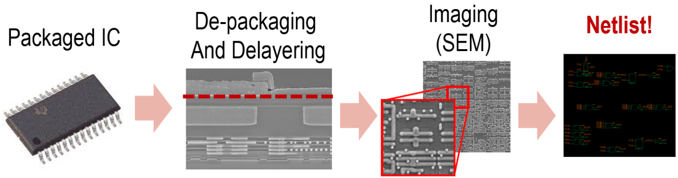
Integrated Circuit (IC) Decamouflaging: Reverse Engineering Camouflaged ICs within Minutes

Mohamed El Massad[†]

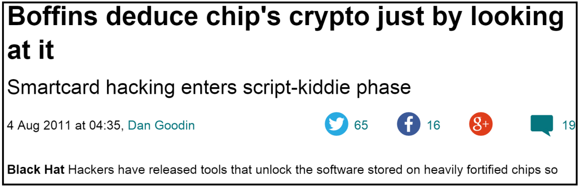
with Siddharth Garg[†] and Mahesh Tripunitara[‡]

[†]New York University, [‡]University of Waterloo

Threat: IC Circuit Extraction



"Extracted an IC with embedded encryption hardware and 12K gates of digital logic....Now we *understood the encryption*, had the keys and full chip simulations running" — [Torrance+, CHES'09]



Boffins deduce chip's crypto just by looking at it

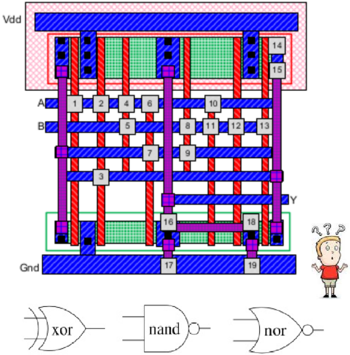
Smartcard hacking enters script-kiddie phase

4 Aug 2011 at 04:35, Dan Goodin 65 16 19

Black Hat Hackers have released tools that unlock the software stored on heavily fortified chips so

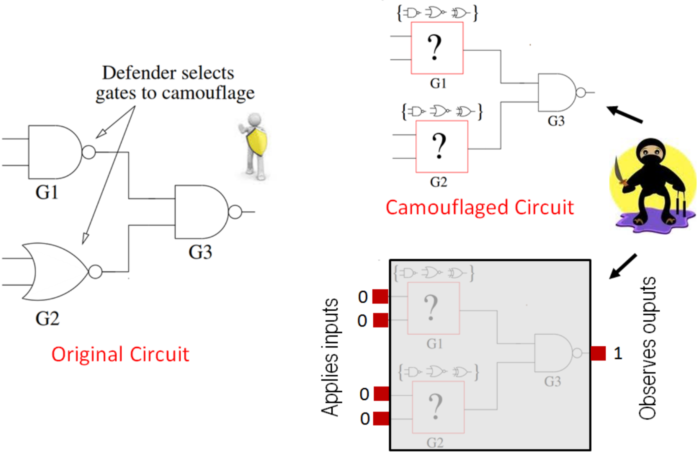
Proposed Solution: IC Camouflaging

- Use of dummy contacts to camouflage a gate. [US6791191]
- Identity of camouflaged gate cannot be determined by attacker. [R+,CCS'13]
  - Ex: {XOR, NAND, NOR} look identical to attacker



[R+, CCS'13] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri. ACM CCS'13. *(Best Student Paper)*

Defender vs. Attacker



Defender selects gates to camouflage

Original Circuit

Camouflaged Circuit

Applies inputs

Observes ouputs

Black-Box Circuit

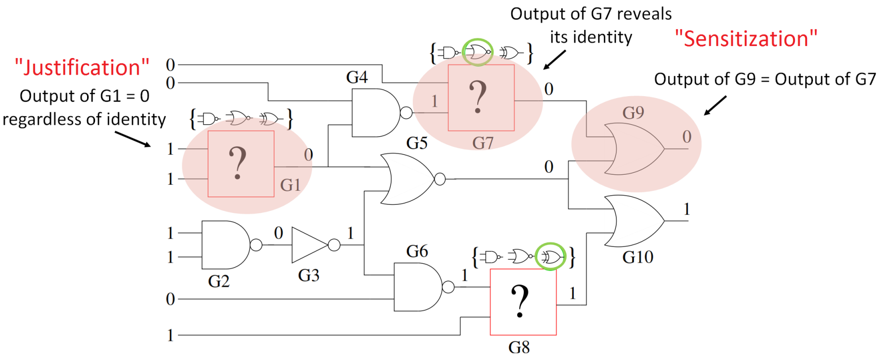
IC Camouflaging – Trade-off

- Camouflaging has a per-gate cost (area/delay/power).
- Claim [R+, CCS'13]: if a small number of judiciously selected gates (> 140) are camouflaged $\Longrightarrow$ attacker would need "1000's of years" to decamouflage.

[R+,CCS'13] seemingly resolves cost vs. security trade-off.

Credit: `partypeopleinc.com`

Which gates. . . ? — mindset from [R+, CCS'13]



"Justification"

Output of G1 = 0 regardless of identity

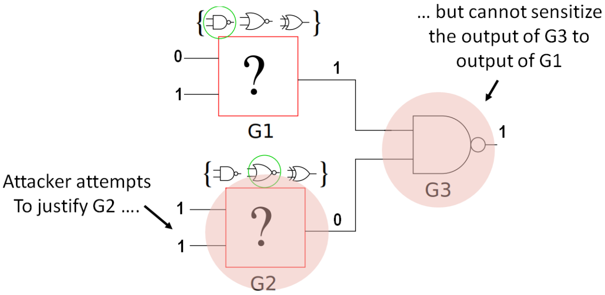
Output of G7 reveals its identity

"Sensitization"

Output of G9 = Output of G7

Polynomial-time attack strategy if gates can be simultaneously justified and sensitized.

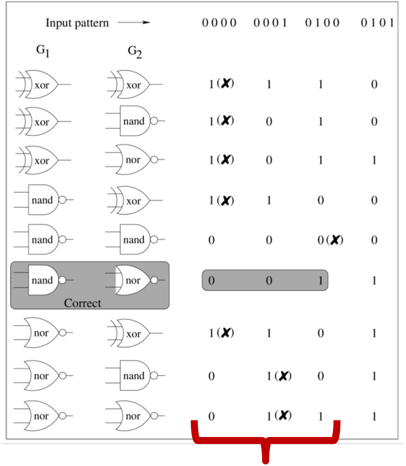
Non-Resolvable Gates


… but cannot sensitize the output of G3 to output of G1
0
1
?
1
G1
1
G3
Attacker attempts To justify G2 ….
1
1
?
0
G2

Claim [R+, CCS'13]: If gates *cannot* be simultaneously justified and sensitized, attacker must resort to brute-force attack ⟶ exponential complexity in number of camouflaged gates.

Procedure to camouflage gates such that this property is satisfied.

The Example, Revisited



Input pattern →		0000	0001	0100	0101
G1	G2				
xor	xor	1 (✗)	1	1	0
xor	nand	1 (✗)	0	1	0
xor	nor	1 (✗)	0	1	1
nand	xor	1 (✗)	1	0	0
nand	nand	0	0	0 (✗)	0
nand Correct	nor	0	0	1	1
nor	xor	1 (✗)	1	0	1
nor	nand	0	1 (✗)	0	1
nor	nor	0	1 (✗)	1	1

Discriminating set of size 3

- Each input eliminates a subset of solutions (aka *completions*).
- A set of inputs *sufficient* to eliminate all but the right completion → discriminating set.

Discriminating Set of Inputs

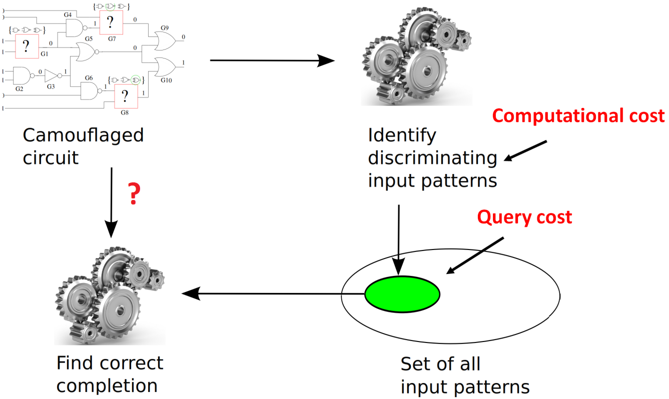
C is the camouflaged circuit.
X is a completion, i.e., assignment to camouflaged gates.
C_X is the camouflaged circuit with completion X.
$\mathcal{C}$ is the blackbox circuit.

Definition

I, a set of input patterns, is discriminating if:

for every incorrect completion X, $\exists i \in I$ s.t. $C_X(i) \neq \mathcal{C}(i)$

Attack — Preview



Camouflaged circuit

?

Identify discriminating input patterns

Computational cost

Query cost

Find correct completion

Set of all input patterns

This Paper: In practice, both query cost and computational cost of attack are low ⟶ IC decamouflaging in minutes.

Credit: `liv9.ca`

Devising the Two Procedures

$\overline{\textsc{Disc-Set-Dec}}$, Inputs: C, I, $\mathcal{C}(I)$.
Is I NOT a discriminating set?

Certificate for $\overline{\textsc{Disc-Set-Dec}}$:
Distinct completions X_1 and X_2 that agree on all inputs in I but not on new input $i \notin I$.
$\implies \in$ **NP**

Oracle for $\overline{\textsc{Disc-Set-Dec}}$
Outputs $\langle X_1, X_2, i\rangle$

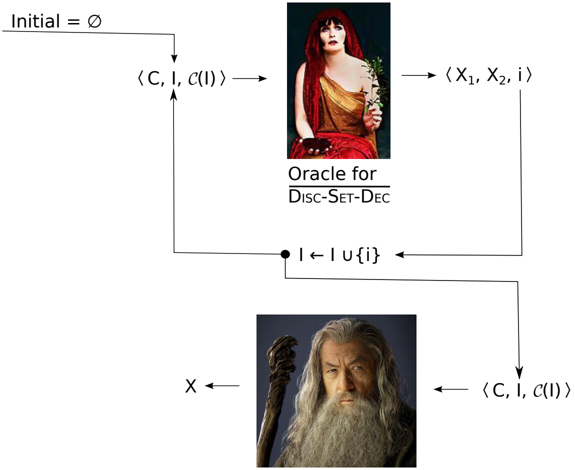
$\textsc{Completion-Dec}$, Inputs: C, I, $\mathcal{C}(I)$.
$\exists$ a completion X such that $C_X(I) = \mathcal{C}(I)$?

Certificate for $\textsc{Completion-Dec}$:
A valid completion X.
$\implies \in$ **NP**

Oracle for $\textsc{Completion-Dec}$
Outputs X

Credit: `squarespace.com`, `redbubble.net`

Attack Procedure



Initial = ∅

$\langle C, I, \mathcal{C}(I) \rangle$

$\langle X_1, X_2, i \rangle$

Oracle for Disc-Set-Dec

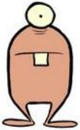
$I \leftarrow I \cup \{i\}$

X

$\langle C, I, \mathcal{C}(I) \rangle$

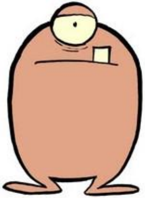
Oracle for Completion-Dec

Building the Oracles



$\leq$

(reduce)



+

$\overline{\text{Disc-Set-Dec}}$/
Completion-Dec

CNF-SAT

SAT Solver
(e.g., MiniSat)

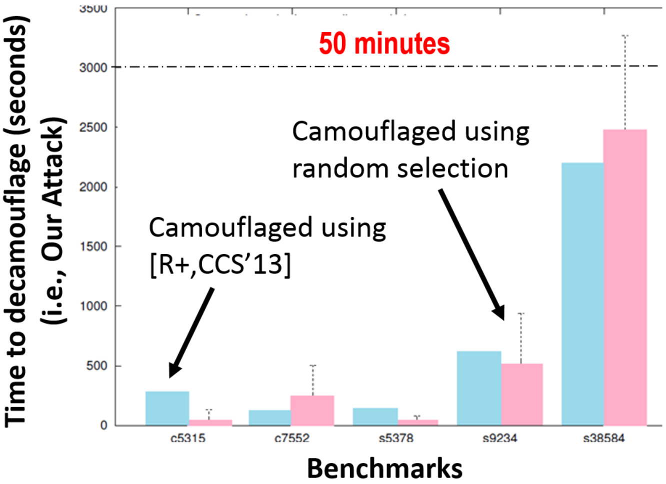
Credit: `bigcommerce.com`, `aclib.net`

Benchmarks

B'mark	Inputs	Outputs	Gates	Camouflaged
c432	36	7	160	10
s298	3	6	133	6
s400	3	6	164	7
s444	3	6	181	7
s713	35	23	393	9
c5315	178	123	2406	63
c7552	207	108	3512	65
s5378	35	49	2779	56
s9234	19	22	5597	79
s38584	38	304	19234	128

Same number of gates camouflaged as in [R+,CCS'13].

Time to Decamouflage



50 minutes

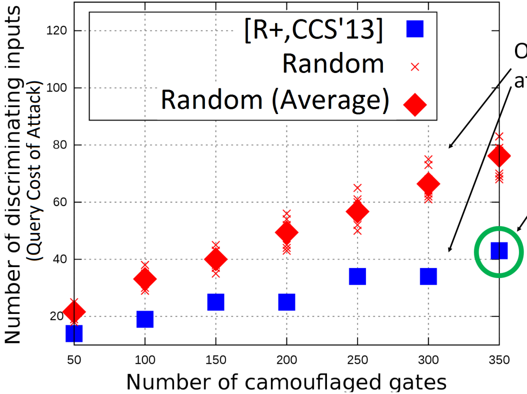
Camouflaged using random selection

Camouflaged using [R+,CCS'13]

Brute-force → Our Attack : 10^{13} Years → 50 Minutes.

Why Does the Attack Work?

Discriminating sets (i.e., query costs) are small, in practice.

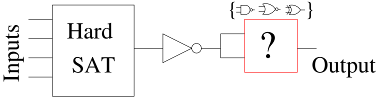


Only linear increase in # inputs attacker needs to apply

Attacker needs only 40 inputs to decamouflage a netlist with 350 camouflaged gates

Camouflaging insecure even with > 5× increase in cost.

Can IC Camouflaging Work?

- Increase attacker's query-complexity.
- 

- Increase # possible gate-types.

Takeaways

Strong caution for IC designers.

Appealing claims on secure IC camouflaging with low cost need to be vetted carefully.

Mindset rooted in foundations is helpful.

Credit: `pluspack.com`

Related Work

Chipworks.
Inside the Apple Lightning Cable.
http://www.chipworks.com/en/technical-competitive-analysis/resources/blog/inside-the-apple-lightning-cable/, Oct. 2012.

Degate.
Reverse engineering integrated circuits with degate.
http://www.degate.org/documentation/

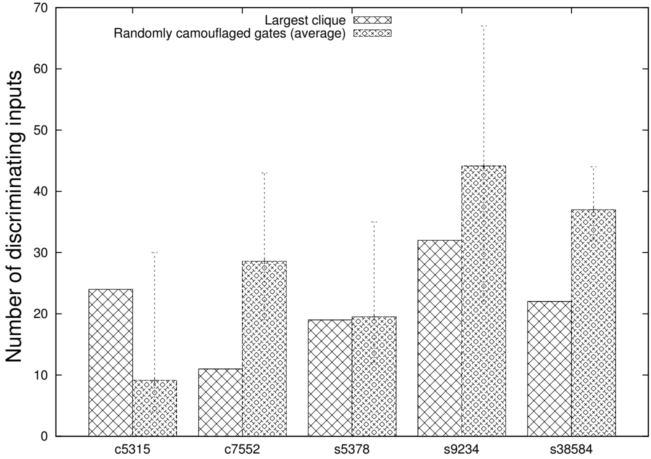
L.-W. Chow, J. P. Baukus, and W. M. Clark, Jr.
Integrated circuits protected against reverse engineering and method for fabricating the same using vias without metal terminations.
US Patent 6,791,191, Sept. 2004.

J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri.
Security Analysis of Integrated Circuit Camouflaging.
ACM SIGSAC Conference on Computer and Communications Security, CCS, 2013.

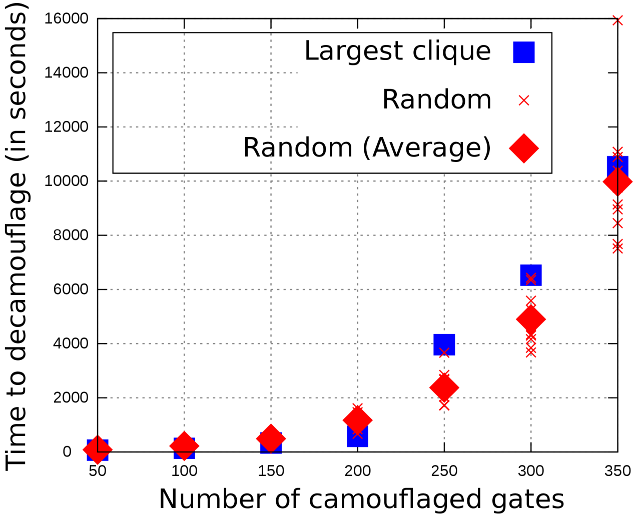
SypherMedia.
Syphermedia library circuit camouflage technology.
http://www.smi.tv/solutions.htm

A. Baumgarten, A. Tyagi and J. Zambreno.
Preventing IC piracy using reconfigurable logic barriers.
IEEE Design and Test of Computers, 27(1):6675, 2010.

Why Does the Attack Work?



Increased # Camouflaged Gates (c5315)


Time to decamouflage (in seconds)
Number of camouflaged gates
Largest clique ■
Random ×
Random (Average) ◆