Securing Computer Hardware Using 3D Integrated Circuit (IC) Technology and Split Manufacturing for Obfuscation

Frank Imeson

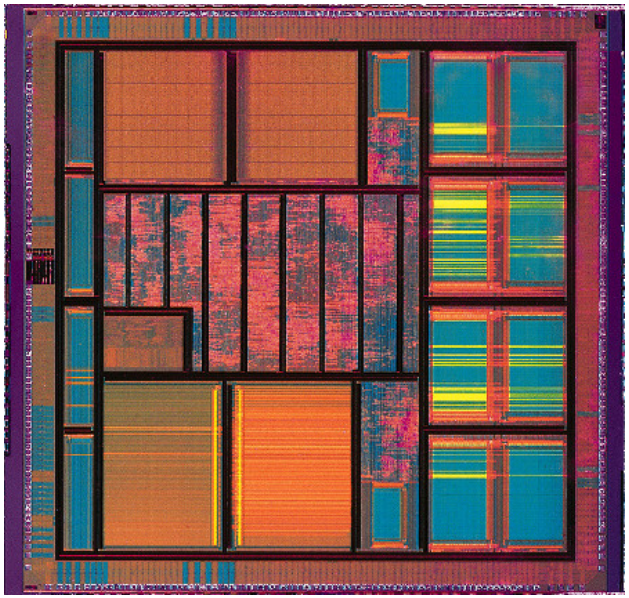
ECE, University of Waterloo

USENIX Security 13

Collaborators: Ariq Emtenan, Siddharth Garg, and Mahesh V. Tripunitara (Waterloo).

Computer Hardware

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

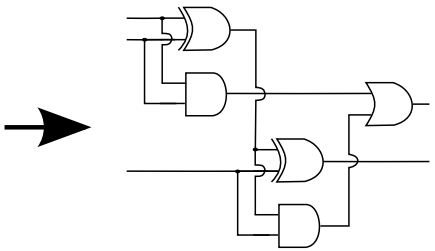


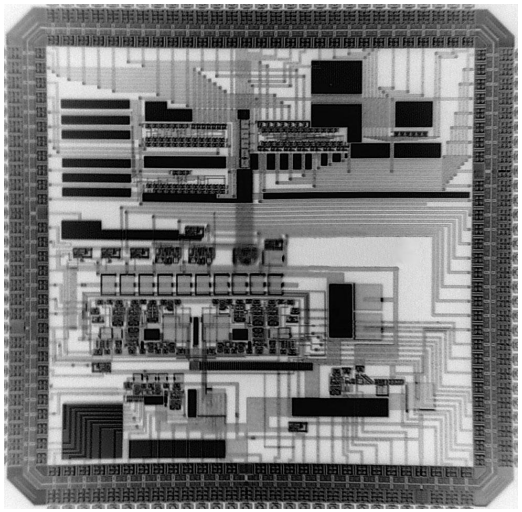
Credit: `http://www.newsplink.com/2009/05/20/the-silicon-valley-trail/`

Manufacturing Process

HDL **Netlist** **IC**

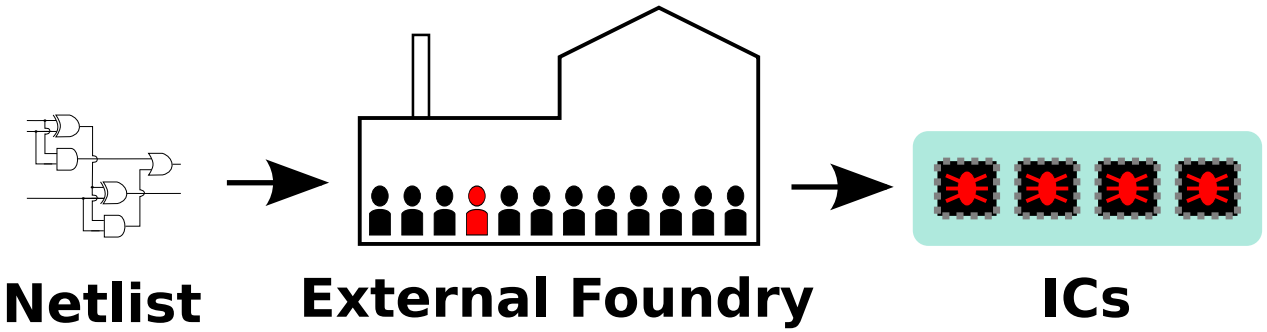
```
case(display_state)
 UPDATE : begin
  seg00_reg <= seg00;
  seg01_reg <= seg01;

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

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





Credit: www.theverge.com/2011/11/16/2565638/mit-neural-connectivity-silicon-synapse

Threat Model

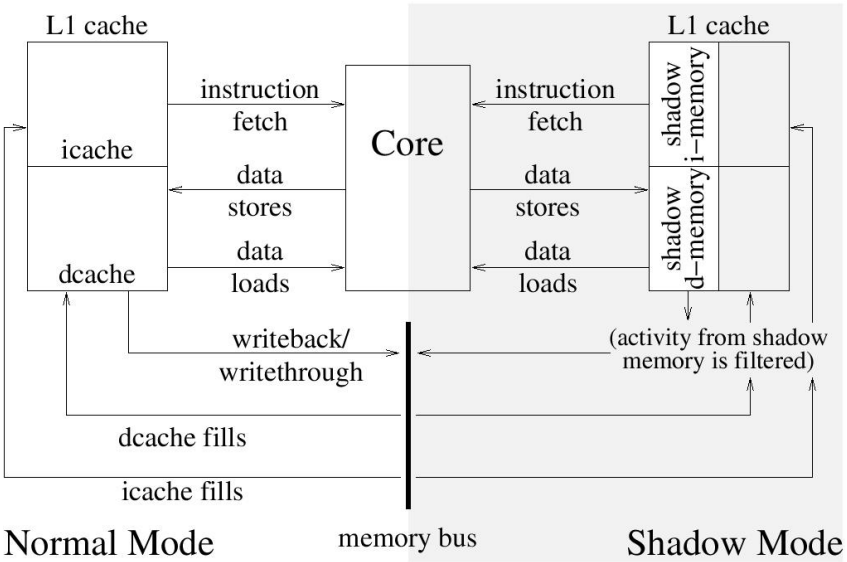


News story, May 2012: "Security backdoor found in US military chip made in [foreign country]."

Attack Types

Examples:

- Privilege escalation [King et al., LEET'08]
- Leaking private information [Skorobogatov et al., CHES 2012]



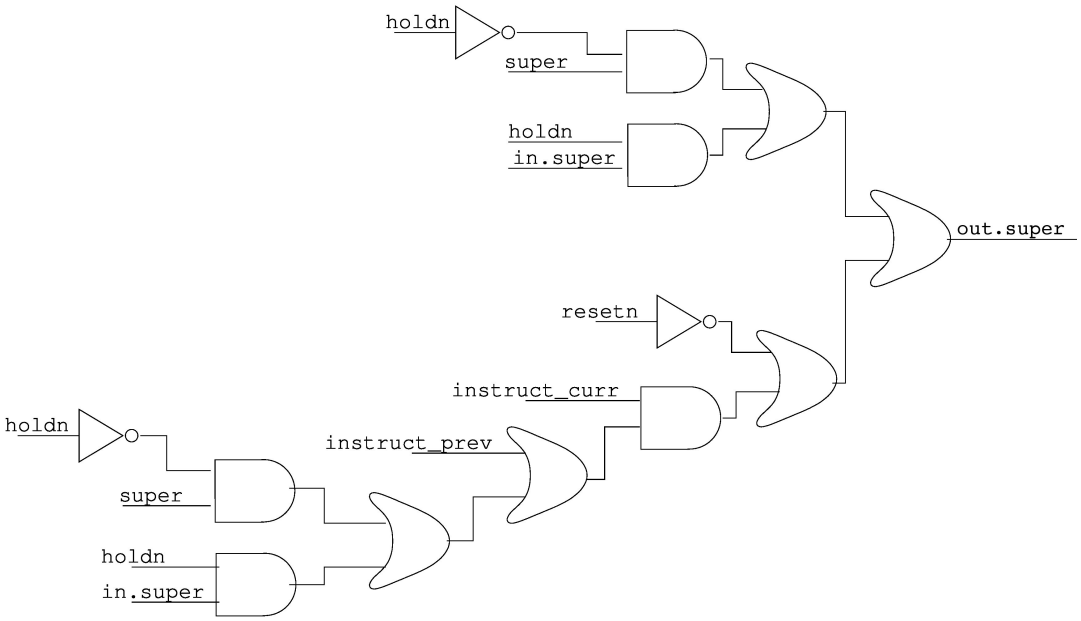
Credit: King et al., LEET'08

Premise

Successful Attack

$\Downarrow$

Uniquely identify at least one gate



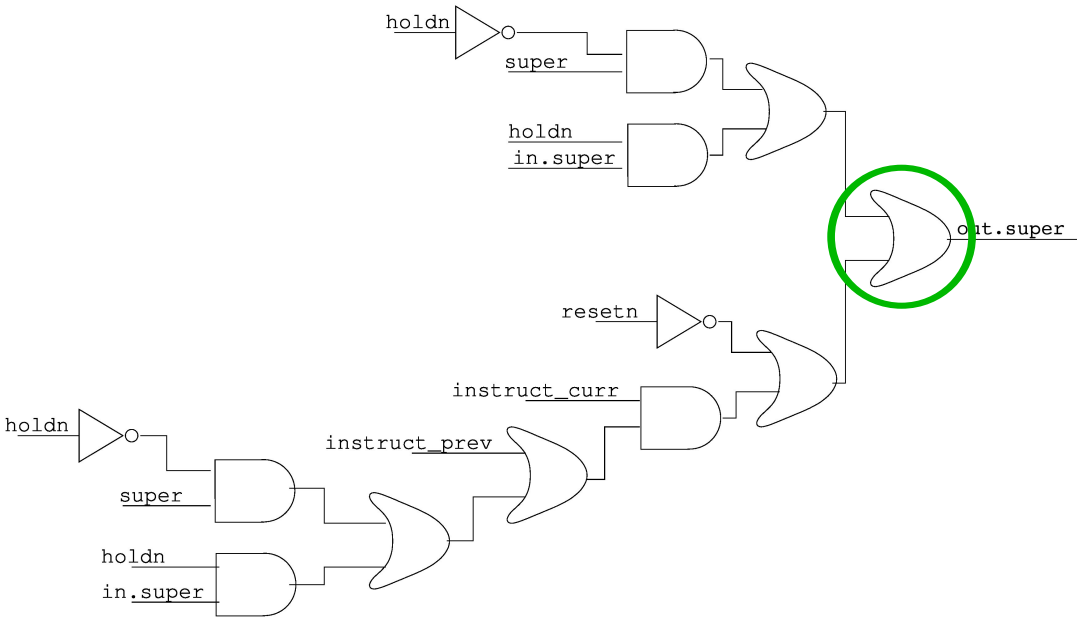
Credit: Cynthia Sturton, Matthew Hicks, David Wagner, and Samuel T. King. "Defeating UCI: Building stealthy and malicious hardware." In Security and Privacy (SP), 2011 IEEE Symposium on, pp. 64-77. IEEE, 2011.

Premise

Successful Attack

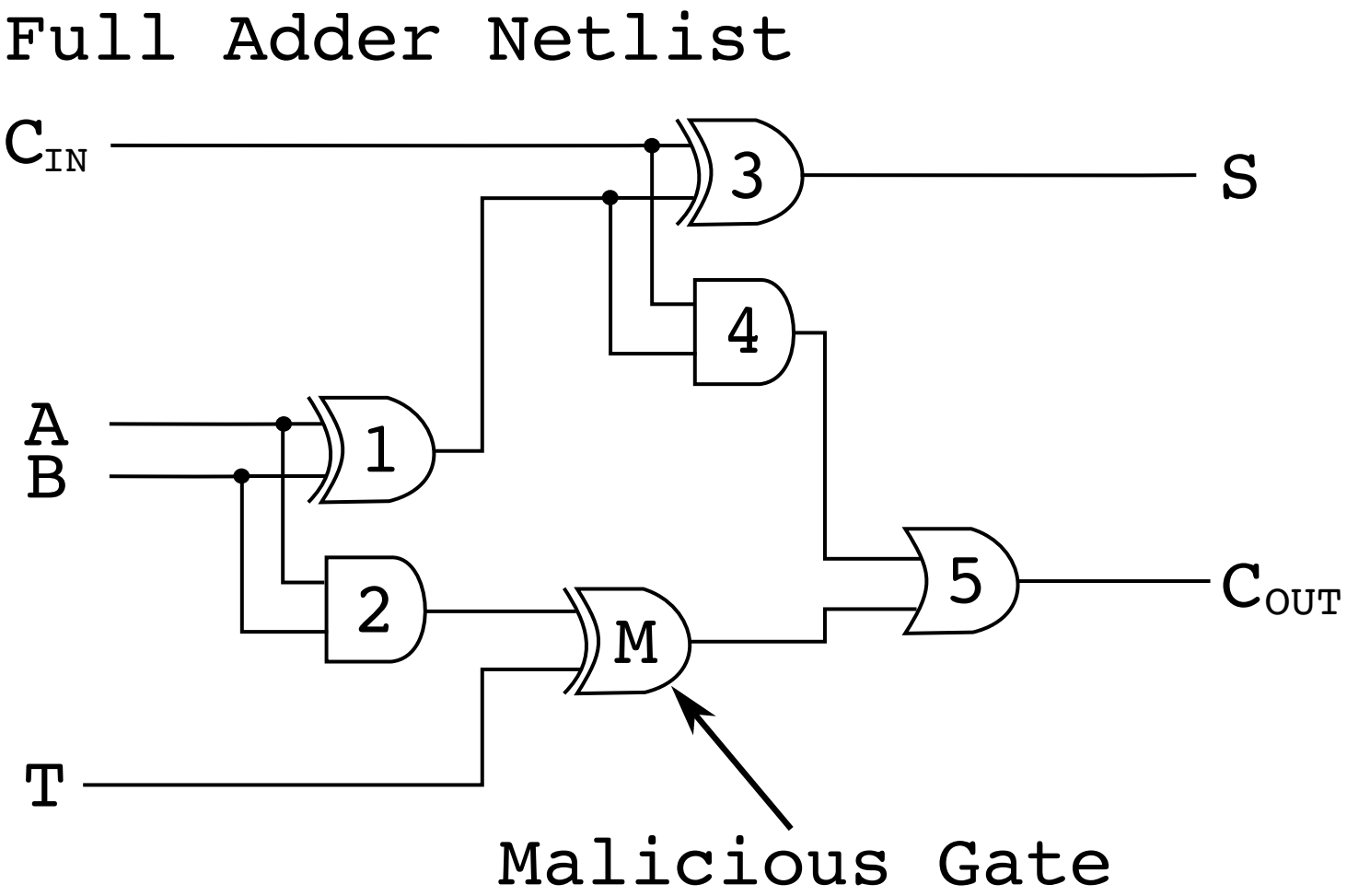
$\Downarrow$

Uniquely identify at least one gate

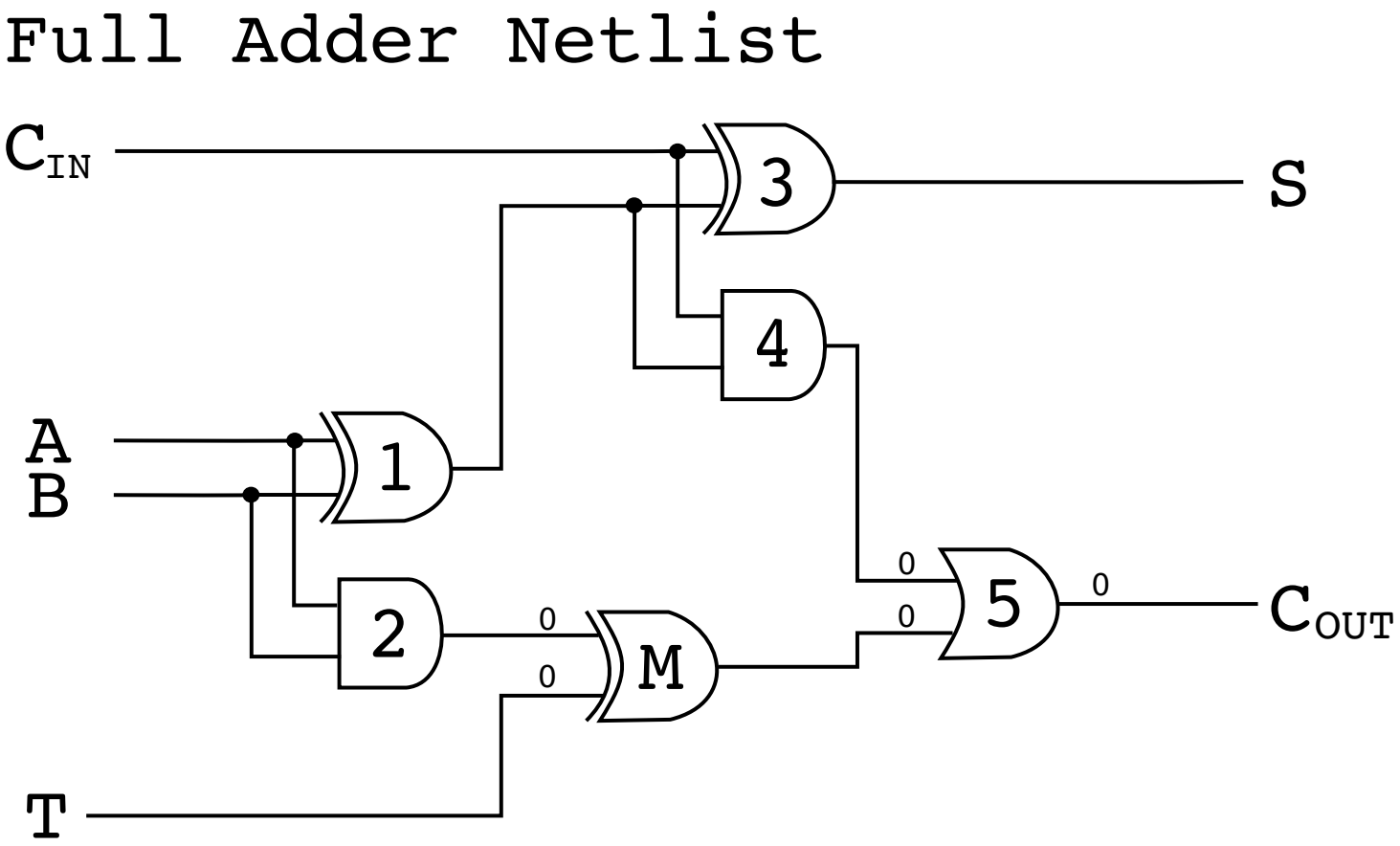


Credit: Cynthia Sturton, Matthew Hicks, David Wagner, and Samuel T. King. "Defeating UCI: Building stealthy and malicious hardware." In Security and Privacy (SP), 2011 IEEE Symposium on, pp. 64-77. IEEE, 2011.

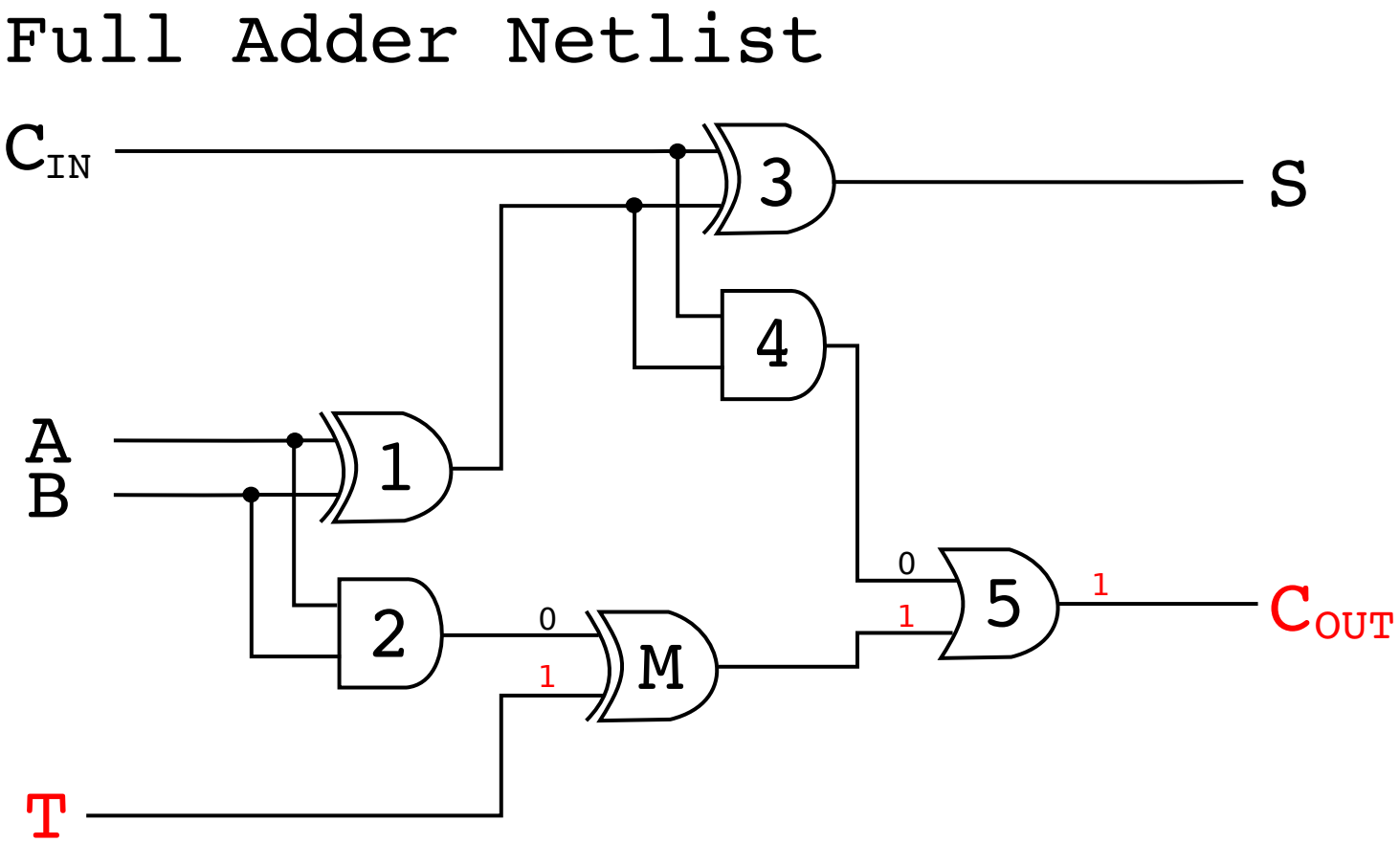
Example



Example

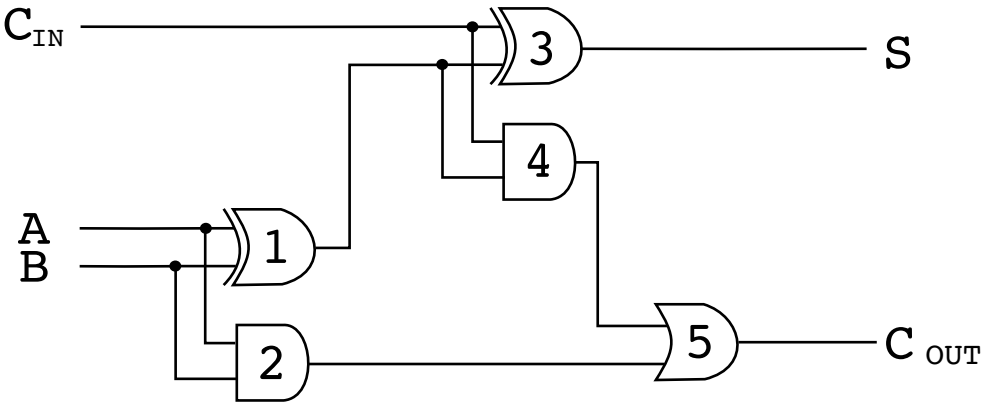


Example

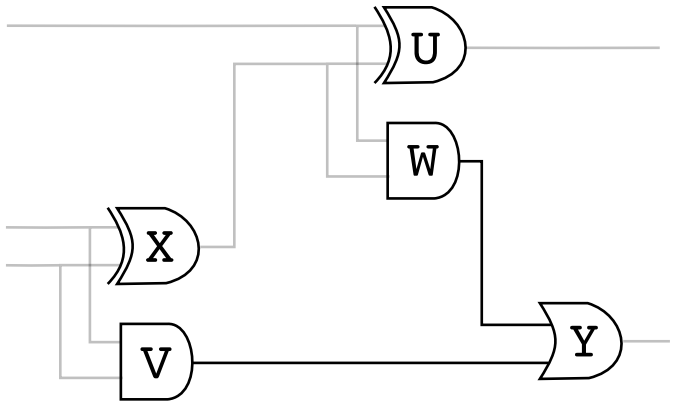


Our Solution – Circuit Obfuscation

Full Adder Netlist

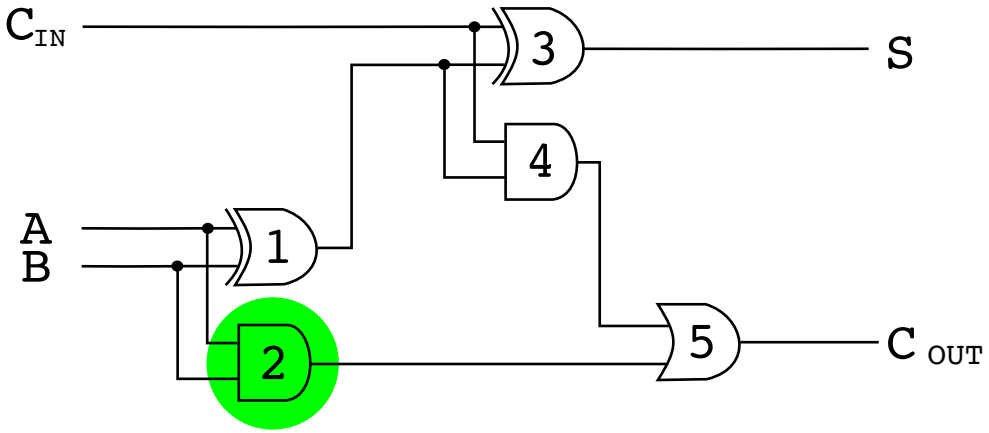


Obfuscated Netlist

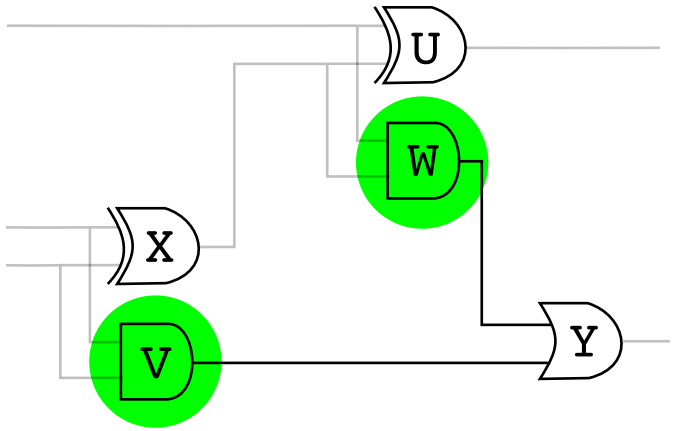


Our Solution – Circuit Obfuscation

Full Adder Netlist

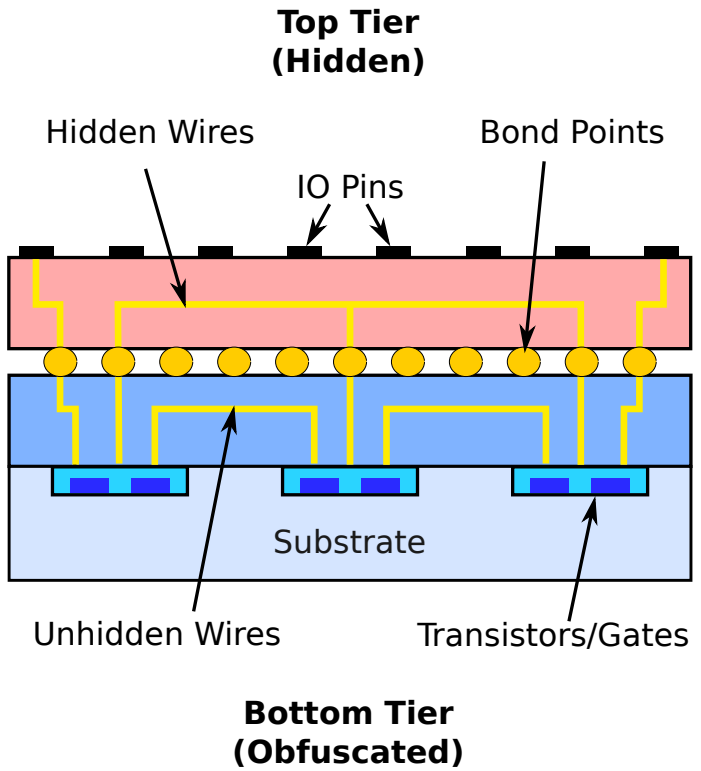


Obfuscated Netlist



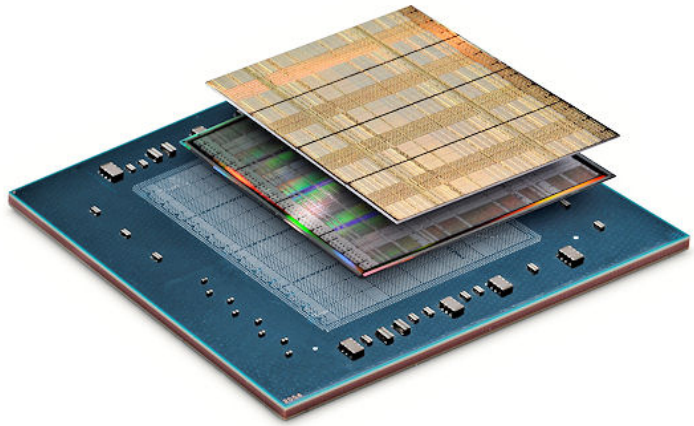
3D IC Technology

- Two or more tiers
- Tiers are connected via bond points
- Wire only tiers are relatively inexpensive



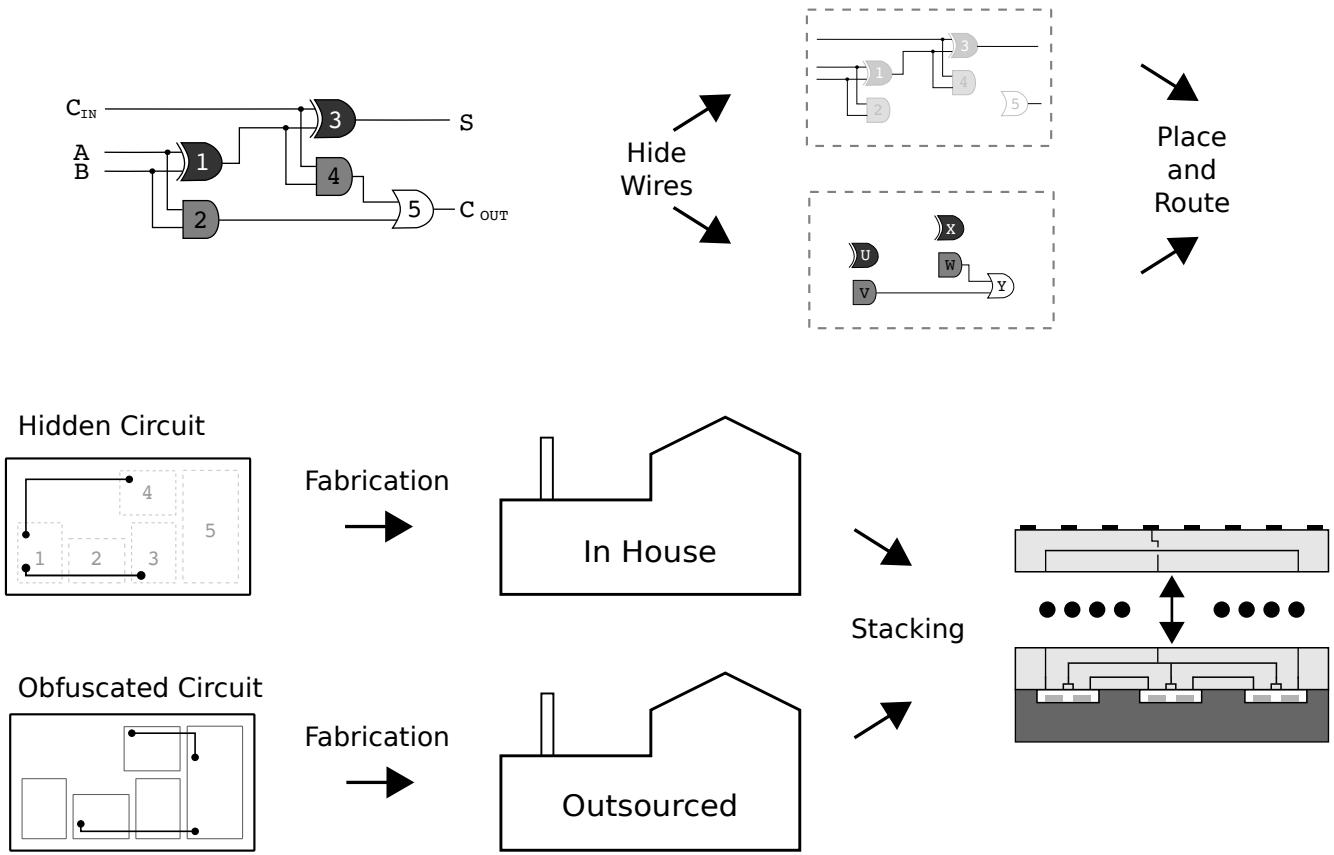
3D Xilinx FPGA

- 6.8 billion transistors
- 1,954,560 logic cells
- 21.55 Mbits of SRAM
- 46,512 Kbits of RAM
- 1200 user I/O
- 2.5D

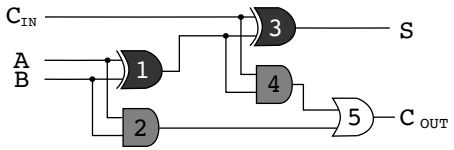


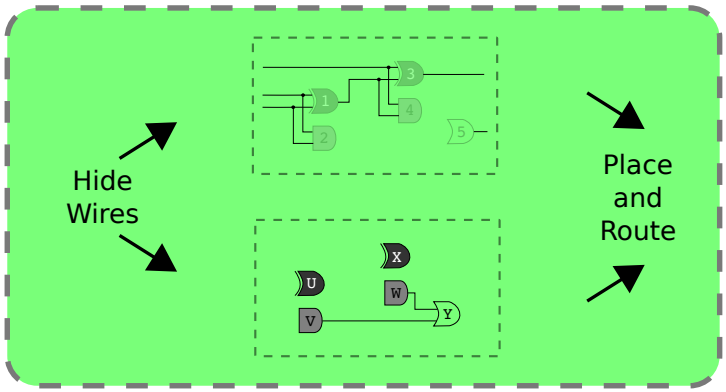
Credit: `http://www.electroiq.com/articles/ap/2011/10/xilinx-fpga-boasts-6-8b-transistors.html`

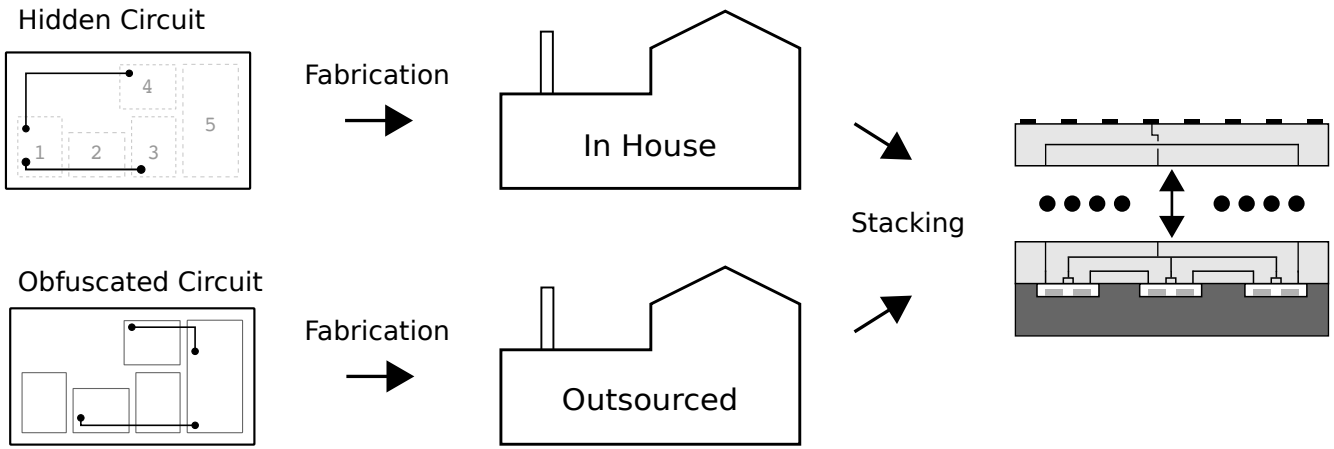
Circuit Obfuscation with 3D Technology



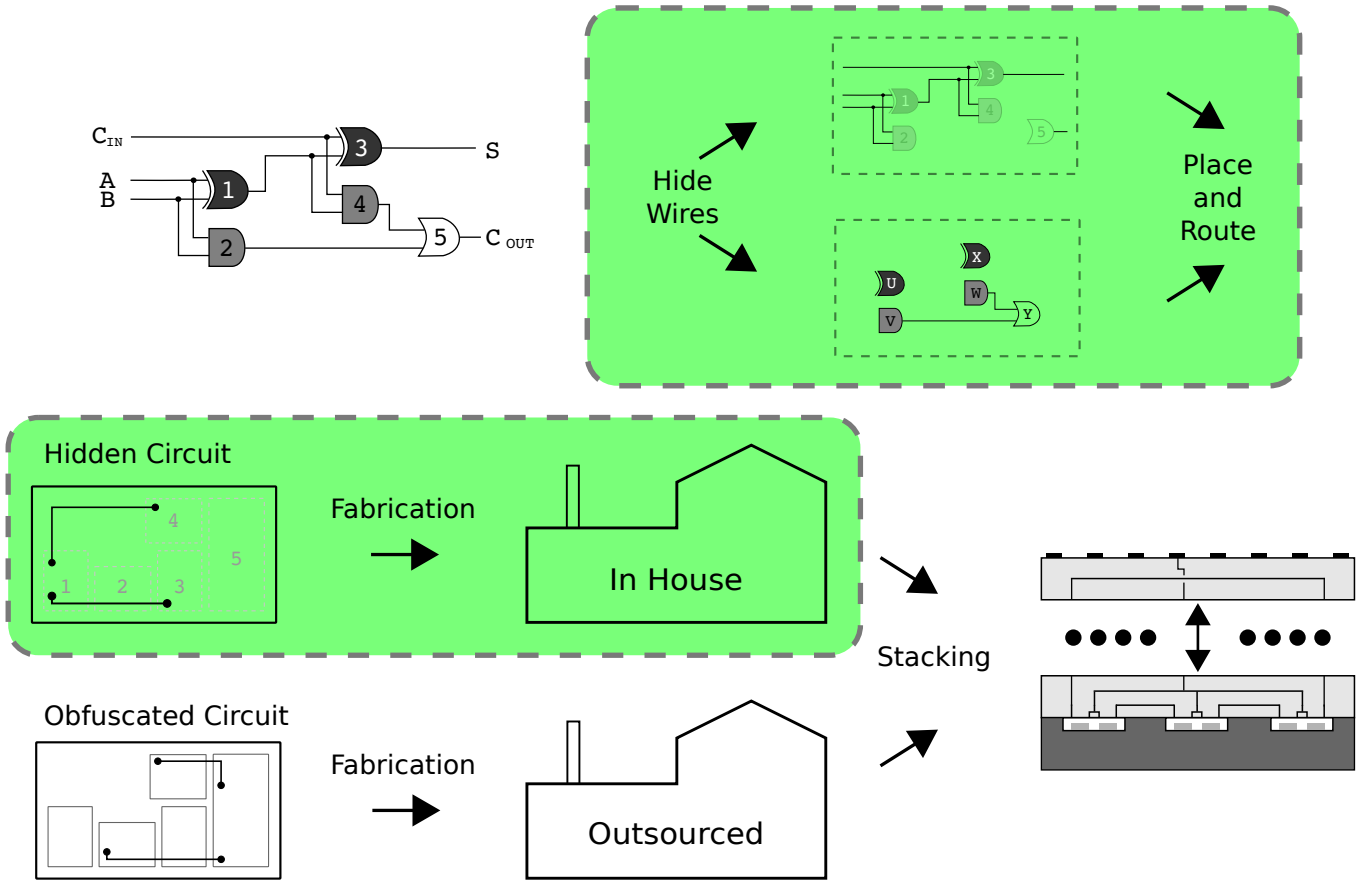
Circuit Obfuscation with 3D Technology



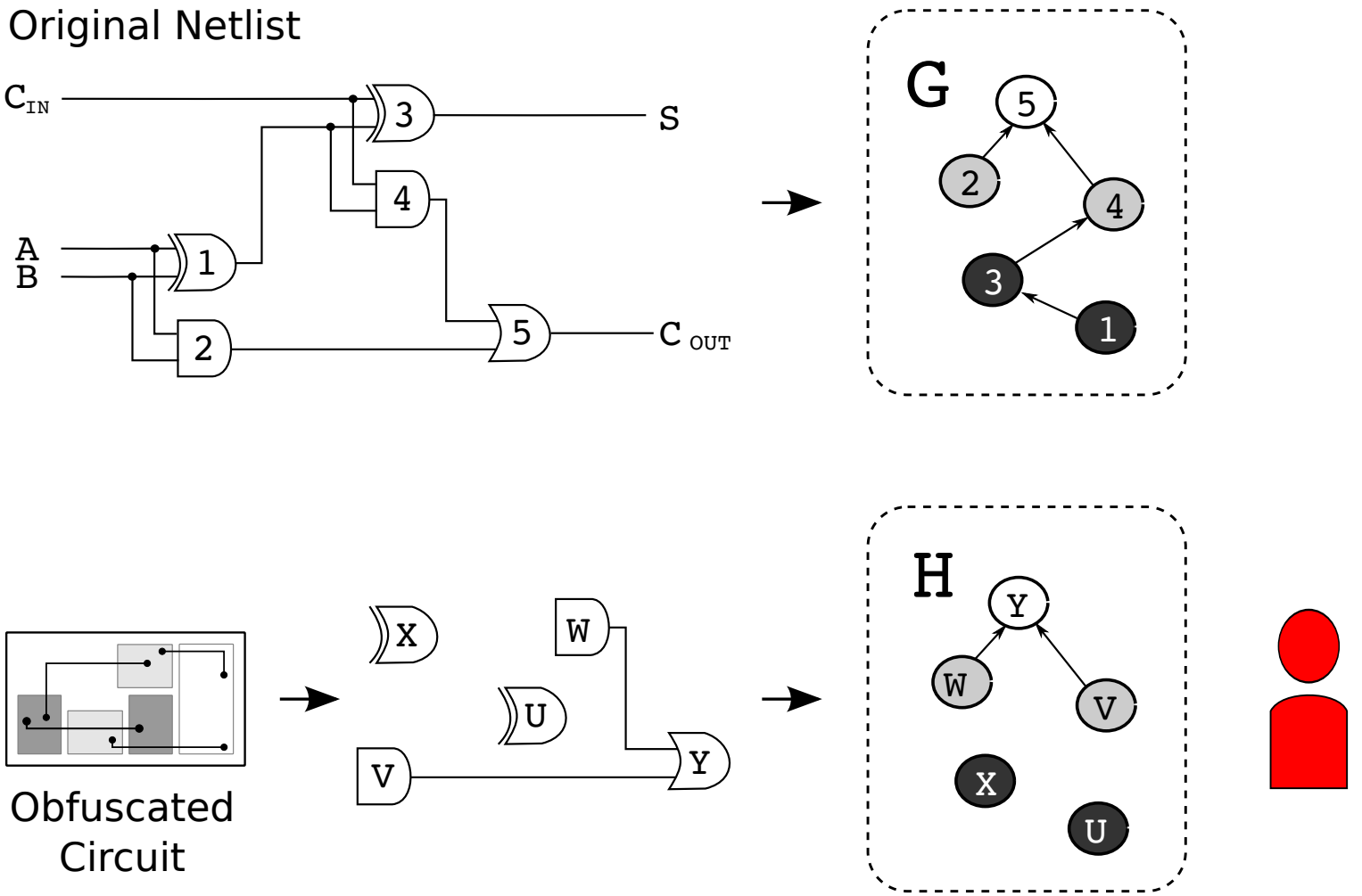




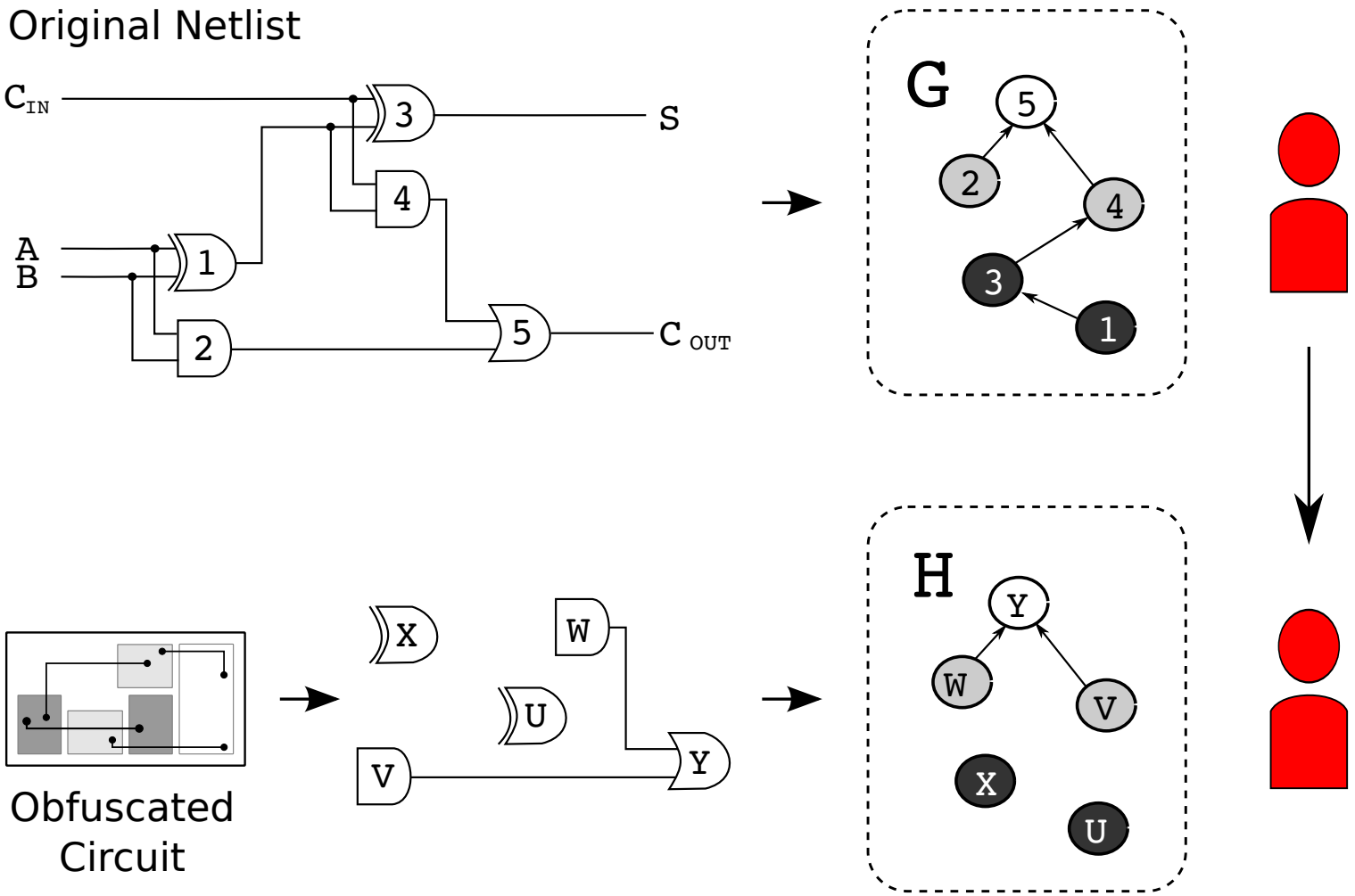
Circuit Obfuscation with 3D Technology



Attack Model Summary

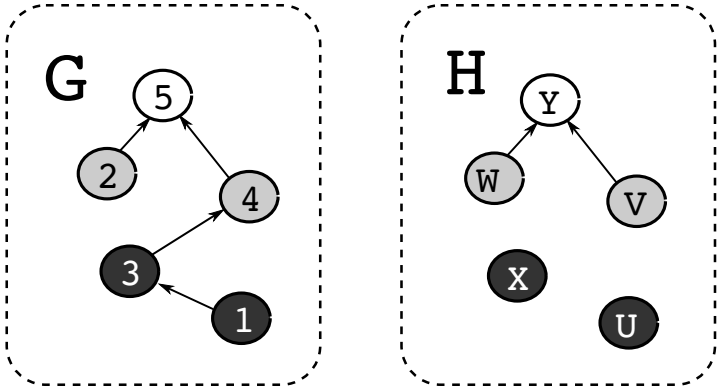


Attack Model Summary



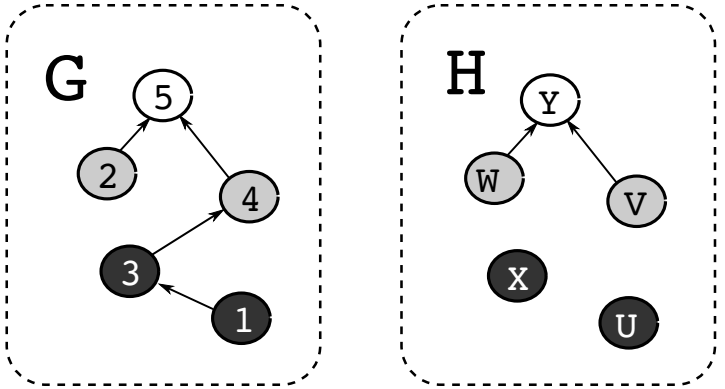
What an Attacker Needs to Do

- Input graphs G and H



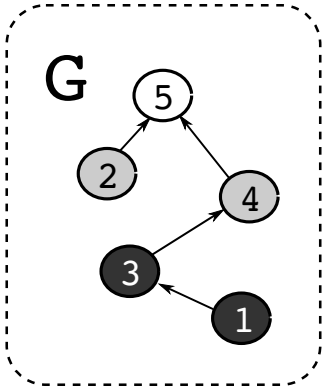
What an Attacker Needs to Do

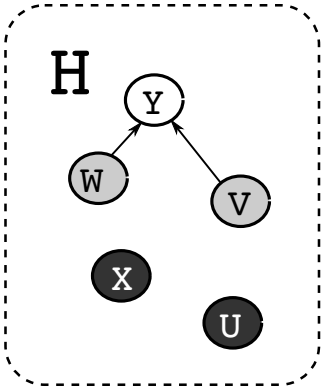
- Input graphs G and H
- Find subgraph isomorphisms

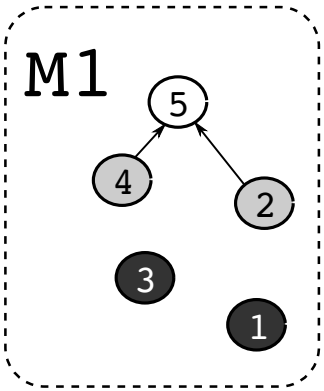


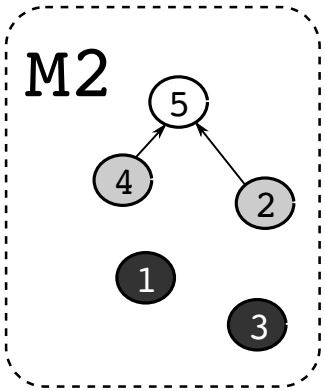
What an Attacker Needs to Do

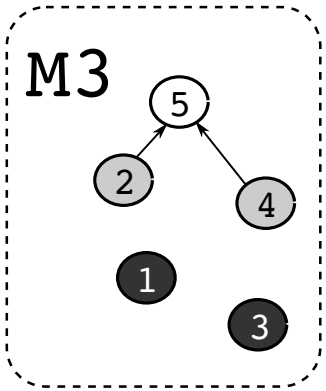
- Input graphs G and H
- Find subgraph isomorphisms

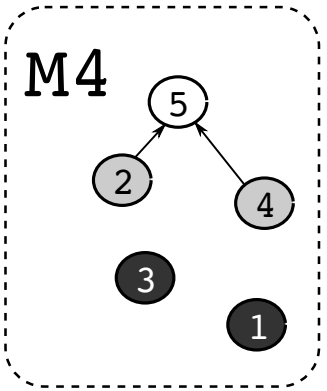






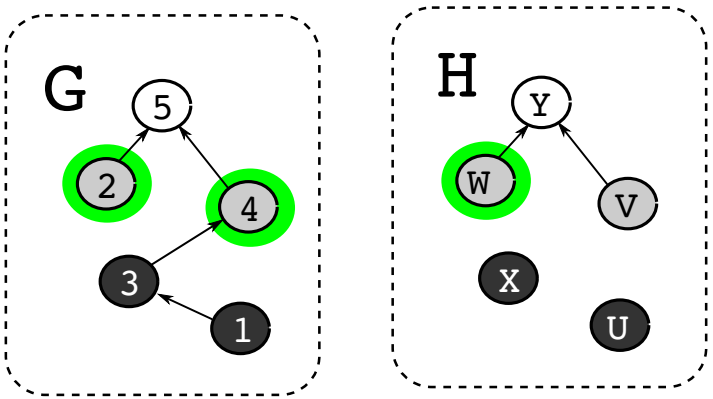






k-Security

- S(w) = 2

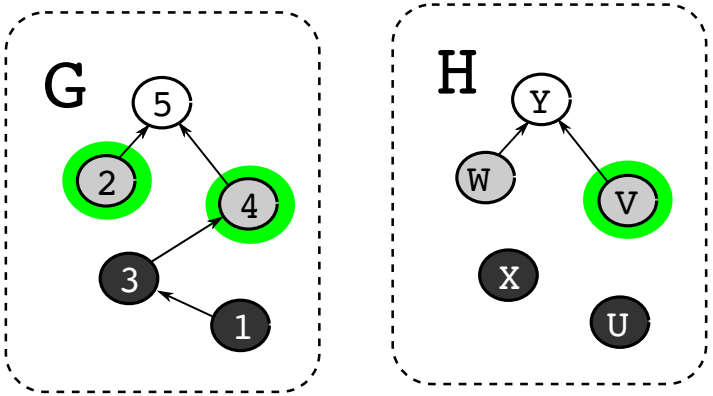


A vertex $v \in H$ is k-secure if there exist at least k subgraph isomorphisms each of which maps v to a distinct vertex in G.

An obfuscated graph (circuit) H is k-secure if every vertex (gate) in H is k-secure.

k-Security

- S(w) = 2
- S(v),S(u),S(x) = 2

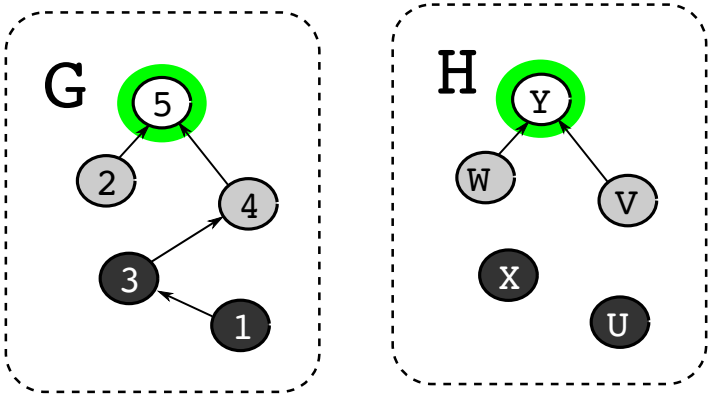


A vertex $v \in H$ is k-secure if there exist at least k subgraph isomorphisms each of which maps v to a distinct vertex in G.

An obfuscated graph (circuit) H is k-secure if every vertex (gate) in H is k-secure.

k-Security

- S(w) = 2
- S(v),S(u),S(x) = 2
- S(y) = 1

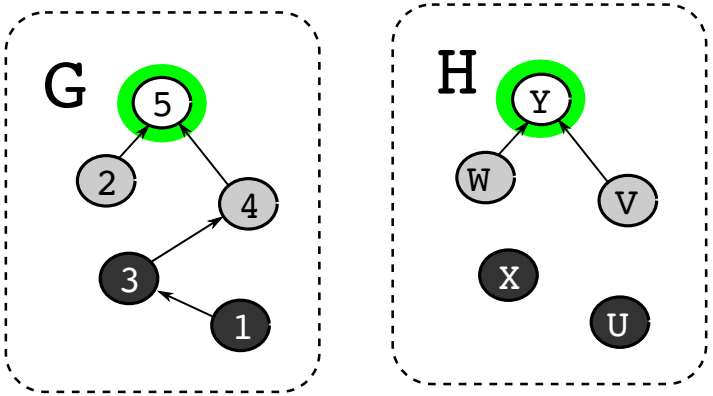


A vertex $v \in H$ is k-secure if there exist at least k subgraph isomorphisms each of which maps v to a distinct vertex in G.

An obfuscated graph (circuit) H is k-secure if every vertex (gate) in H is k-secure.

k-Security

- S(w) = 2
- S(v),S(u),S(x) = 2
- S(y) = 1
- S(H) = 1



A vertex $v \in H$ is k-secure if there exist at least k subgraph isomorphisms each of which maps v to a distinct vertex in G.

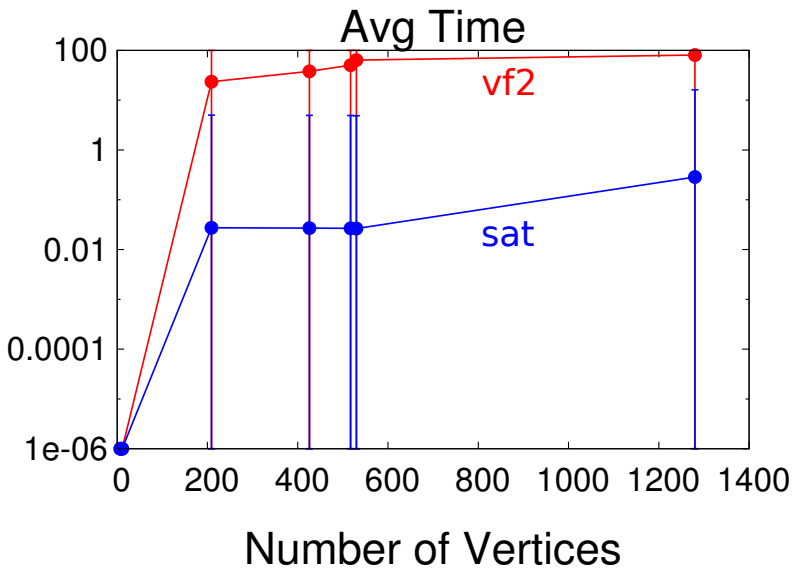
An obfuscated graph (circuit) H is k-secure if every vertex (gate) in H is k-secure.

Computational Complexity

$\langle G, H \rangle$ is k-secure $\in$ **NP**-complete.

We investigated two approaches:

- Reduction to Subgraph Isomorphism and use of VF2 solver
- Reduction to SAT and use of MiniSAT solver



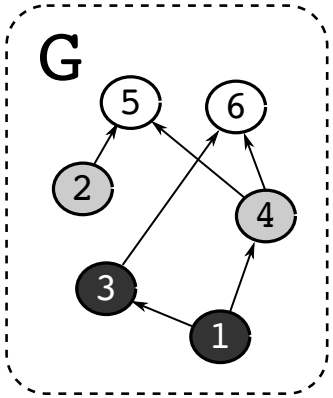
Cost vs. Security

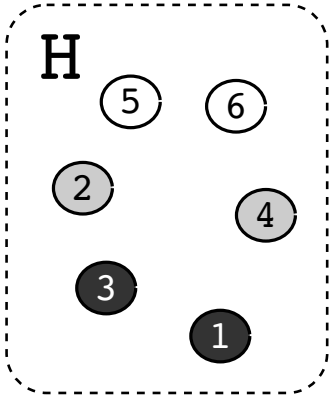
Cost = Number of hidden edges

Goal: Explore Cost vs. Security trade-off

Greedy approach

- Start with no edges in H.





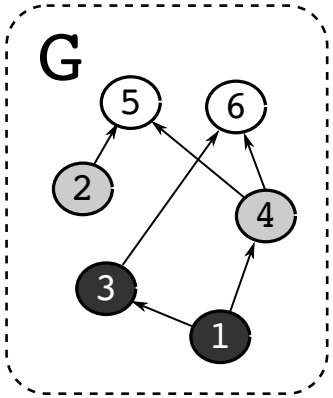
Cost vs. Security

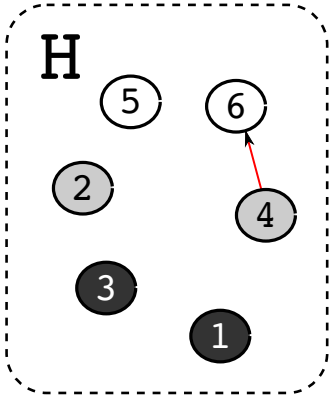
Cost = Number of hidden edges

Goal: Explore Cost vs. Security trade-off

Greedy approach

- Start with no edges in H.
- Greedily pick an edge to add to H that maximizes security.





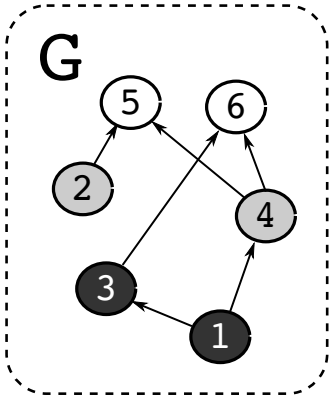
Cost vs. Security

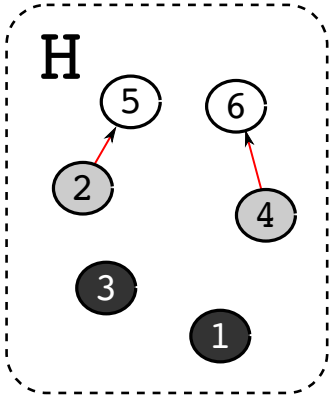
Cost = Number of hidden edges

Goal: Explore Cost vs. Security trade-off

Greedy approach

- Start with no edges in H.
- Greedily pick an edge to add to H that maximizes security.
- Repeat.





Security vs. Number of Removed Edges

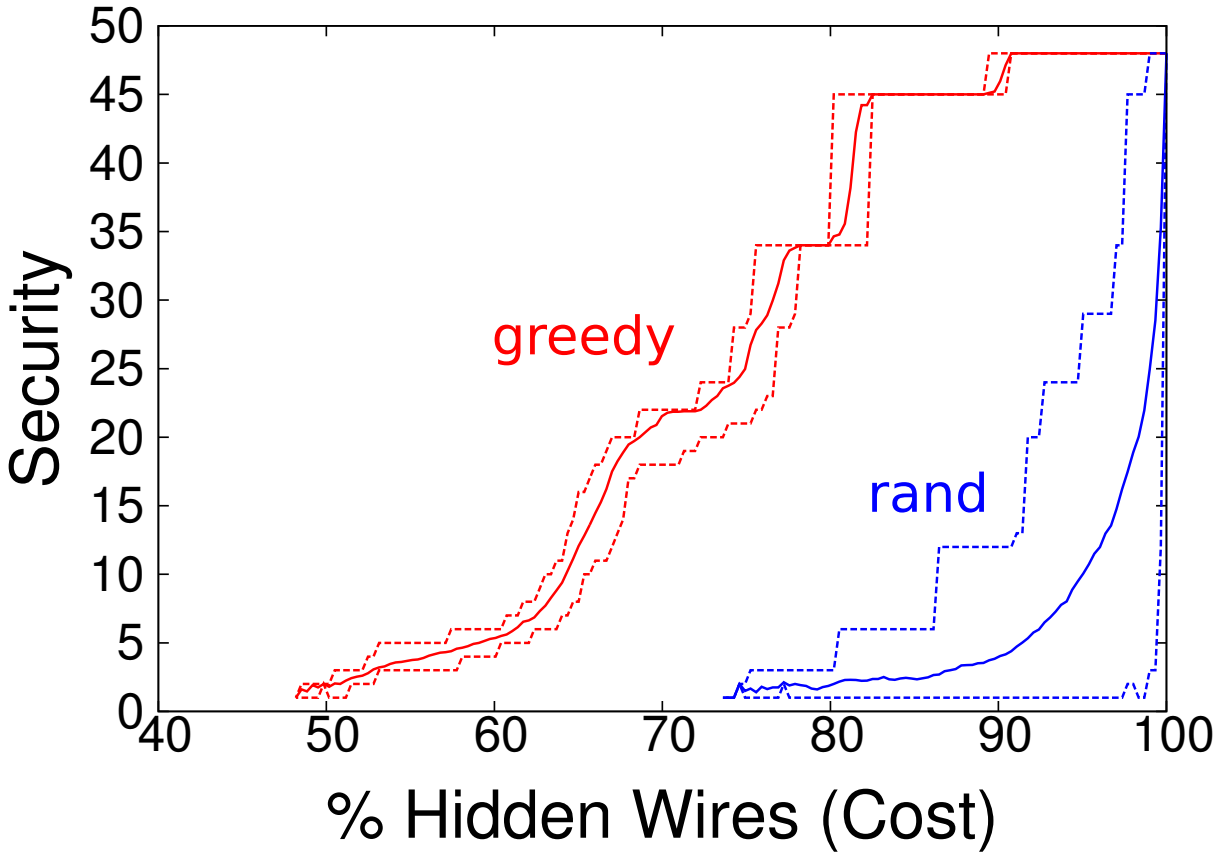


Figure: Experiments on the c432 circuit, which contains 303 edges. The c432 circuit is a 27-channel interrupt controller.

Security vs. Number of Removed Edges

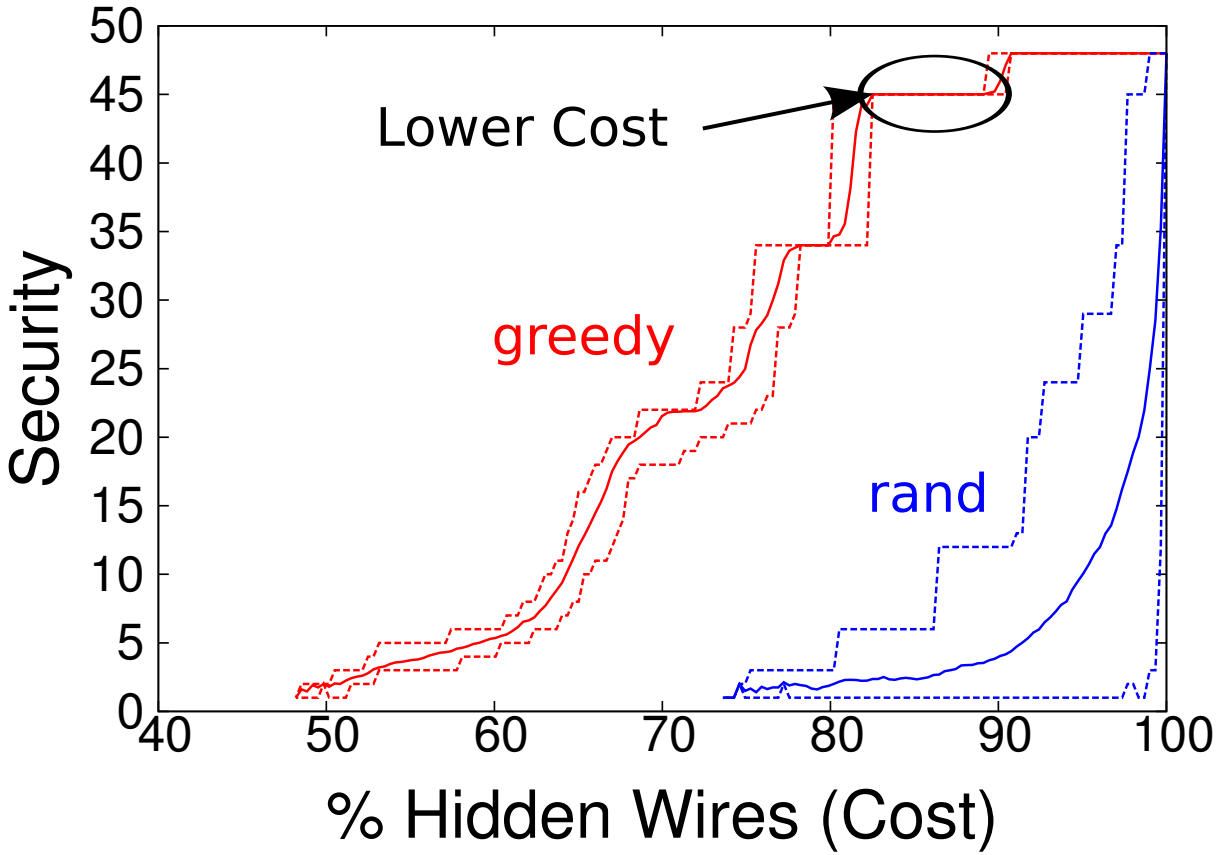
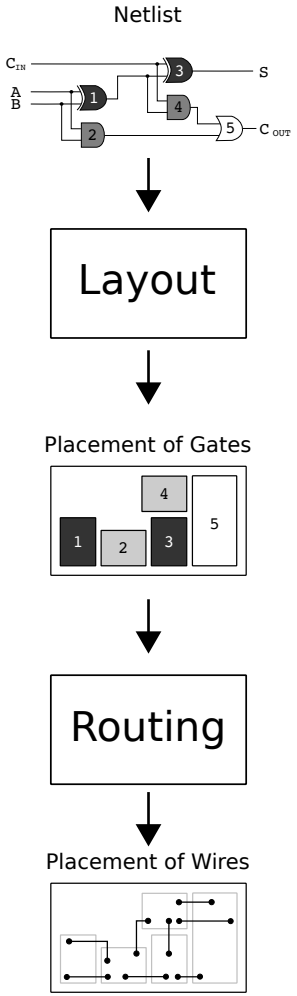
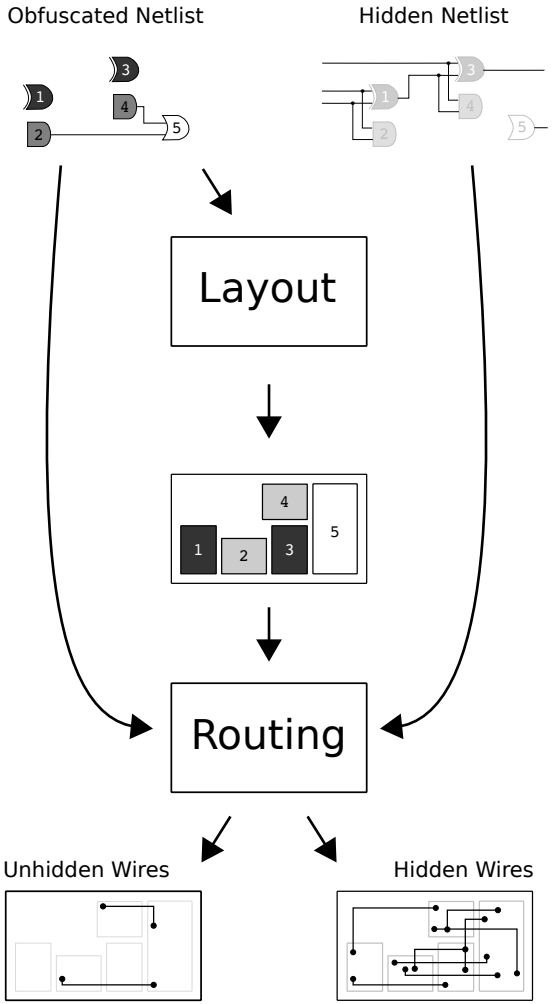


Figure: Experiments on the c432 circuit, which contains 303 edges. The c432 circuit is a 27-channel interrupt controller.

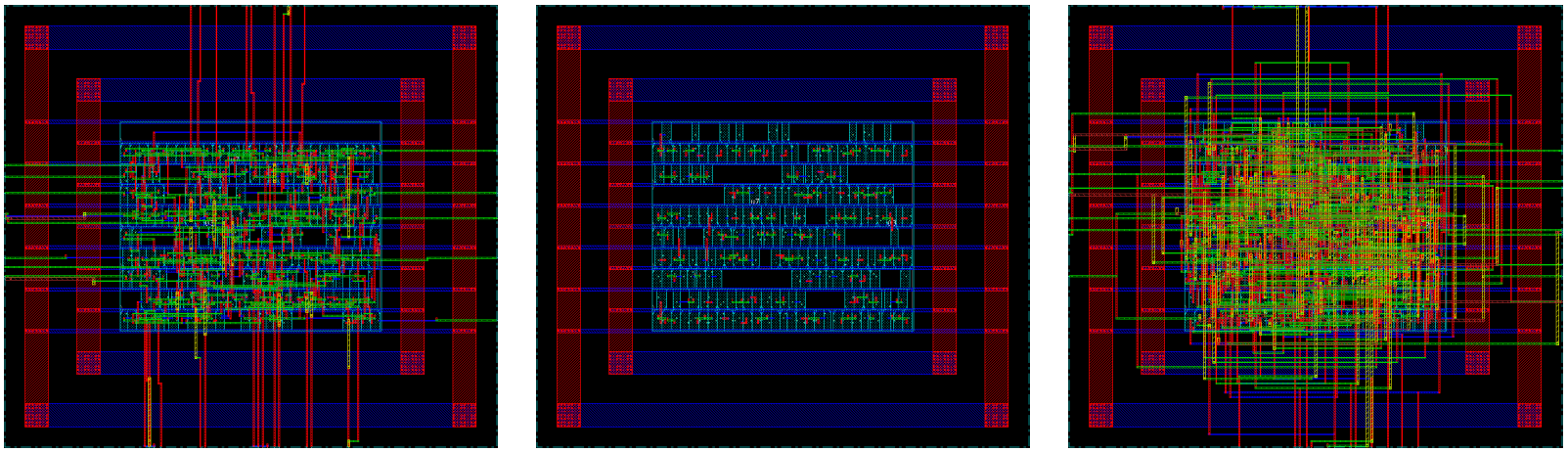
Layout Randomization



Layout Randomization



Layout and Routing Results



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

Figure: Layout of c432 without any security (left), and the obfuscated (middle) and hidden tiers of an 8-secure version of c432 circuit. Green and red lines correspond to metal wires.

Wire Length Distribution

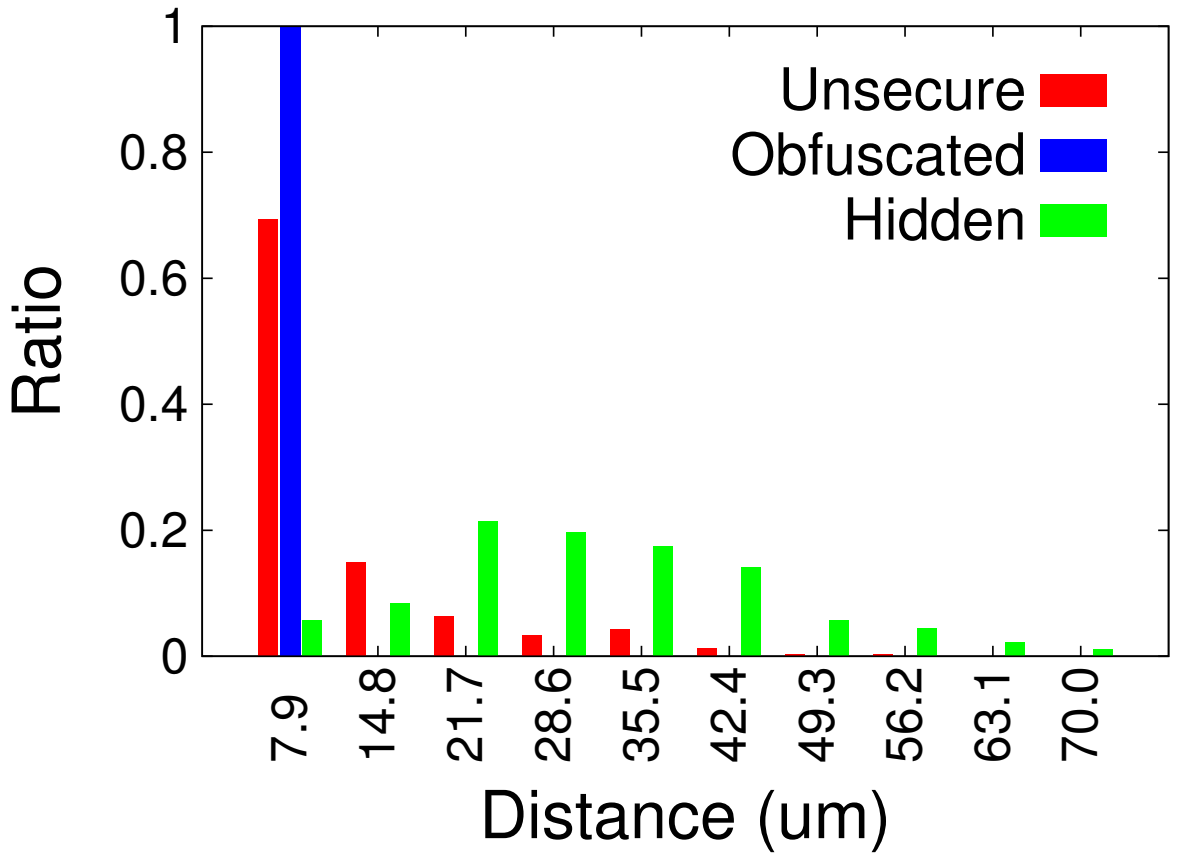


Figure: Comparison of the wire length distribution for the unsecured, obfuscated and hidden circuits. Also the hidden wire length distribution passes the χ^2 test when compared to a random distribution.

Power and Delay Costs

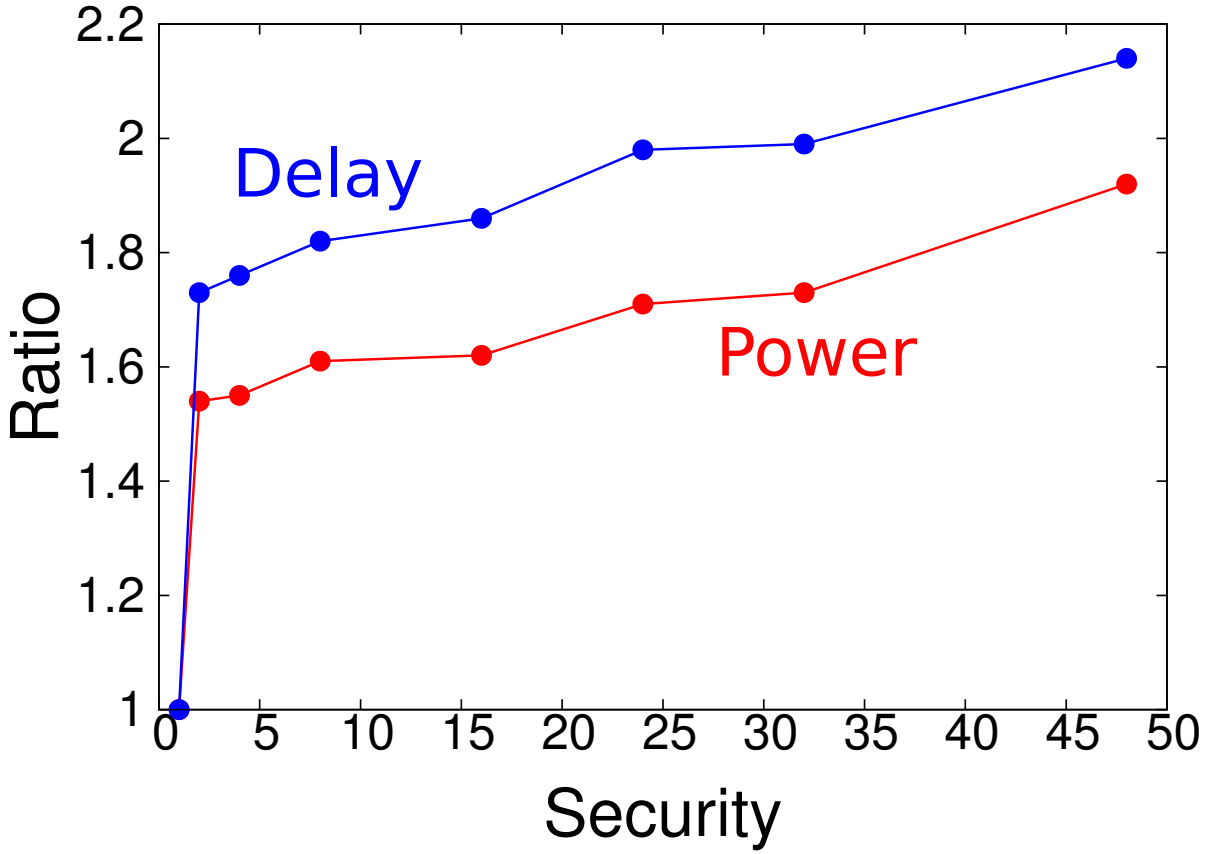
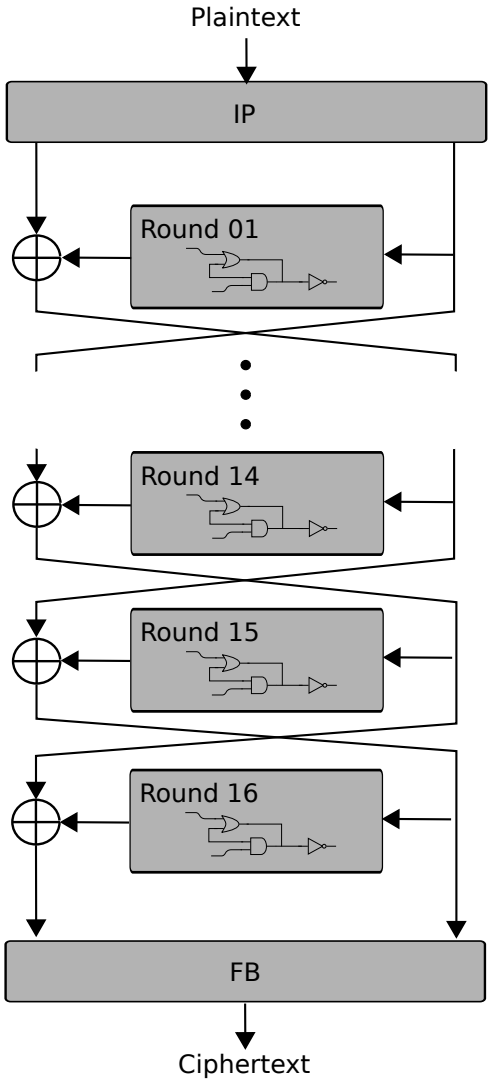


Figure: Power and delay ratio calculated from base/unsecured circuit.

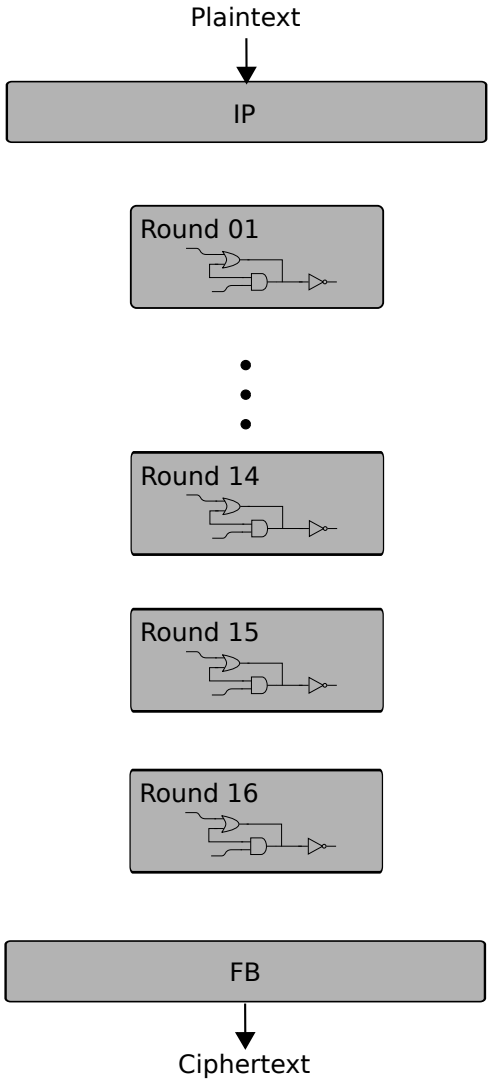
Case Study: DES Circuit

- Symmetric key-based encryption/ decryption algorithm.
- 35,000 gate implementation from OpenCores library.
- A fault in LSB of 14th round reveals secret key [3].



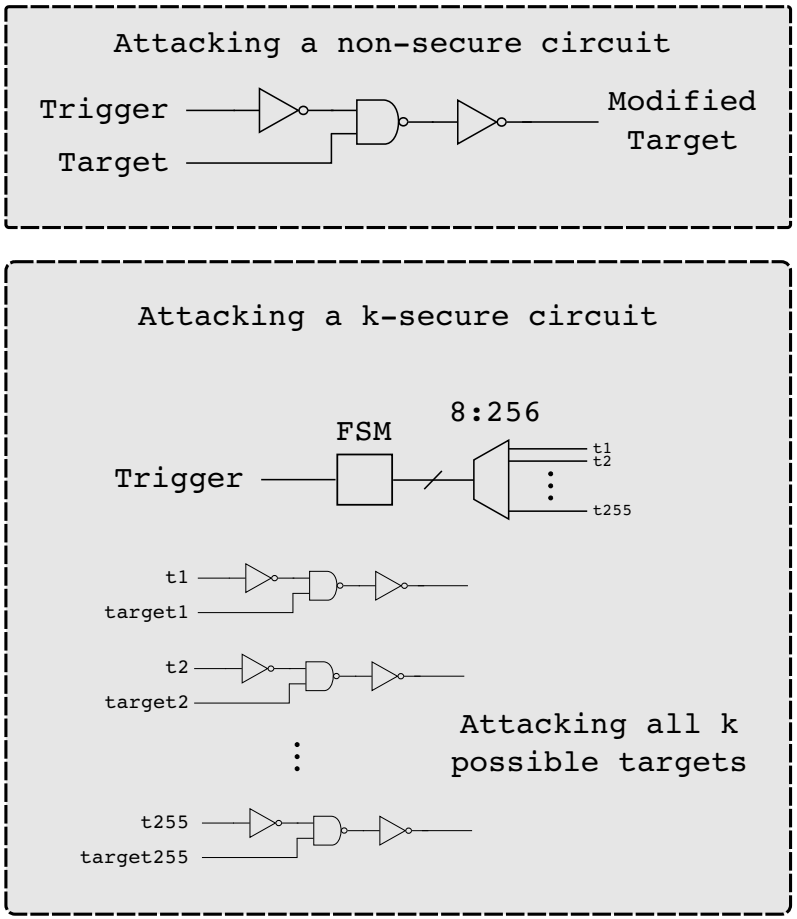
Case Study: DES Circuit

- Symmetric key-based encryption/ decryption algorithm.
- 35,000 gate implementation from OpenCores library.
- A fault in LSB of 14th round reveals secret key [3].
- 16-secure circuit is obtained by removing only 13% of wires.
- Further lifting can increase security.

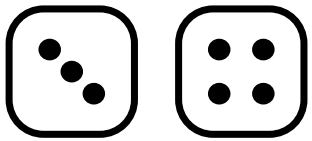


Impact on Attack Footprint

- Implemented a 64-secure DES circuit.
- 14th round LSB is actually 255-secure.
- 420x area overhead to attack a 255-secure gate.



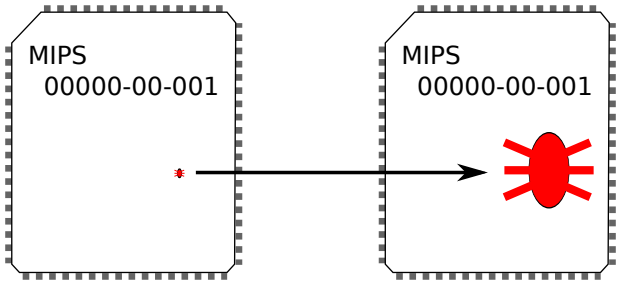
Raising the Bar on the Attacker



Attack 1 out of k gates

–or–

Attack all k gates



Related Work and References

Alina Campan and Traian Truta.

Data and structural k-anonymity in social networks.
Privacy, Security, and Trust in KDD, pages 33–54, 2009.

Alex Baumgarten, Michael Steffen, Matthew Clausman, and Joseph Zambreno.

A case study in hardware trojan design and implementation.
International Journal of Information Security, 10(1):1–14, 2011.

Dan Boneh, Richard DeMillo, and Richard Lipton.

On the importance of checking cryptographic protocols for faults.
In *Advances in CryptologyEUROCRYPT97*, pages 37–51. Springer, 1997.

F. Brglez.

Neutral netlist of ten combinational benchmark circuits and a target translator in fortran.
In *Special session on ATPG and fault simulation, Proc. IEEE Int. Symp. Circuits and Systems, June 1985*, pages 663–698, 1985.

Y. Jin, N. Kupp, and Y. Makris.

Experiences in hardware trojan design and implementation.
In *Hardware-Oriented Security and Trust, 2009. HOST'09. IEEE International Workshop on*, pages 50–57. IEEE, 2009.

S. h and C. Woods.

Breakthrough silicon scanning discovers backdoor in military chip.
Cryptographic Hardware and Embedded Systems–CHES 2012, pages 23–40, 2012.


UNIVERSITY OF
Waterloo