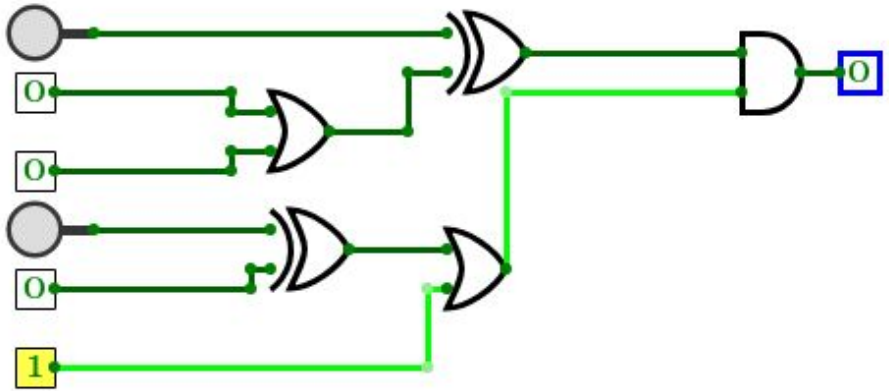
Software Implemenation of Sensitization Attacks on Obfuscated Circuits

By John McLaughlin
ECE 646 Project Presentation

Theoretical Background

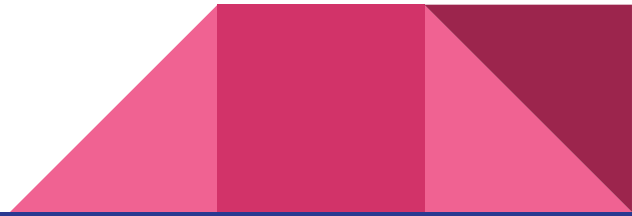
Key-based Hardware Obfuscation

- Randomly add extra gates into a digital circuit
- One of the inputs to these gates is a “key” input
- Without the proper key, the circuit will malfunction



Sensitization Attack

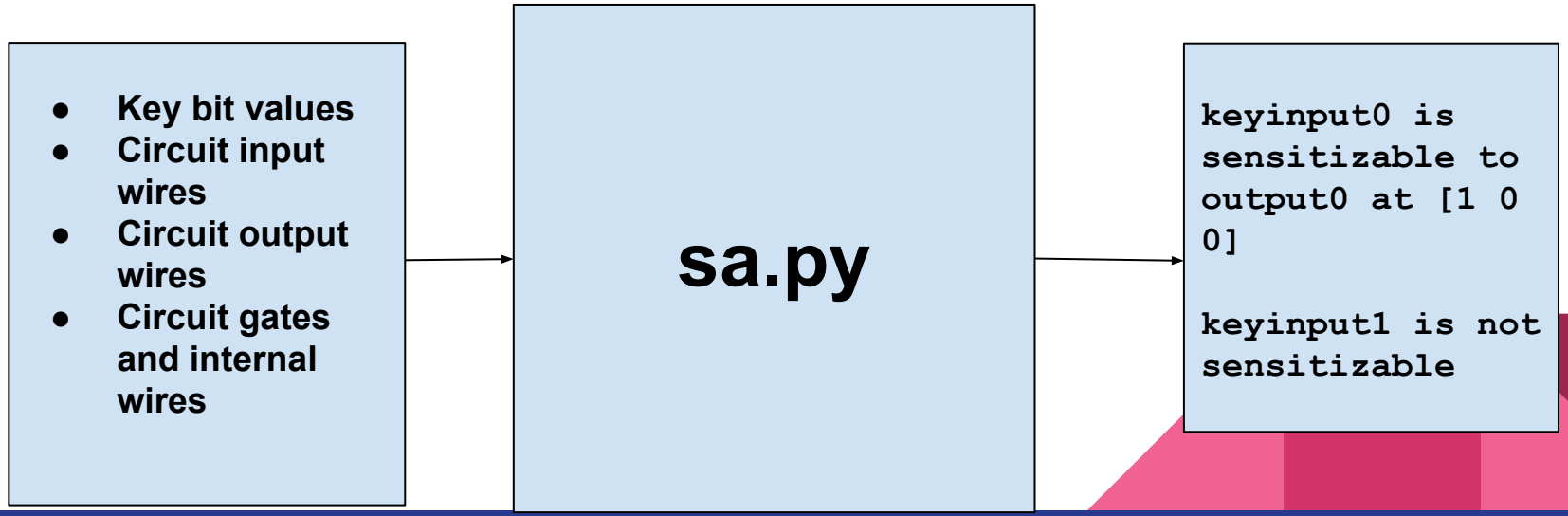
- Determining key bits by “sensitizing” them to outputs
- Attacker has a fully functioning chip with unknown, accurately loaded key
- Attacker has chip’s netlist with key gates, but unknown key
- Find input sequence that propagates a key bit to an output in the netlist
- Check output of other chip when applying that input sequence
- Repeat for each key bit



Project

Description of Project

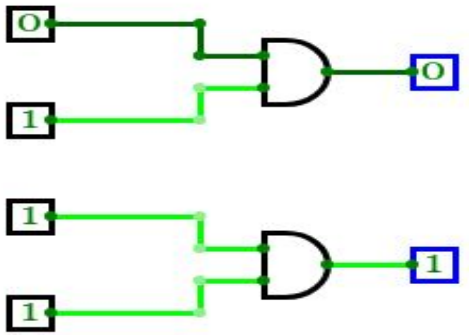
- Python script that performs a sensitization attack
- Input: .bench file, describes a digital circuit at gate level
- Output: Results of sensitization attack for each key bit



Finding propagating values

- Propagate_forward(input1)
  - Check type of gate input1 is going to
  - Set other input, input2, to **propagating value**
  - Propagate_backward(input2)
  - Other input propagated backward?
    - Yes: Is gate output a circuit output?
      - Yes: Return true
      - No: Propagate_forward(gate output)
    - No: Return false

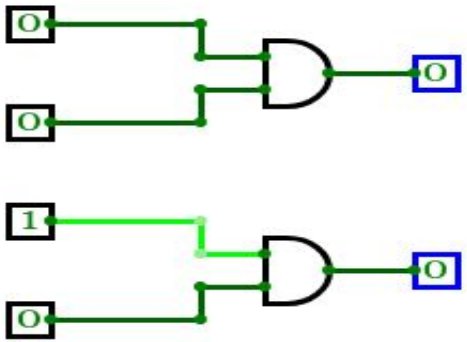
PROPAGATING VALUES	
AND	**1**
OR	**0**
XOR	**0**
XNOR	**1**



Finding muting values

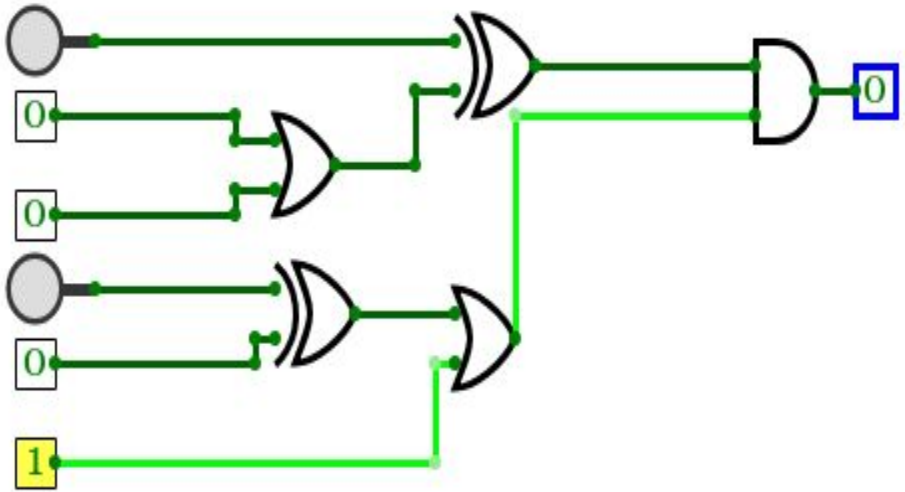
- Propagate_backward(wire)
  - Check gate type that wire is outputting from
  - Are any of the inputs key bits?
    - Yes: Set other input to **muting value**
  - Otherwise, set gate inputs to appropriate values
  - Is the gate input a circuit input?
    - Yes: Set circuit input, return true
    - No: Propagate_backward(input)

MUTING VALUES	
AND	**0**
NAND	**0**
OR	**1**
NOR	**1**



Algorithm -- Main Loop

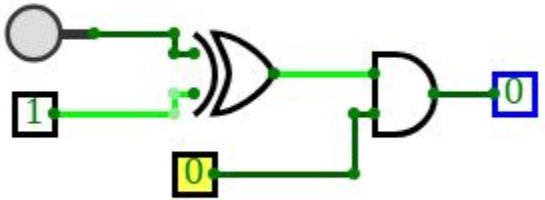
- Loop i through unsolved_keys[]
  - Propagate_forward(unsolved_keys[i])
  - Did key propagate to output?
    - Yes: Print out results
      - Set key value
      - Set i = 0
    - No: Print that key is not sensitizable



Discoveries

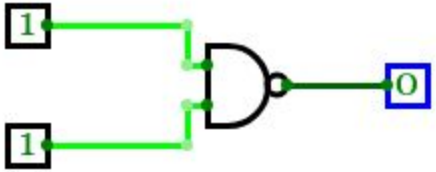
Discoveries

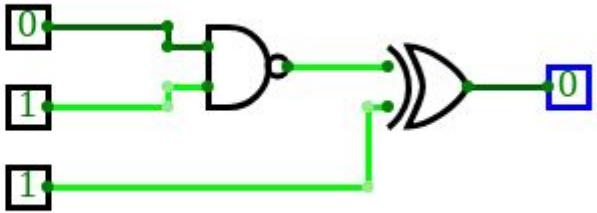
- Muting inputs to XOR, XNOR, or NOT gates require an extra gate (AND, OR, NAND, NOR)
- Cannot perform sensitization attacks on circuits with only XOR, XNOR, and NOT gates



Discoveries (2)

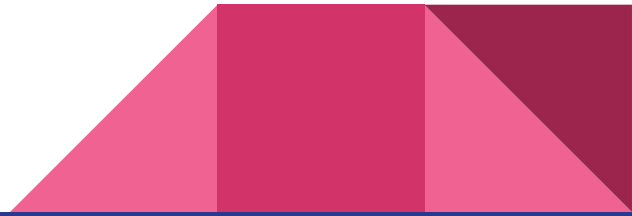
- Propagating through NOR, NAND, or NOT gates require extra gates
  - NOR and NAND gates propagate the opposite value
  - Add a NAND or XOR gate to first gate's output, feed a 1 to other input, or
  - Add a NOR or XNOR gate to first gate's output, feed a 0 to other input, or
  - Add a NOT gate to first gate's output





End

- Special Thanks to
  - Dr. Sasan
  - Dr. Gaj
  - Shervin Roshanisefat
  - Hadi Mardani Kamali
  - Kimia Zamiri Azar



Questions?