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/
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].”
Attack Types

Examples:

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

**Successful Attack**

⇓

**Uniquely identify at least one gate**

Successful Attack

Uniquely identify at least one gate

Example

Full Adder Netlist

C_{IN} \quad \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad S

A \quad \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad C_{OUT}

B

T

Malicious Gate
Example

Full Adder Netlist

- \( C_{IN} \)
- \( A \)
- \( B \)
- \( T \)
- \( S \)
- \( C_{OUT} \)
Example

Full Adder Netlist

\[ \begin{align*}
C_{IN} & \quad \text{A} \quad \text{B} \\
\text{1} & \quad \text{2} \quad \text{M} \\
\text{3} & \quad \text{4} \quad \text{5} \\
S & \quad \text{C\text{OUT}}
\end{align*} \]
Our Solution – Circuit Obfuscation

Full Adder Netlist

Obfuscated Netlist

Frank Imeson, Waterloo ECE

3D Hardware Security
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

Circuit Obfuscation with 3D Technology

Introduction
Attack Model
k-Security
Layout Randomization
Summary

Outsourced
In House
Fabrication
Fabrication
1 3 2 4 5
Hidden Circuit
Obfuscated Circuit
Stacking
AB
CIN S
C OUT
1 2 3 4 5
U V X W Y
Hide Wires
Place and Route

Frank Imeson, Waterloo ECE
3D Hardware Security
11/26
Circuit Obfuscation with 3D Technology

- **Introduction**
- **Attack Model**
- **k-Security**
- **Layout Randomization**
- **Summary**

Outsourced

In House

Fabrication

Fabrication

1 3 2

4

5

Hidden Circuit

Obfuscated Circuit

Stacking

AB

C INC

C OUT

CIN S

1

2

3

4

5

U

V

X

W

Y

Hide Wires

Place and Route

Frank Imeson, Waterloo ECE

3D Hardware Security
Circuit Obfuscation with 3D Technology

Frank Imeson, Waterloo ECE 3D Hardware Security 11/26
Attack Model Summary

Original Netlist

C_{IN} → 3 → S

A, B → 1 → 2 → 4 → 5 → C_{OUT}

Obfuscated Circuit

AB
CIN S
C OUT
1
2
3
4
5
Original Netlist
Obfuscated
Circuit
V
X
U
W
Y
2 4
5
3
1
G
W V
Y
X
U
H

Frank Imeson, Waterloo ECE
3D Hardware Security
### Attack Model Summary

#### Original Netlist

- Circuit Diagram
- Variables: $C_{IN}$, $A$, $B$, $S$, $C_{OUT}$

#### Obfuscated Circuit

- Circuit Diagram
- Variables: $X$, $W$, $U$, $Y$

#### Graphs

- Graph $G$
  - Nodes: 1, 2, 3, 4, 5
  - Edges: 1-2, 2-3, 3-4, 4-5
- Graph $H$
  - Nodes: X, Y, V, U
  - Edges: X-V, V-U, U-Y

Frank Imeson, Waterloo ECE
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

![Graphs G and H](image-url)
What an Attacker Needs to Do

- Input graphs $G$ and $H$
- Find subgraph isomorphisms
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.
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.
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.
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

\[ \langle G, H \rangle \text{ is } k\text{-secure } \in \mathbf{NP}\text{-complete.} \]

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

Netlist

Placement of Gates

Routing

Placement of Wires
Layout Randomization

- Obfuscated Netlist
- Hidden Netlist
- Layout
- Routing
- Unhidden Wires
- Hidden Wires
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.
Figure: Comparison of the wire length distribution for the unsecured, obfuscated and hidden circuits. Also the hidden wire length distribution passes the $\chi^2$ 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.
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.

Alex Baumgarten, Michael Steffen, Matthew Clausman, and Joseph Zambreno.
A case study in hardware trojan design and implementation.

Dan Boneh, Richard DeMillo, and Richard Lipton.
On the importance of checking cryptographic protocols for faults.

F. Brglez.
Neutral netlist of ten combinational benchmark circuits and a target translator in fortran.

Y. Jin, N. Kupp, and Y. Makris.
Experiences in hardware trojan design and implementation.

S. h and C. Woods.
Breakthrough silicon scanning discovers backdoor in military chip.