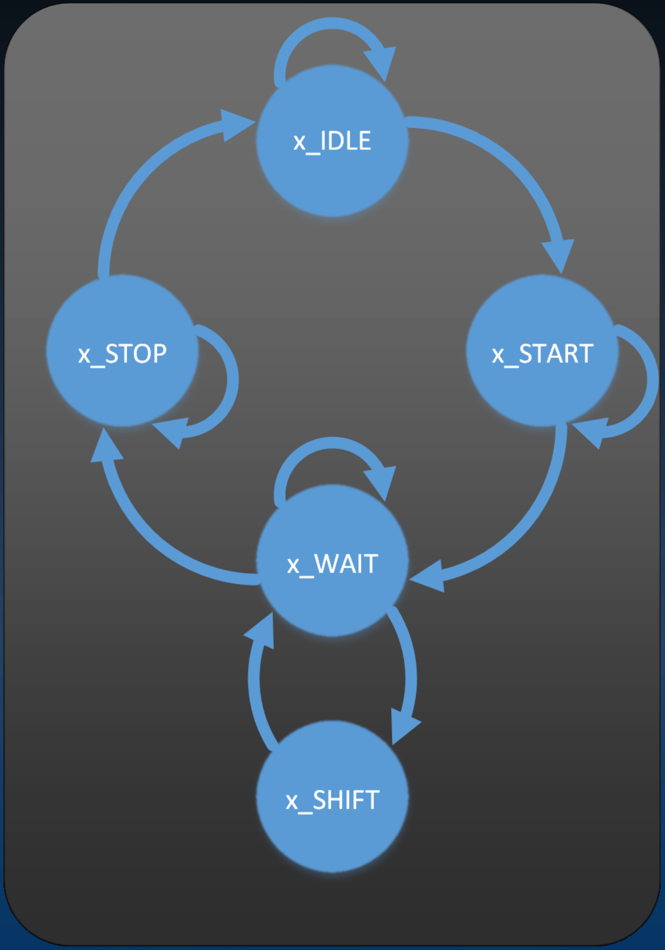
Results Validation

- Actual FSMs of Two Submodules

FSM for Receiver



FSM for Transmitter



Experimental Results

- REFSM Performance Analysis
  - Depth vs Time
  - Can handle circuits of various sizes
  - Overall computation time is low

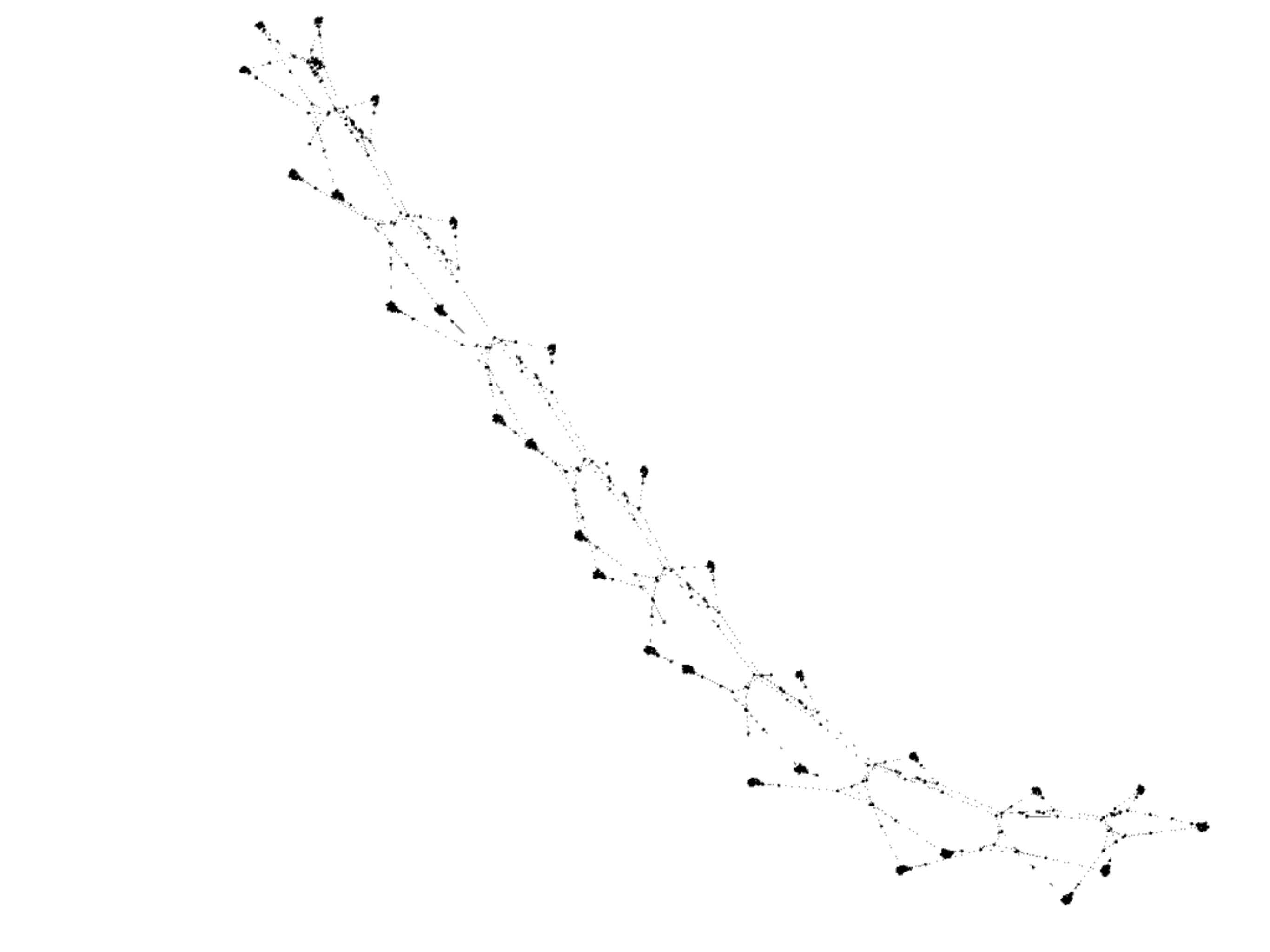
Name	Depth	Time (s)	Total Registers	Total Gates
UART	Inf	1	59	168
s349	inf	< 1	15	176
32-bit RSA	0	< 1	555	2139
MC 8051 uP	0	39	578	6590
SPARC uP	0	600	119911	232978

REBUS: Datapath Recovery

- RELIC-based Datapath Recovery Tool
  - Input: Known word (input and output data)
  - Output: A graph model of the data buses within a Netlist
- Traces Word Paths Through Netlist
  - Relies on known word signal pairs to generate new word pairs
    - Fan-out/Fan-in pairs are examined
    - Similar signals are added to the known words list
  - Edges are added based on word-to-word interactions
- Case Study
  - Pipelined version of AES-128
  - 174,856 gates (no explicit control logic, fully pipelined)

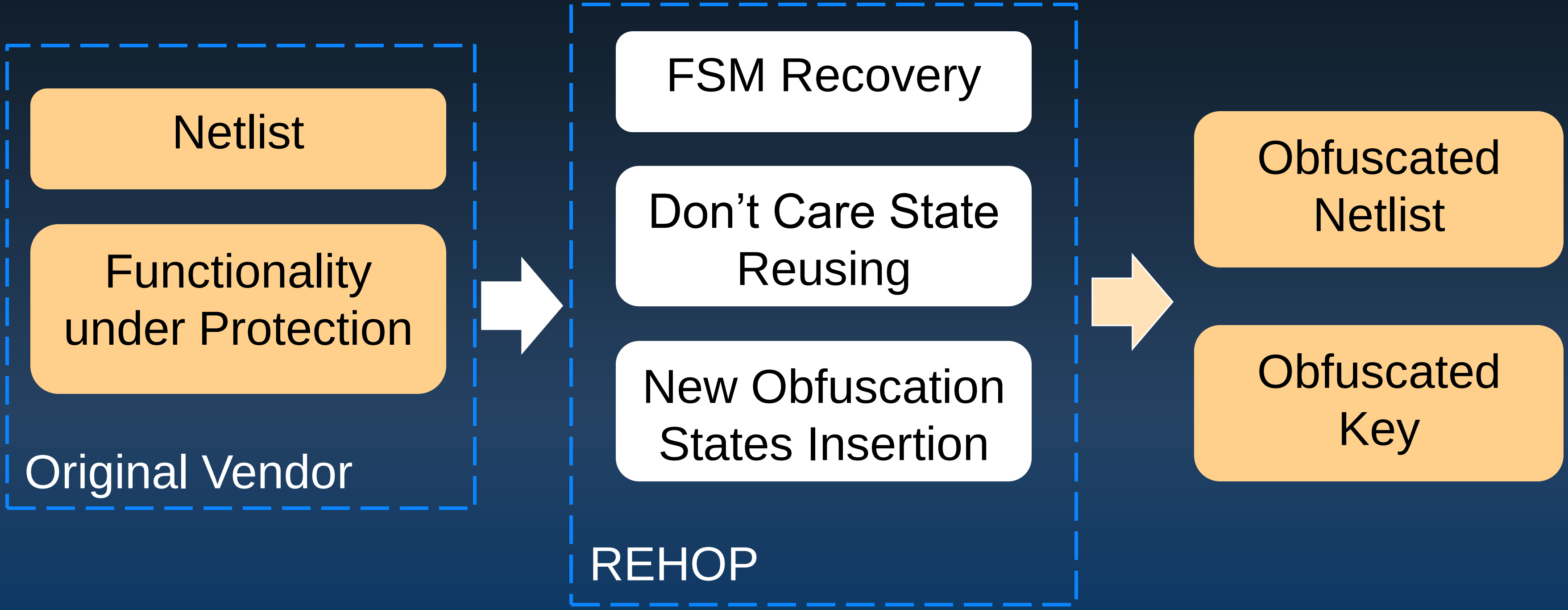
Case Study: AES-128

Case Study: AES-128



REHOP

- Objective
  - Third-party service for IP protection
  - No RTL code is required
- Working Procedure



Netlist

Functionality under Protection

Original Vendor

FSM Recovery

Don't Care State Reusing

New Obfuscation States Insertion

REHOP

Obfuscated Netlist

Obfuscated Key

Questions?

Thanks!

Yier Jin
University of Central Florida
Email: yier.jin@eecs.ucf.edu