Hardware IP Protection

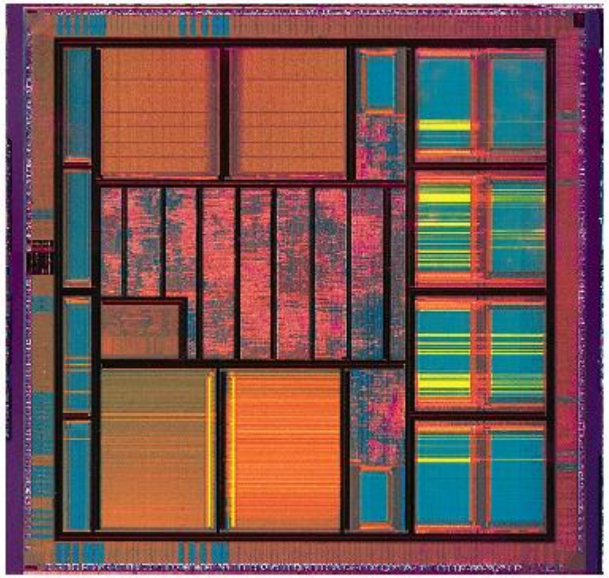
Yu Bi

ELE594 – Special Topic on Hardware Security & Trust

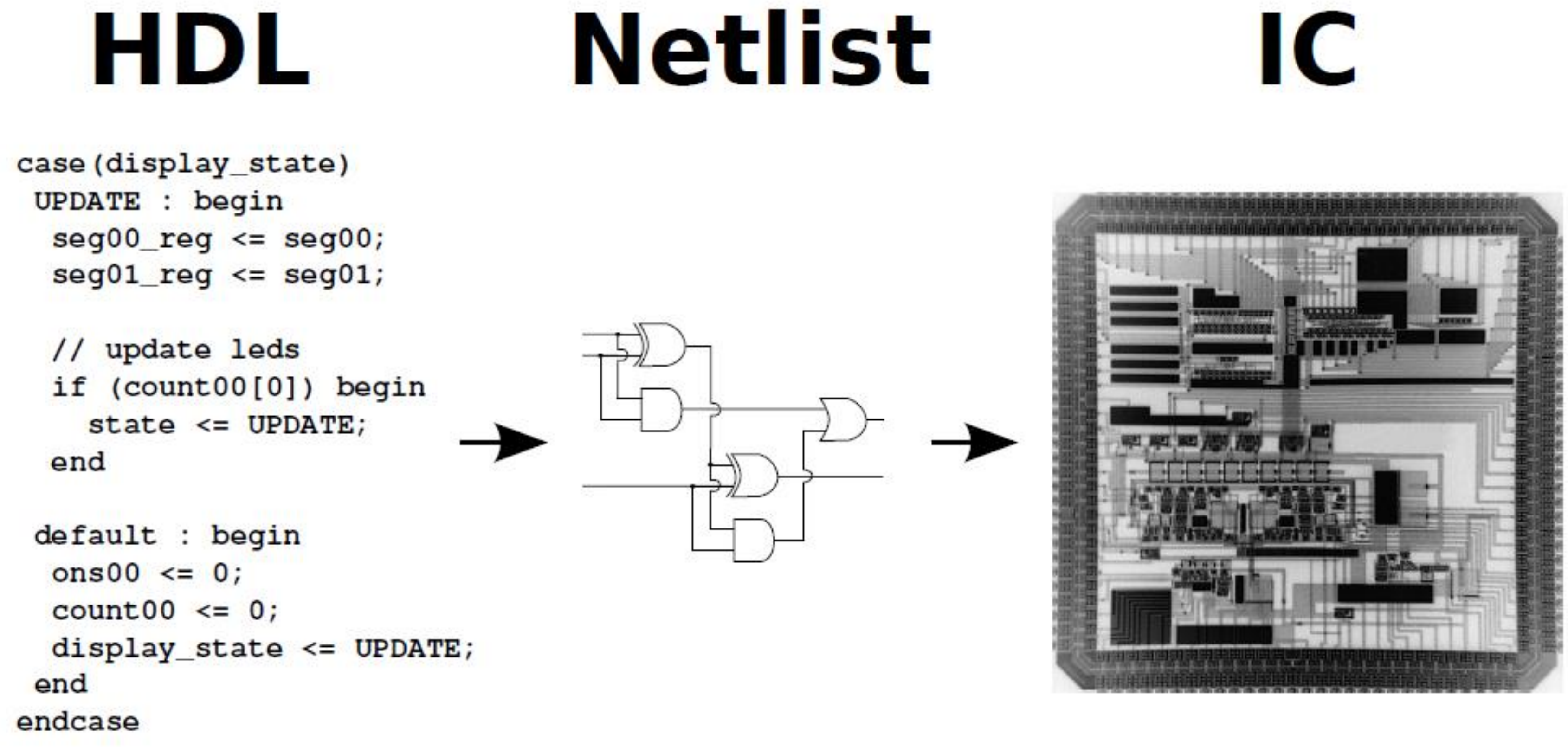
University of Rhode Island

Computer Hardware

- Computer Hardware = Digital IC
- Physical realization of digital logic
- Complex and ubiquitous

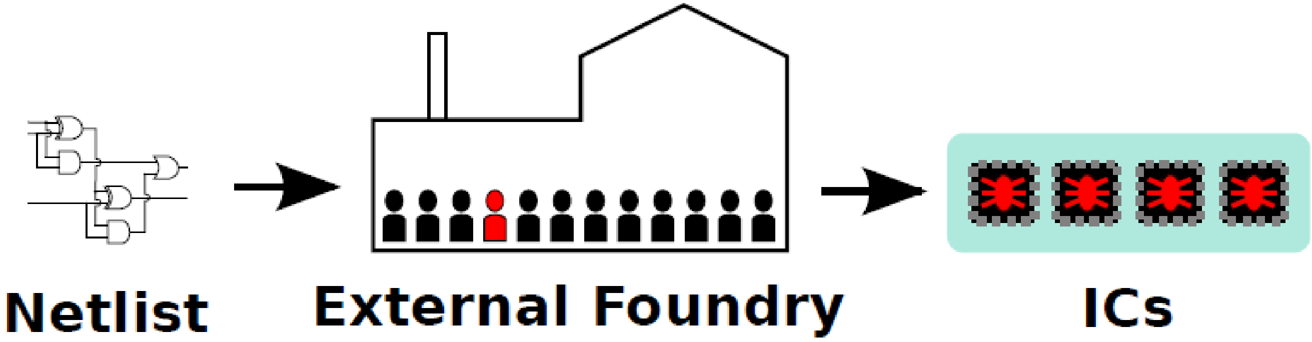


Manufacturing Process



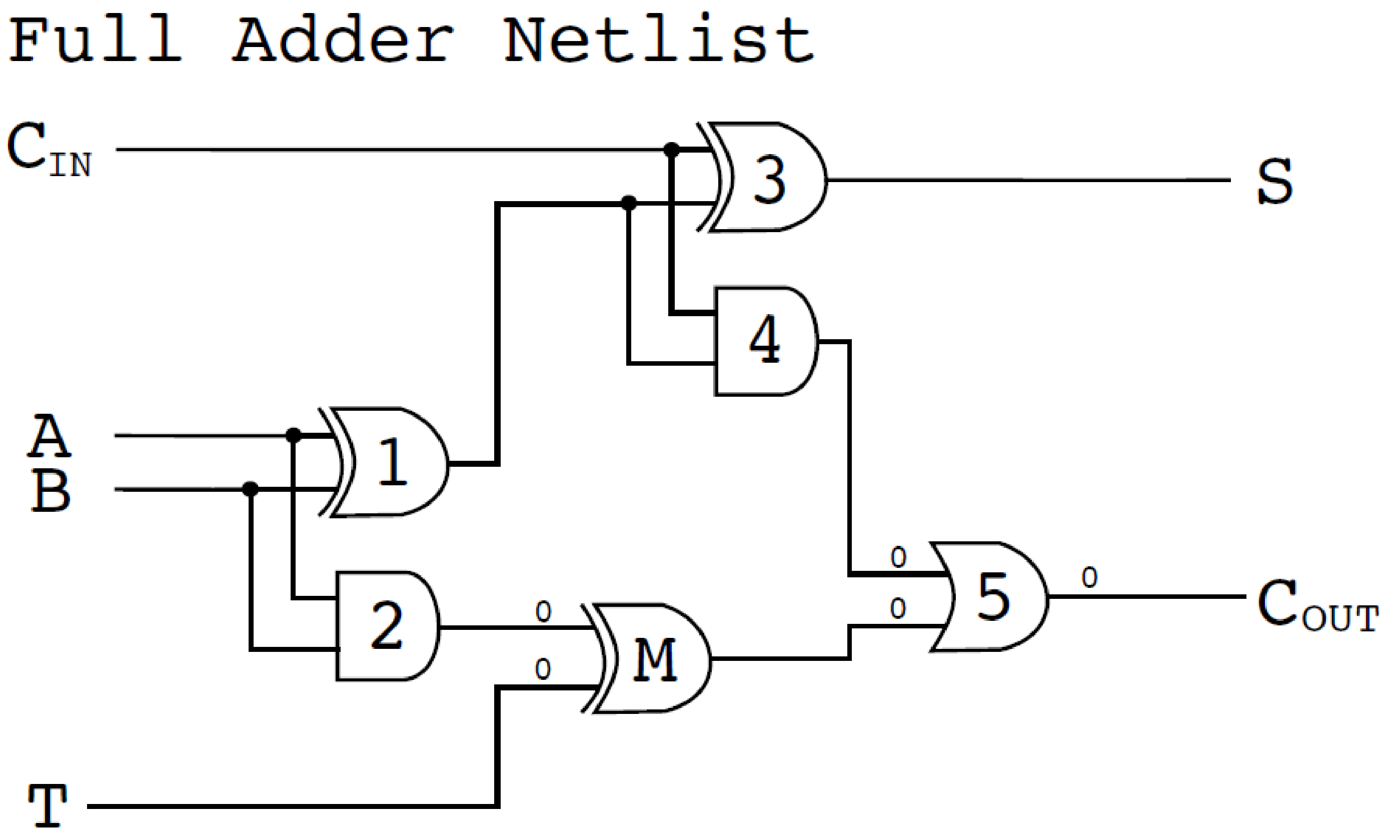
```
case(display_state)
 UPDATE : begin
  seg00_reg <= seg00;
  seg01_reg <= seg01;

  // update leds
  if (count00[0]) begin
    state <= UPDATE;
  end

 default : begin
  ons00 <= 0;
  count00 <= 0;
  display_state <= UPDATE;
 end
endcase
```

Threat Model



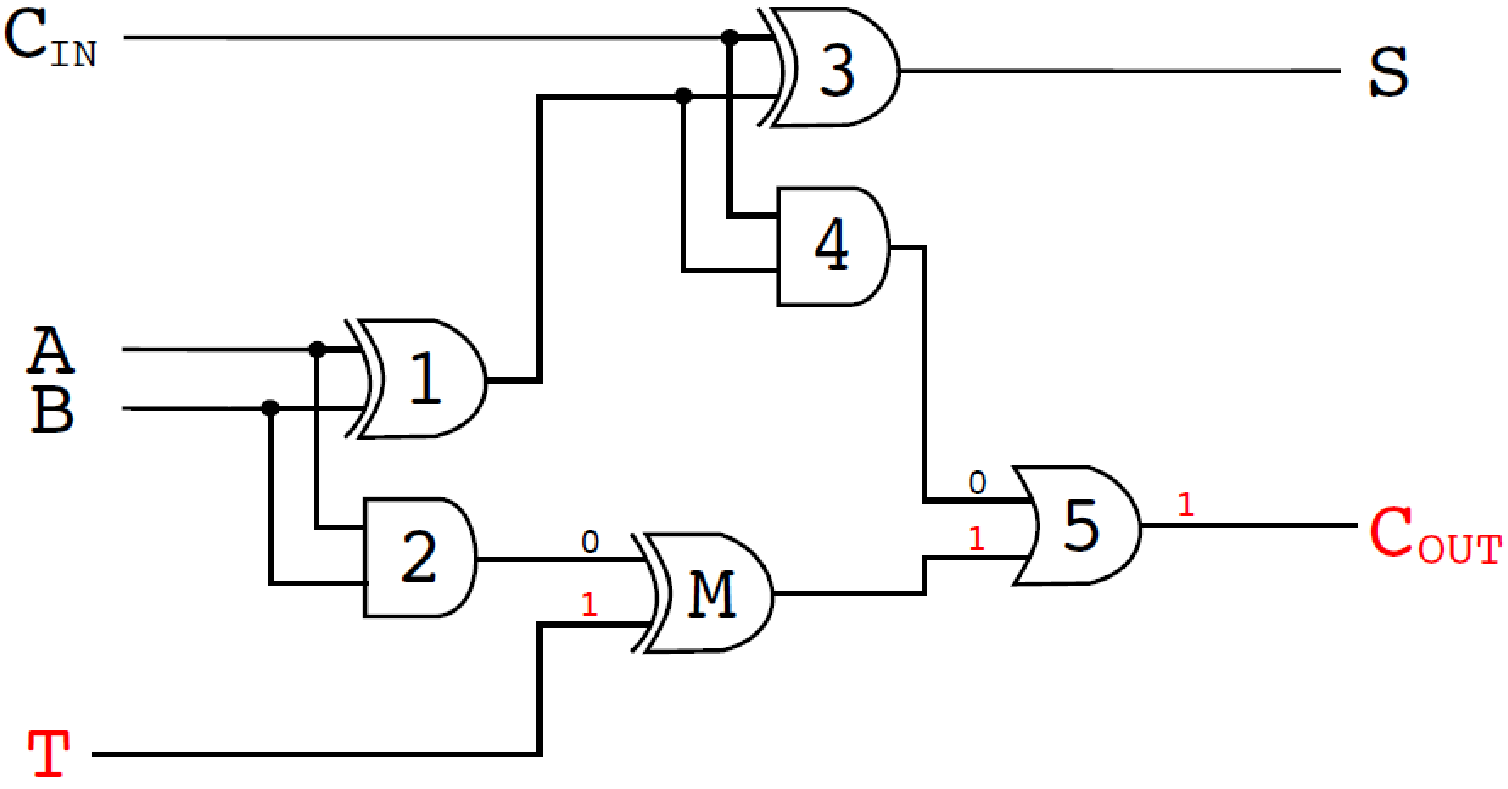
News story, May 2012: "Security backdoor found in US military chip made in [foreign country]."

Example

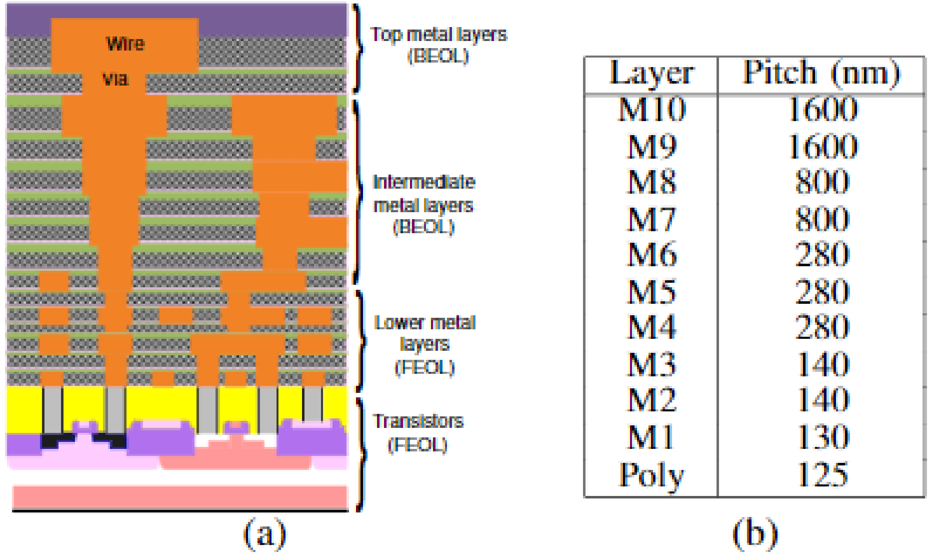


Example

Full Adder Netlist



IC Layers



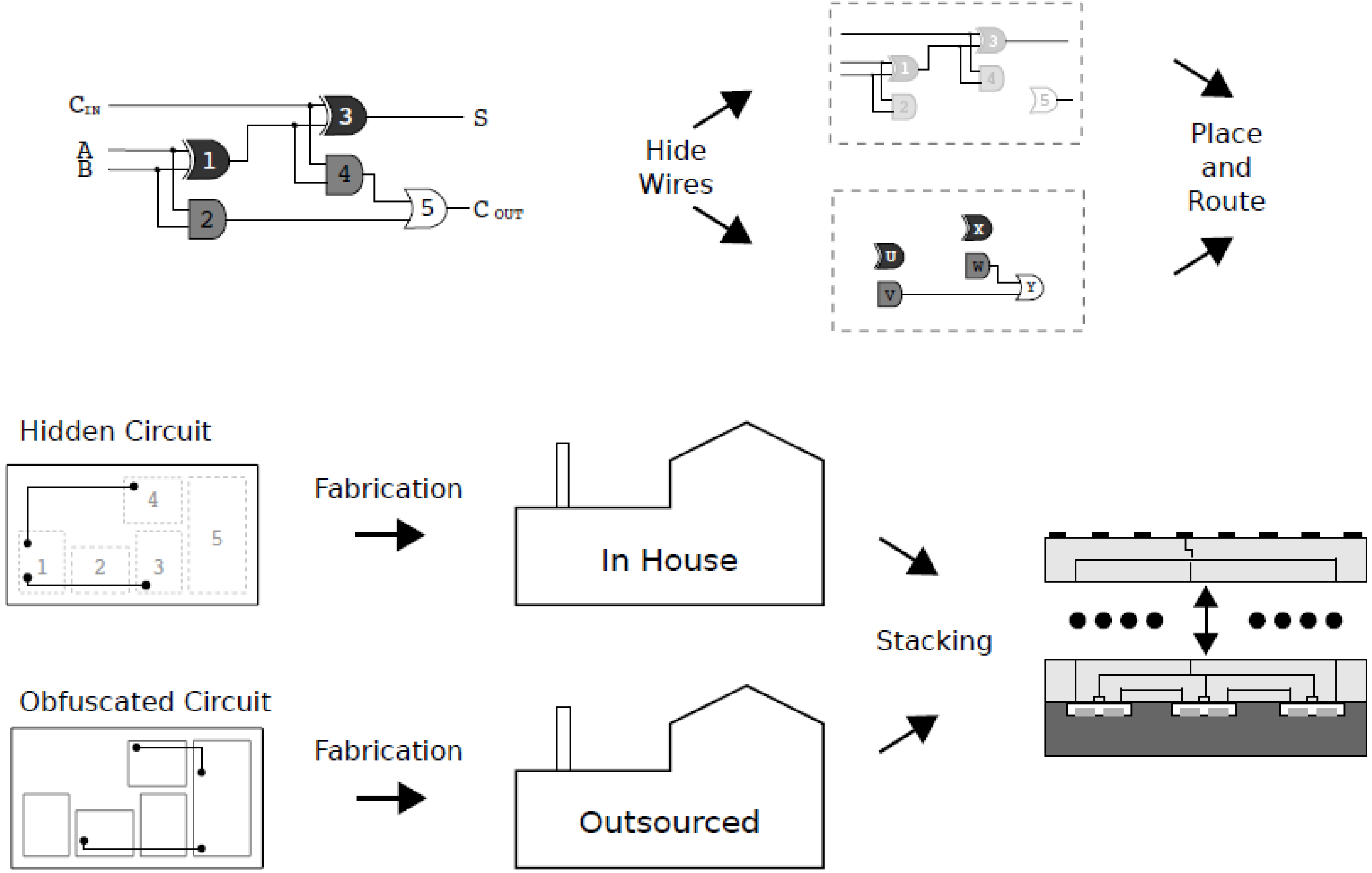
(a)

Layer	Pitch (nm)
M10	1600
M9	1600
M8	800
M7	800
M6	280
M5	280
M4	280
M3	140
M2	140
M1	130
Poly	125

(b)

Fig. 1: (a) A cross-section of an IC layout. The layout has two parts: Front End Of Line or FEOL layers(transistors, lower metal layers) and Back End Of Line or BEOL layers (intermediate, and top metal layers)[Source: [10]]. (b) Pitch length of different metal layers in 45nm CMOS technology [1].

Split Manufacturing



Hide Wires

Place and Route

Hidden Circuit

Obfuscated Circuit

Fabrication

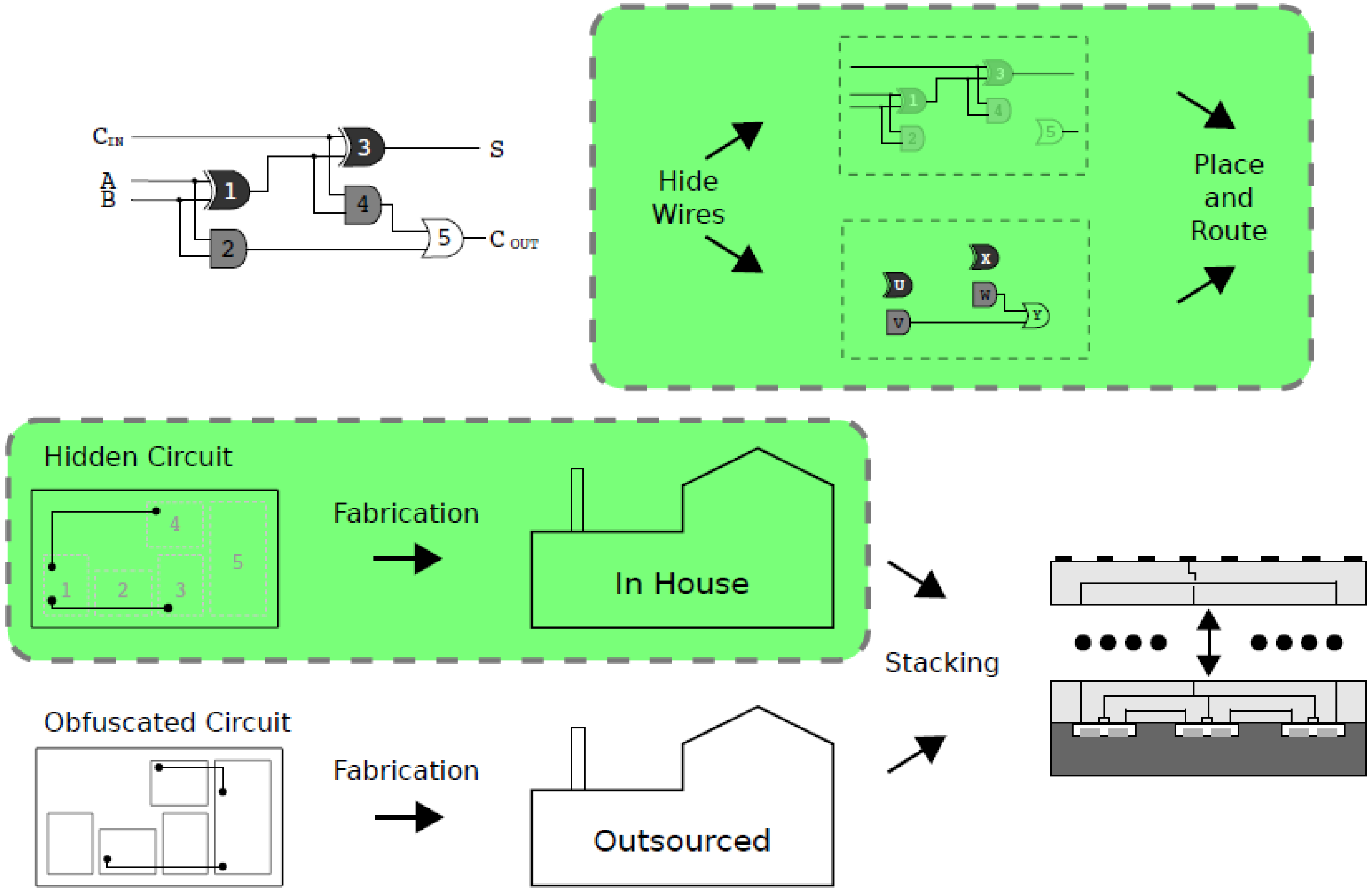
Fabrication

In House

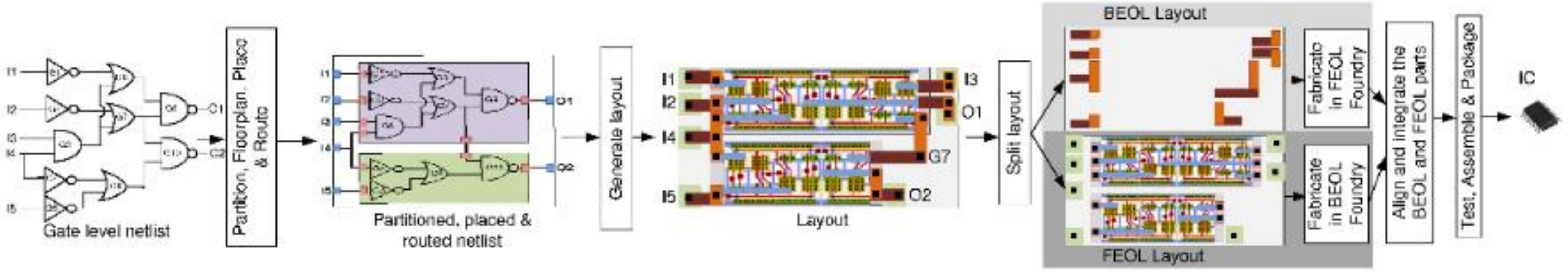
Outsourced

Stacking

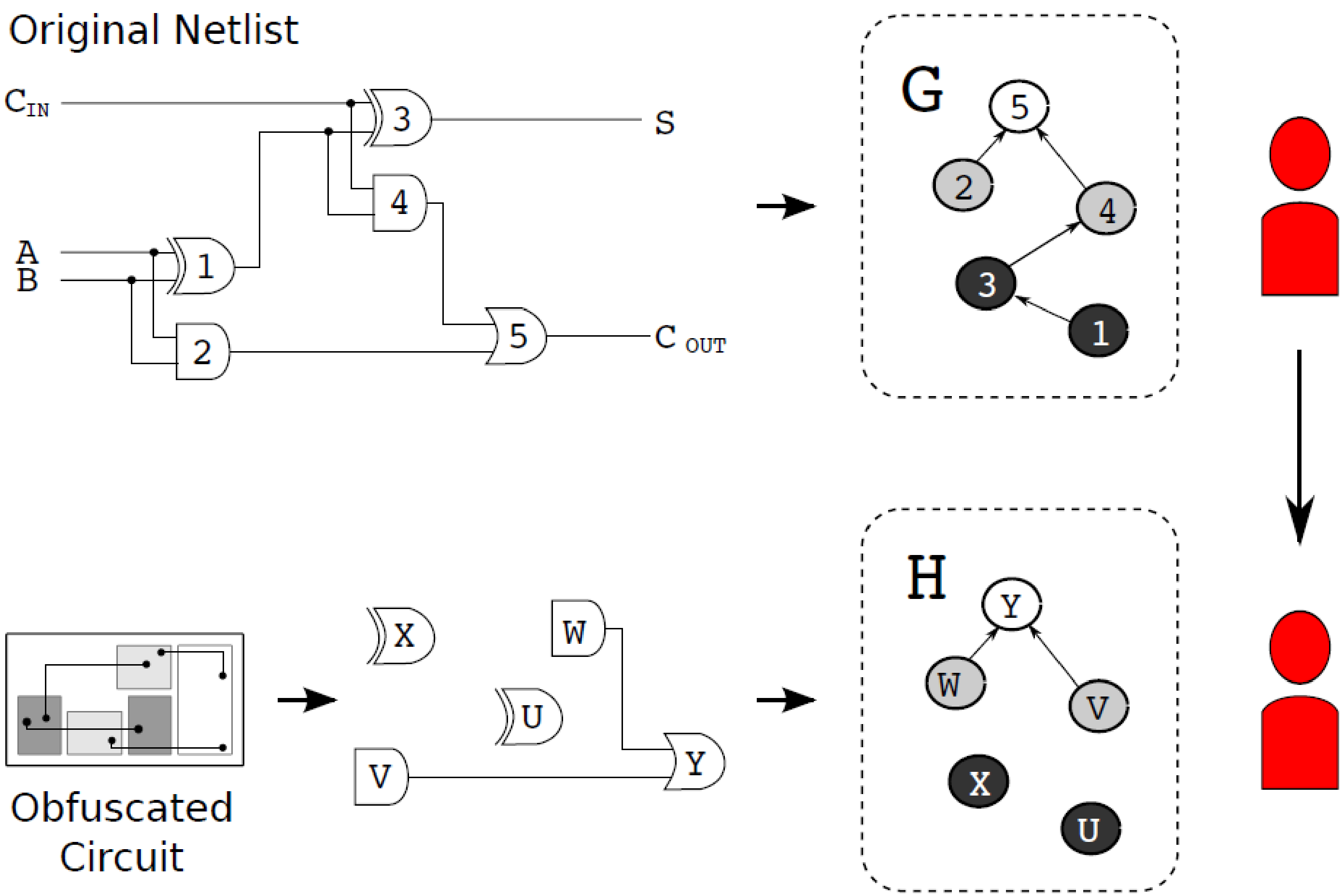
Split Manufacturing



Split Manufacturing Flow


I1
I2
I3
I4
I5
O1
O2
Gate level netlist
Partition, Floorplan, Place & Route
Partitioned, placed & routed netlist
Generate layout
I1
I2
I4
I5
I3
O1
G7
O2
Layout
Split layout
BEOL Layout
FEOL Layout
Fabricate in FEOL Foundry
Fabricate in BEOL Foundry
Align and integrate the BEOL and FEOL parts
Test, Assemble & Package
IC

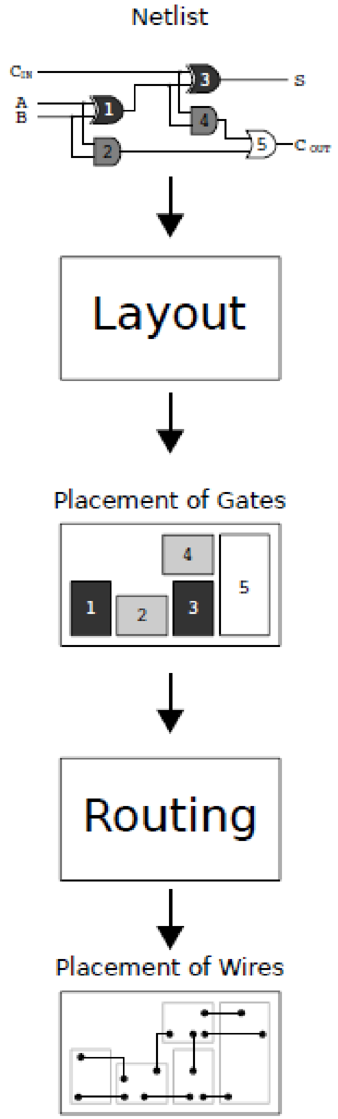
Attack Summary



Original Netlist

Obfuscated Circuit

Layout Randomization



Netlist

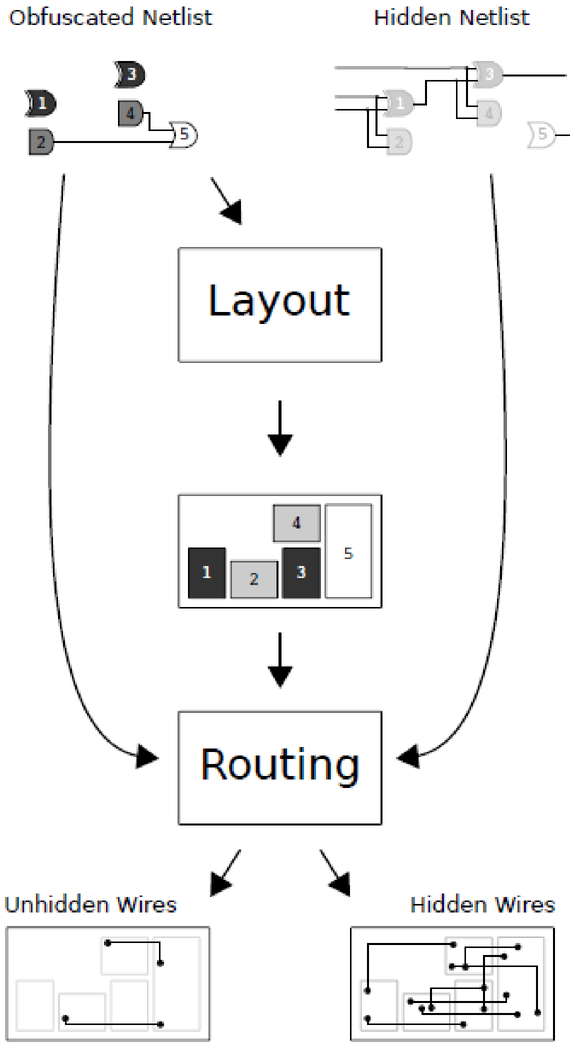
Layout

Placement of Gates

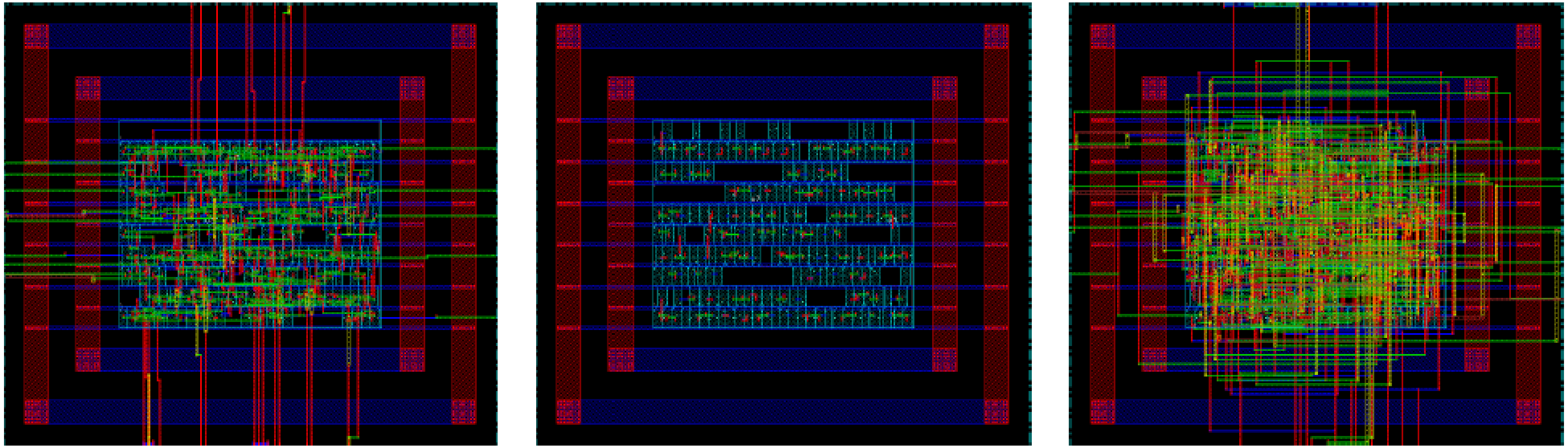
Routing

Placement of Wires

Layout Randomization



Layout and Routing Results



(a) Unsecure Circuit (b) Obfuscated Tier (c) Hidden Tier

Wire Length Distribution

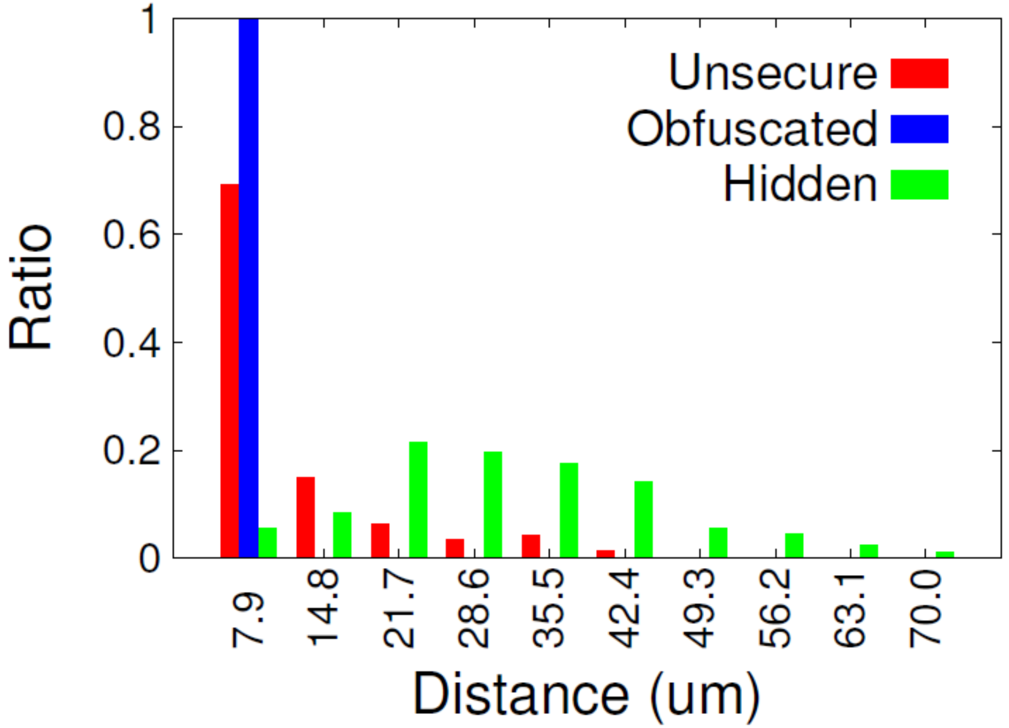


Figure: Comparison of the wire length distribution for the unsecured, obfuscated and hidden circuits. Also the hidden wire length distribution passes the χ^2 test when compared to a random distribution.

Power and Delay Costs

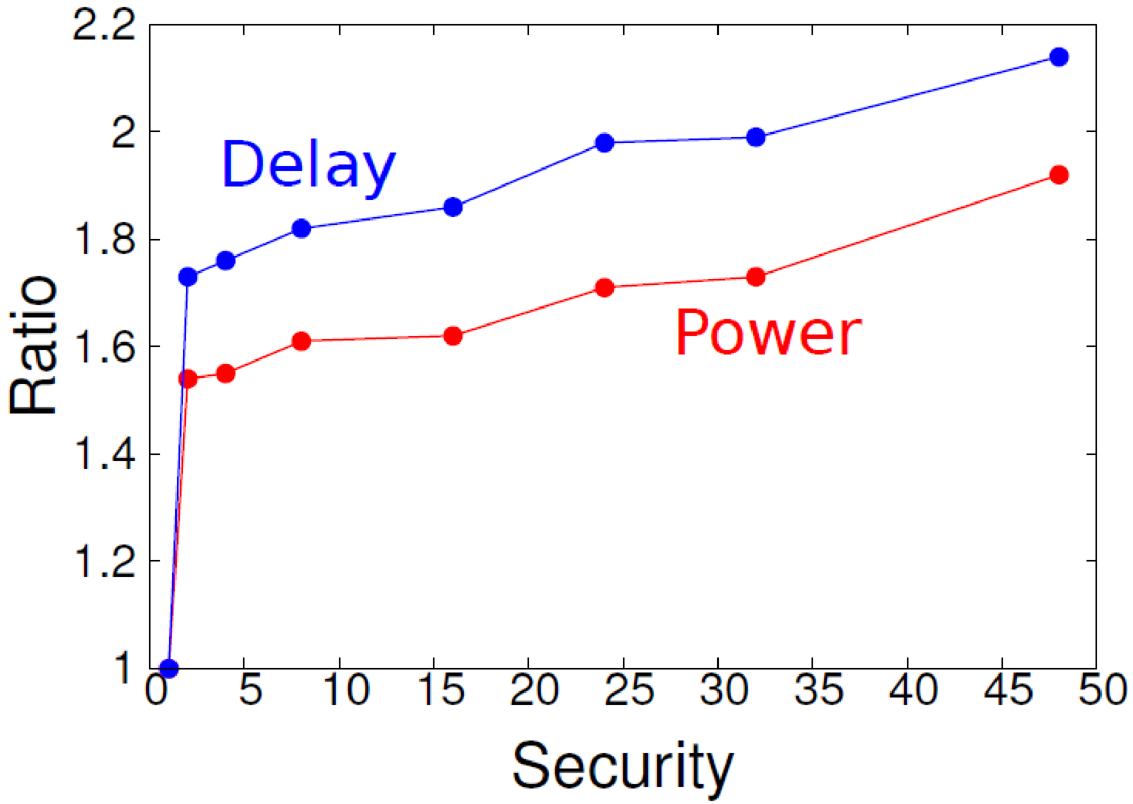


Figure: Power and delay ratio calculated from base/unsecured circuit.

Layout-level Logic Obfuscation

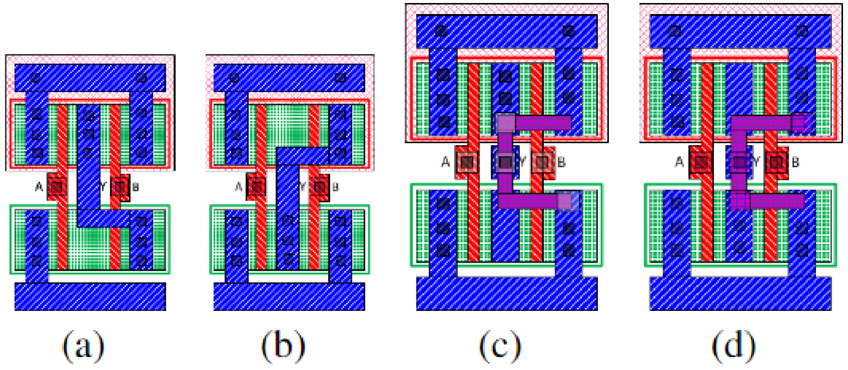
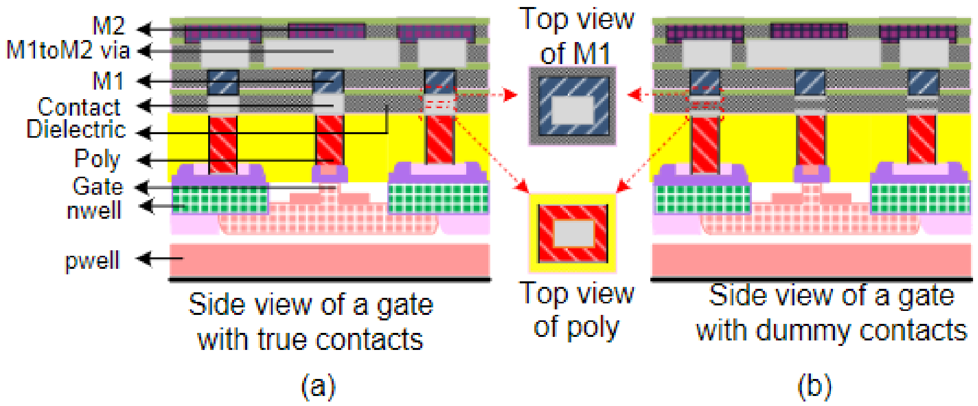
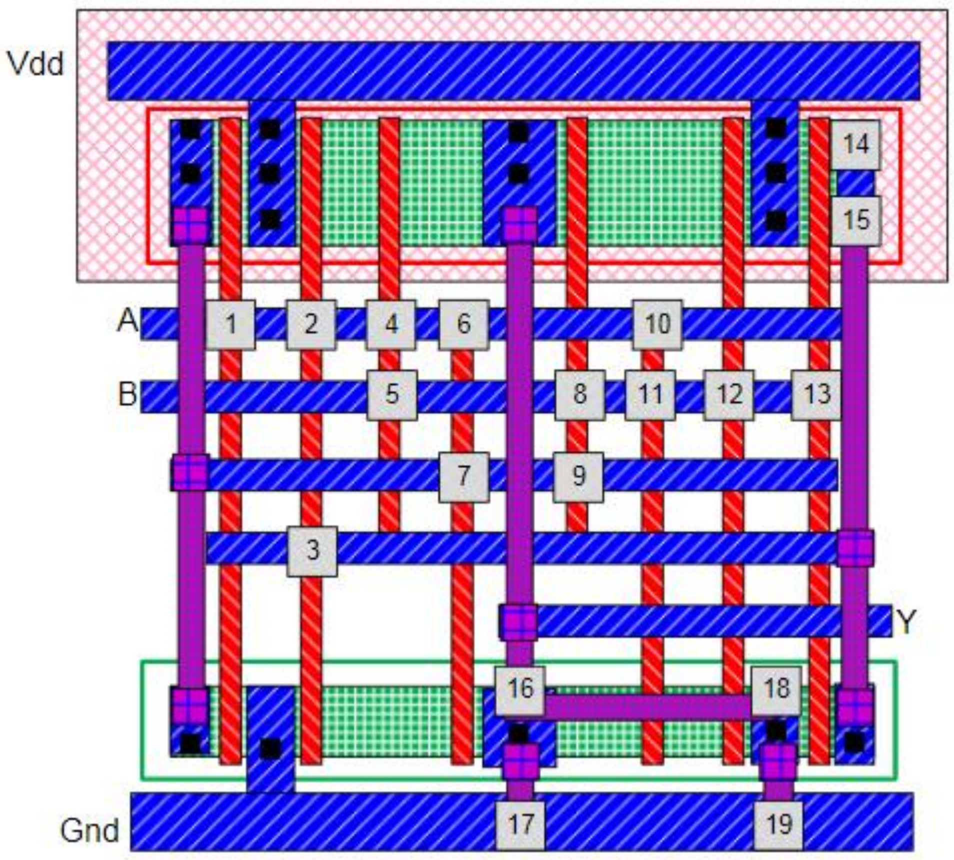


Figure 1: Standard cell layout of regular 2-input (a) NAND and (b) NOR gates. The metal layers are different and hence it is easy to differentiate them by just looking at the top metal layer. Camouflaged standard cell layouts of 2-input (c) NAND and (b) NOR gates. The metal layers are identical and hence it is difficult to differentiate them by just looking at the top metal layer.



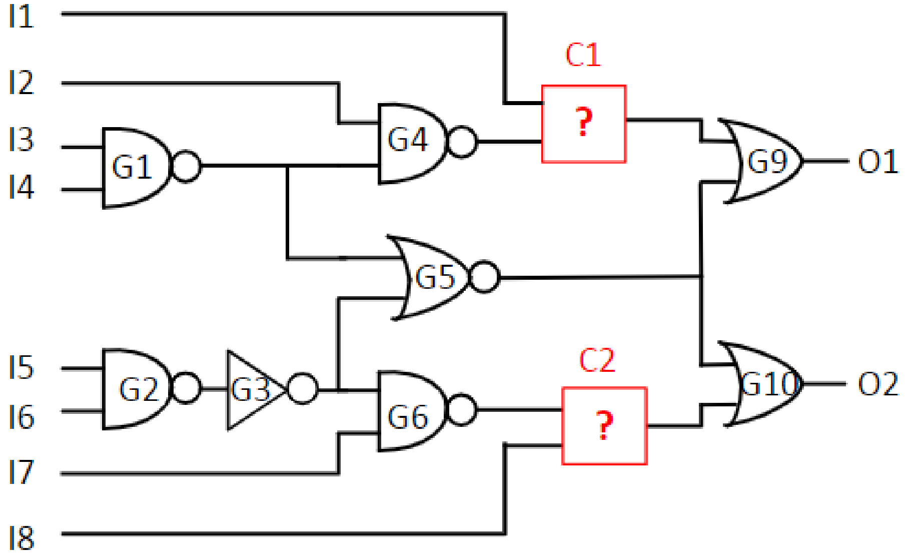
Obfuscated Layout

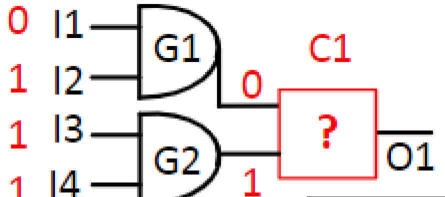


Function	Contacts	
	True	Dummy
NAND	2, 4, 6, 8, 11, 12, 16, 17	1, 3, 5, 7, 9, 10, 13, 14, 15, 18, 19
NOR	2, 5, 6, 11, 12, 18, 19	1, 3, 4, 7, 8, 9, 10, 13, 14, 15, 16, 17
XOR	1, 3, 4, 7, 9, 10, 12, 13, 14, 15, 18, 19	2, 5, 6, 8, 11, 16, 17

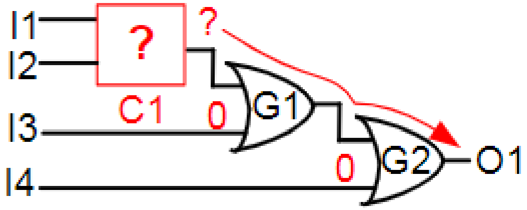
Achieved Functions

Obfuscated Circuits

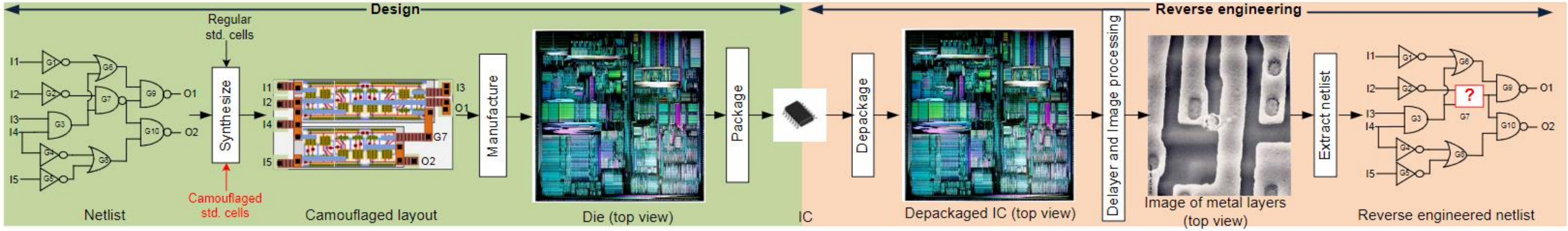




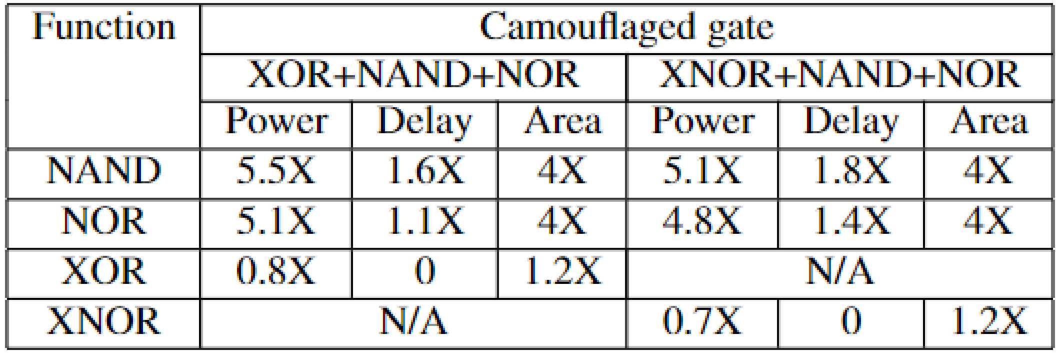
XOR	1
NAND	1
NOR	0



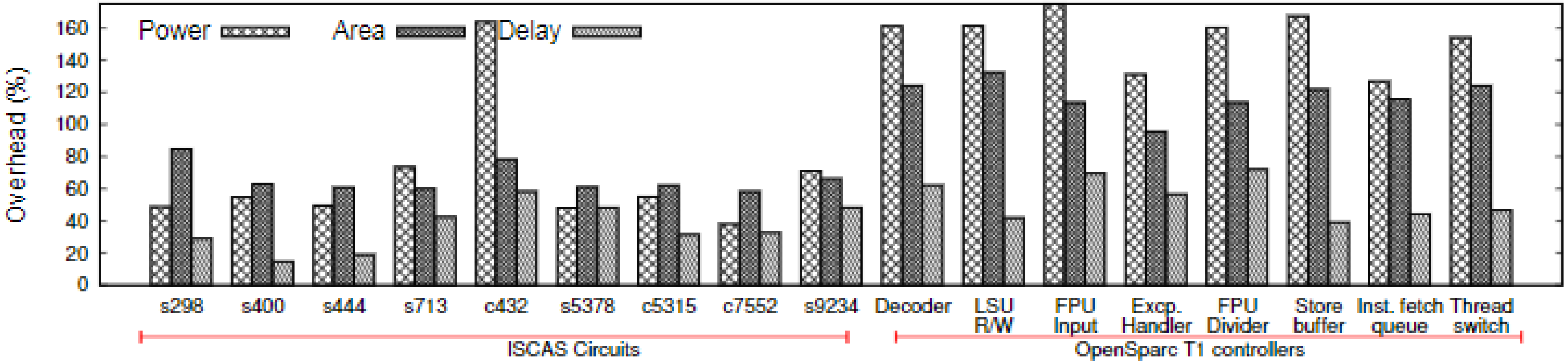
Logic Obfuscation Flow



Results



Function	Camouflaged gate					
	XOR+NAND+NOR			XNOR+NAND+NOR		
	Power	Delay	Area	Power	Delay	Area
NAND	5.5X	1.6X	4X	5.1X	1.8X	4X
NOR	5.1X	1.1X	4X	4.8X	1.4X	4X
XOR	0.8X	0	1.2X	N/A		
XNOR	N/A			0.7X	0	1.2X


Power
Area
Delay
Overhead (%)
s298
s400
s444
s713
c432
s5378
c5315
c7552
s9234
Decoder
LSU R/W
FPU Input
Excp. Handler
FPU Divider
Store buffer
Inst. fetch queue
Thread switch
ISCAS Circuits
OpenSparc T1 controllers