NYU TANDON SCHOOL OF ENGINEERING

CENTER FOR CYBER SECURITY

جامعة نيويورك أبوظبي

NYU ABU DHABI

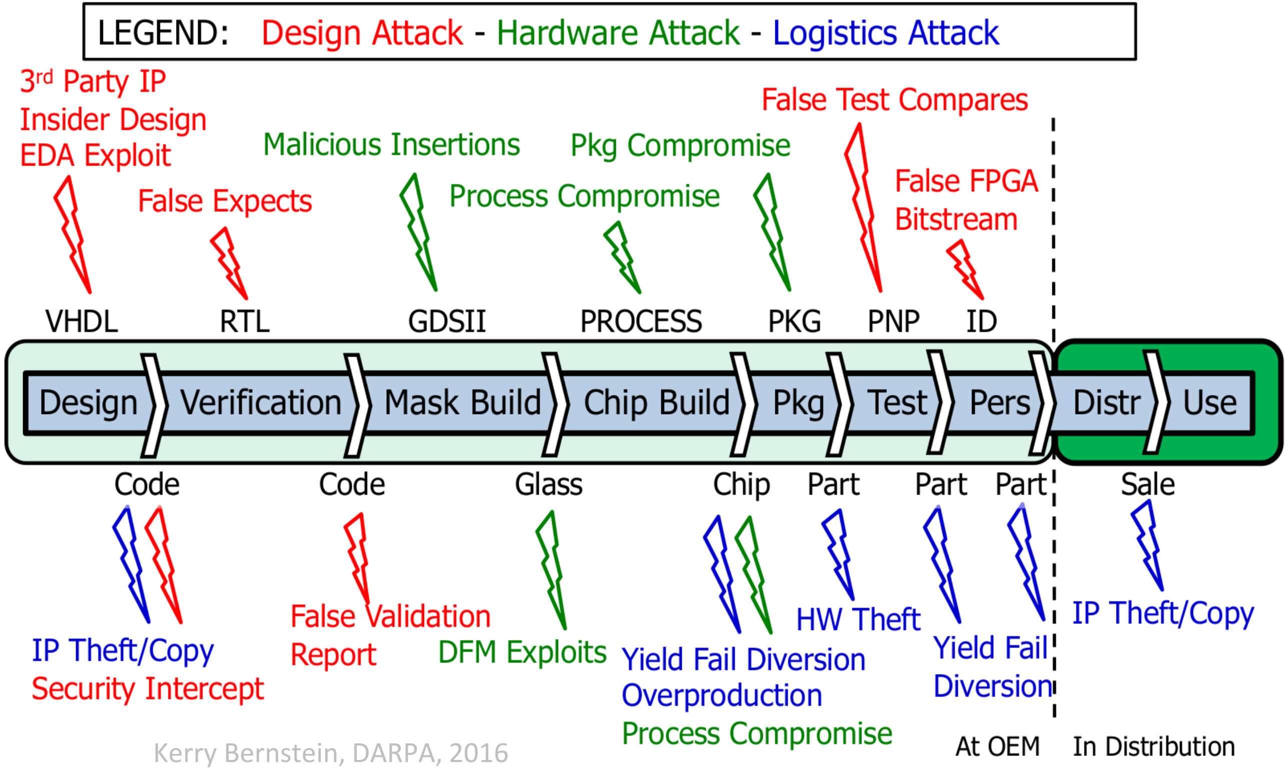
Protect Your Chip Design Intellectual Property: An Overview

Johann Knechtel, Satwik Patnaik, and Ozgur Sinanoglu

{johann, sp4012, ozgursin}@nyu.edu

COINS 2019, May 6, Crete, Greece

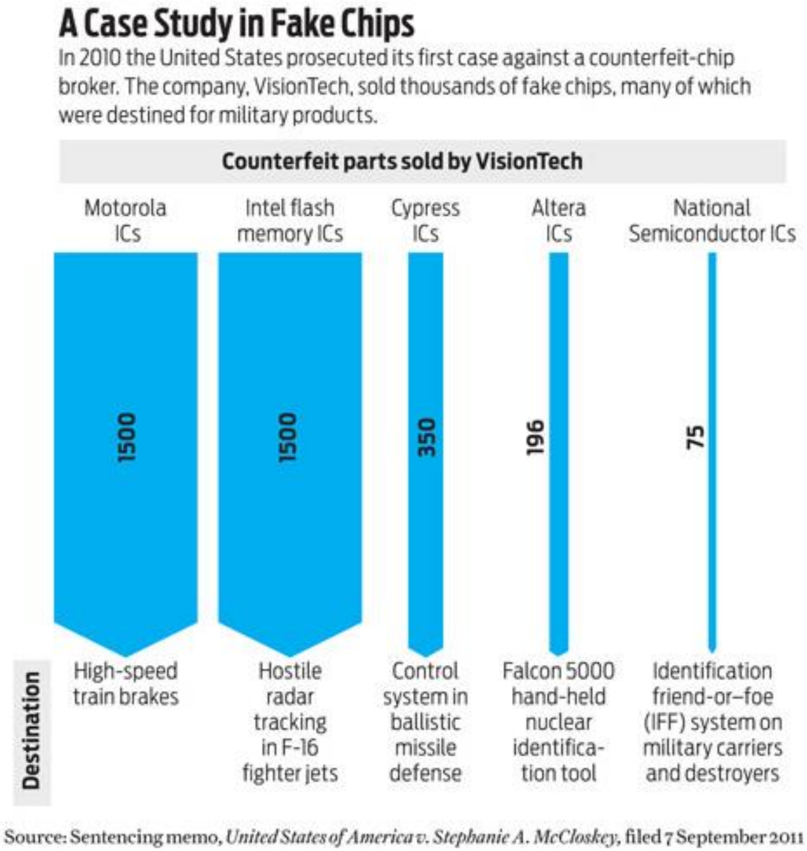
Threats for IC Fabrication and Hardware Security



Kerry Bernstein, DARPA, 2016

Knechtel et al., Protect Your Chip Design Intellectual Property: An Overview, COINS 2019

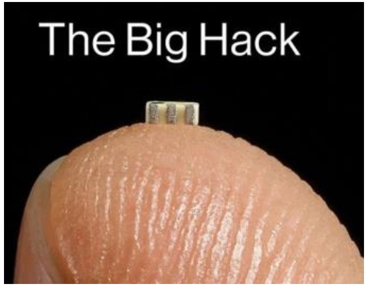
Growing Demand for Protection of Design IP



A Case Study in Fake Chips

In 2010 the United States prosecuted its first case against a counterfeit-chip broker. The company, VisionTech, sold thousands of fake chips, many of which were destined for military products.

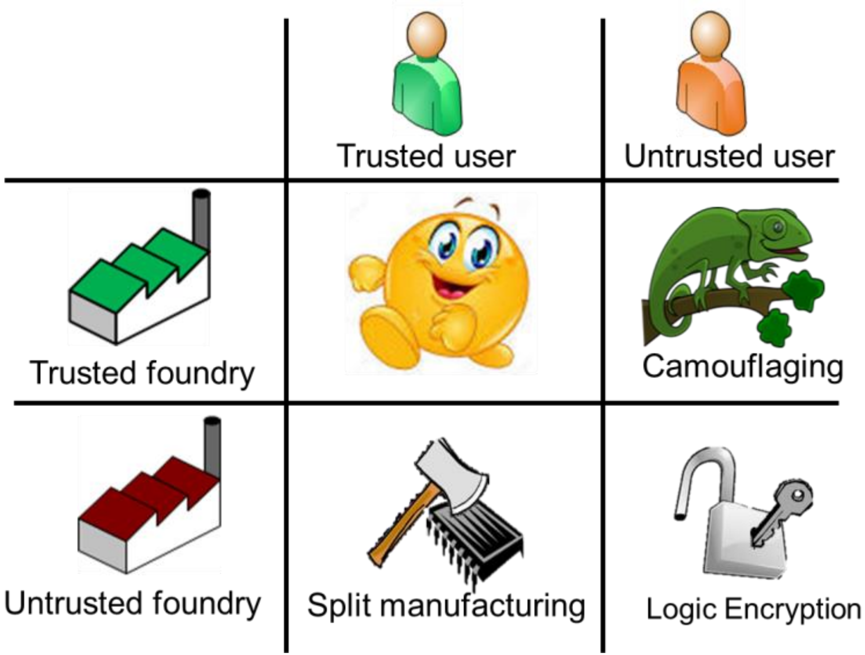
Source: Sentencing memo, *United States of America v. Stephanie A. McCloskey*, filed 7 September 2011



APRIL 2019: ZHENGZHOU CUSTOMS DESTROYS COUNTERFEIT TI CHIPS WORTH 704M YUAN

Zhengzhou Customs seized 20,000 automotive CPU ICs labeled with the Texas Instruments (TI) trademark, suspecting them to be counterfeit. [...] The intended function of the CPUs was to prevent short circuits caused by instantaneous current overload when a vehicle is started. Total value of the fake chips was estimated at 704 million yuan. (around 100 million USD).

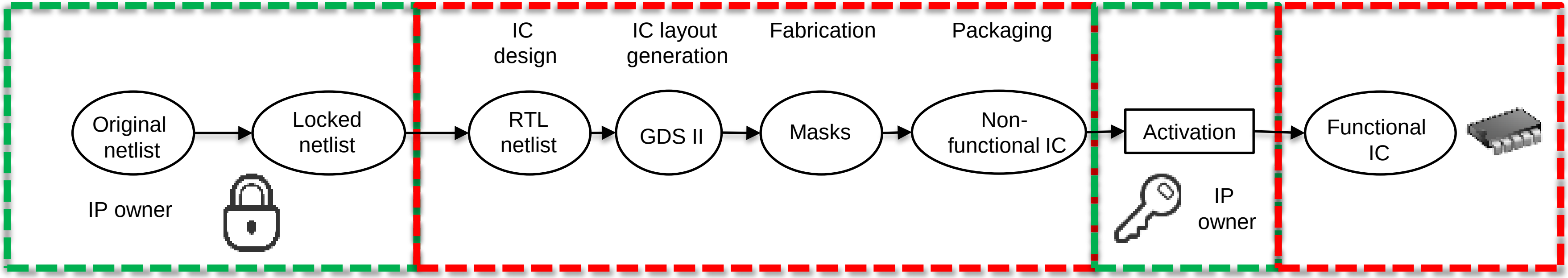
Protect Your Chip Design IP: An Overview



	Trusted user	Untrusted user
Trusted foundry		Camouflaging
Untrusted foundry	Split manufacturing	Logic Encryption

Knechtel et al., Protect Your Chip Design Intellectual Property: An Overview, COINS 2019

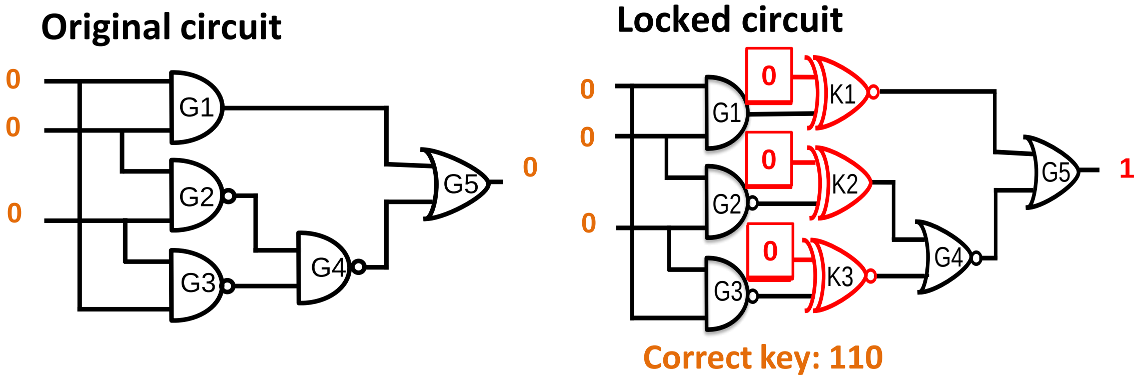
Basics of Logic Locking (Encryption)



- IP owner **locks** the design at RTL, by inserting dedicated **locking structures**
- IP owner unlocks the design after fabrication, by loading secret key onto memory
- Protects against **untrusted end-user + fab**

Knechtel et al., Protect Your Chip Design Intellectual Property: An Overview, COINS 2019

Basics of Logic Locking (Encryption)


Original circuit

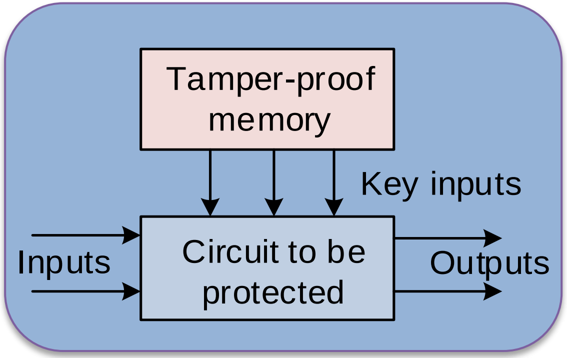
Locked circuit

Correct key: 110

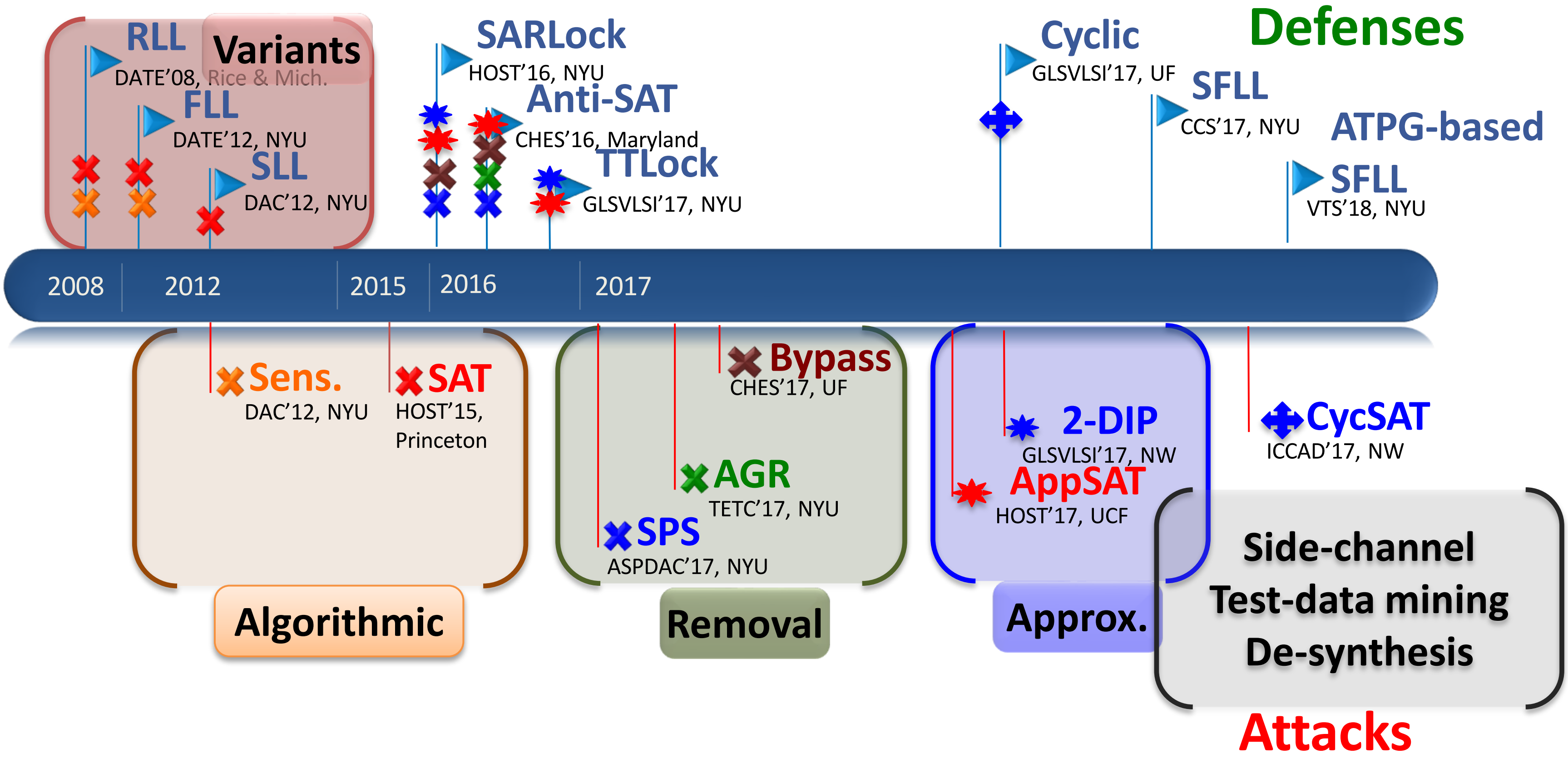
- Incorrect key → Incorrect output

⚠ Secure realization of tamper-proof memories

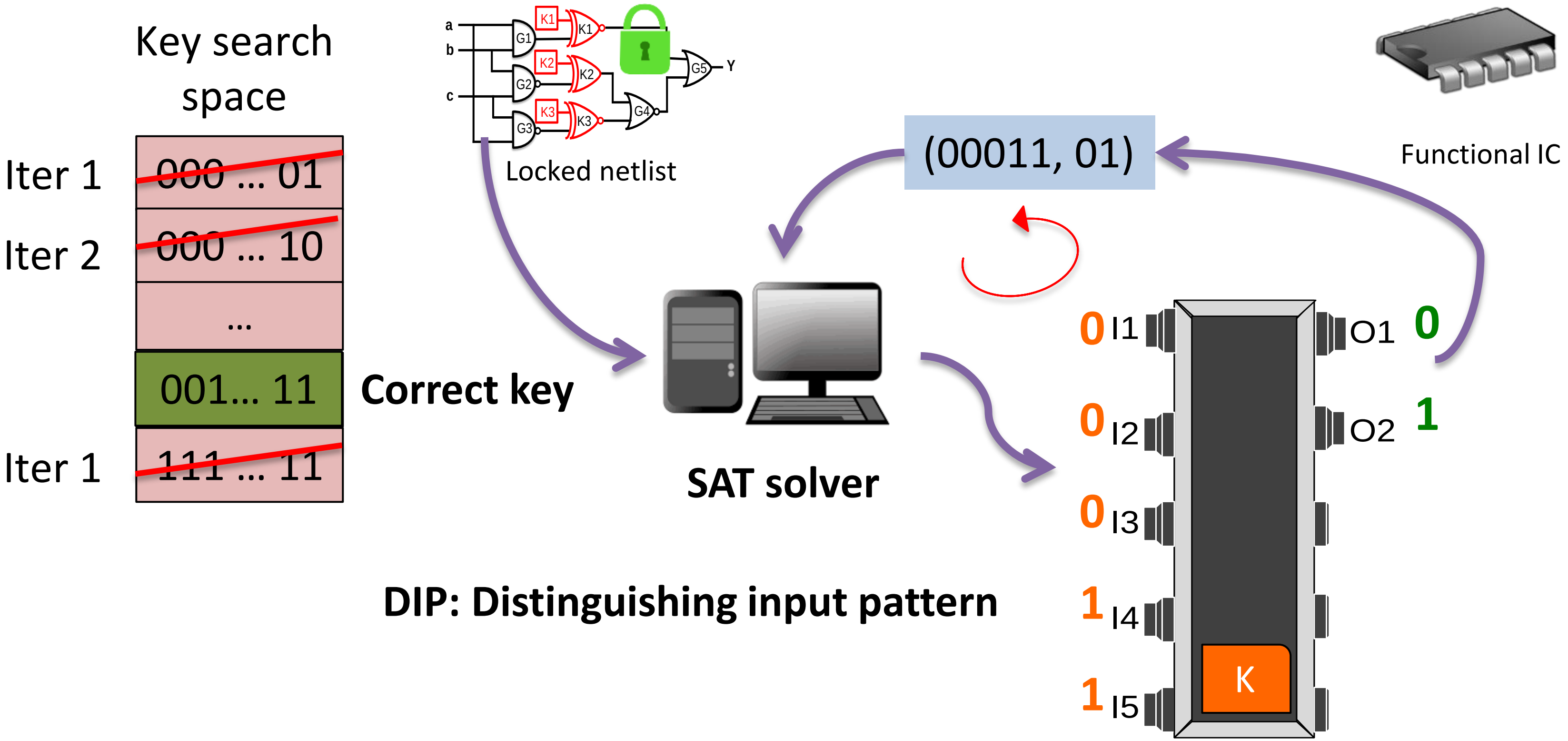
⚠ Prone to analytical and invasive attacks



Evolution of Logic Locking



Boolean Satisfiability: A Powerful Attack on Logic Locking



Key search space

Iter 1 ~~000 … 01~~

Iter 2 ~~000 … 10~~

…

001… 11 **Correct key**

Iter 1 ~~111 … 11~~

Locked netlist

(00011, 01)

Functional IC

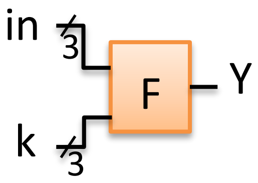
SAT solver

DIP: Distinguishing input pattern

SAT attacks broke all basic logic locking techniques

SAT Attack Success

					Output Y for different key values								
No.	a	b	c	Y	k0 ✗	k1 ✗	k2 ✗	k3 ✗	k4 ✗	k5 ✗	k6 ✓	k7 ✗	Pruned key values
0	0	0	0	0	1	1	1	1	1	1	0	1	
1	0	0	1	0	1	1	1	1	1	1	0	1	
2	0	1	0	0	1	1	1	1	1	1	0	1	
DIP 1	0	1	1	1	1	1	1	1	0	1	1	1	Iter 1: {k4}
DIP 3	1	0	0	0	1	1	1	1	1	1	0	1	Iter 3: all incorrect
5	1	0	1	1	1	1	1	1	1	1	1	0	
6	1	1	0	1	1	1	0	1	1	1	1	1	
DIP 2	1	1	1	1	1	0	0	1	1	1	1	1	Iter 2: {k1, k2}



Attack success ≈ effectiveness and selection of DIPs

SAT Attack Success

Worst-case scenario for attack:
Each DIP can eliminate only one key

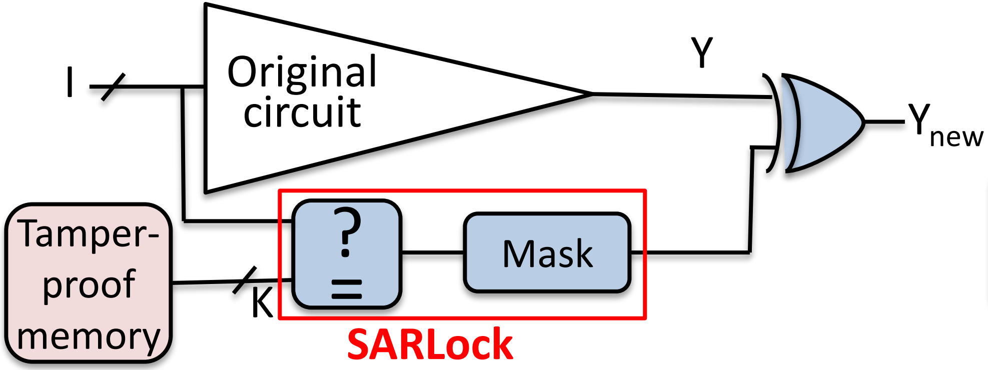
Worst case for attack:
#DIPs = 2^k-1

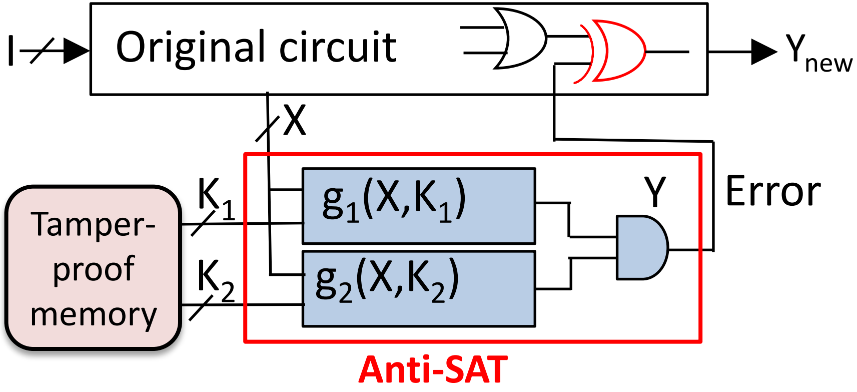
Trade-off:
SAT attack resilience v/s output corruptibility

					Output Y for different key values							
No.	**a**	**b**	**c**	**Y**	**k0**	**k1**	**k2**	**k3**	**k4**	**k5**	**k6** ✓	**k7**
0	0	0	0	0	0	1	0	0	0	0	0	0
1	0	0	1	0	1	0	0	0	0	0	0	0
2	0	1	0	0	0	0	0	1	0	0	0	0
3	0	1	1	1	1	1	1	1	1	1	1	1
4	1	0	0	0	0	0	0	0	0	1	0	0
5	1	0	1	1	1	1	1	1	0	1	1	1
6	1	1	0	1	1	1	1	1	1	1	1	1
7	1	1	1	1	1	1	1	1	1	1	1	0

Knechtel et al., Protect Your Chip Design Intellectual Property: An Overview, COINS 2019

Point-Function-Based Logic Locking Techniques

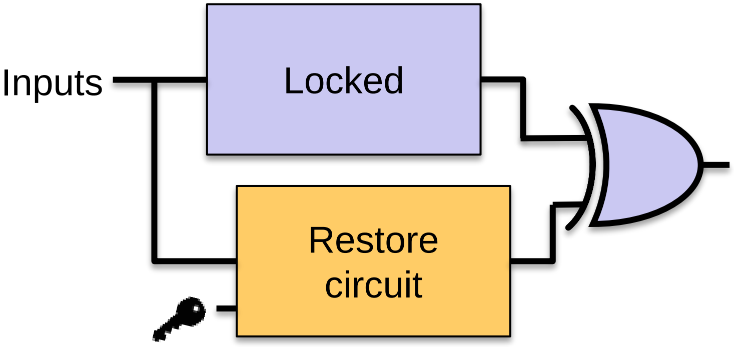




- Integration of point functions
  - E.g., AND/OR tree
  - Allows to control error injected into circuit
- Renders number of DIPs exponential in key size
- Vulnerability: Structural traces (identify & remove)

Stripped Functionality Logic Locking (SFLL)

- Based on “strip and restore”
  - ○ *Locked* circuit obtained from *original* circuit by making various changes at gate/RTL level
  - ○ *Restore circuit* is intertwined
- **In principle secure against all known attacks**
- **Quantifiable protection**



One output locked via SFLL

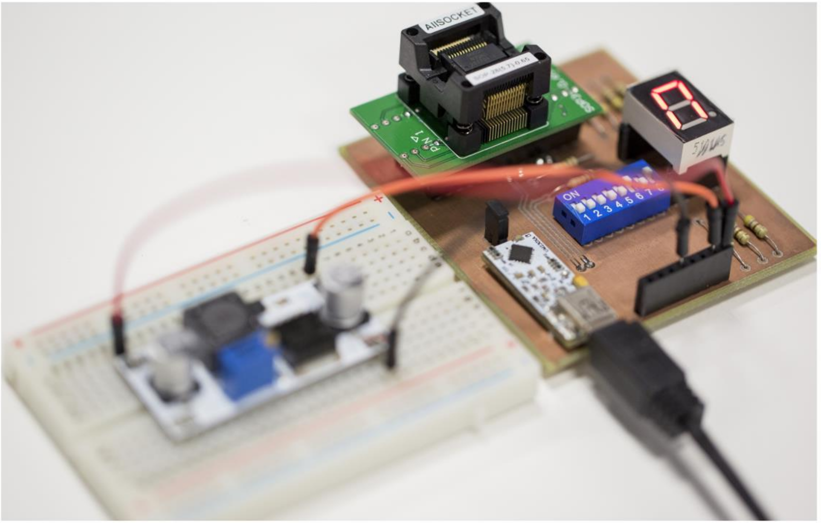
I2	I1	I0	original	locked
0	0	0	0	0
0	0	1	1	1
0	1	0	1	0
0	1	1	1	1
1	0	0	0	1
1	0	1	1	1
1	1	0	0	0
1	1	1	1	0

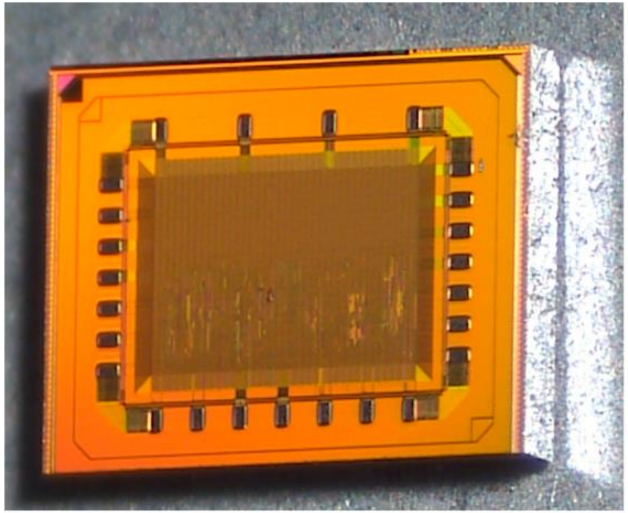
Example: 3 protected input patterns;

Error Rate = 3/8 (on locked output)

SFLL Chip

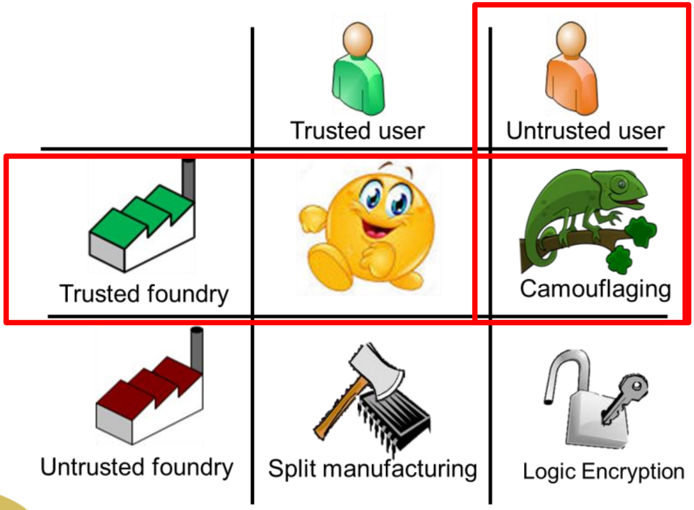
- First-of-its kind demonstration of resilient logic locking in 2017
- ARM Cortex-M0 microprocessor, 65nm GlobalFoundries technology
  - Layout cost affordable (1.6% A, 5.6% P, 5.4% D)
- https://github.com/DfX-NYUAD/CCS17



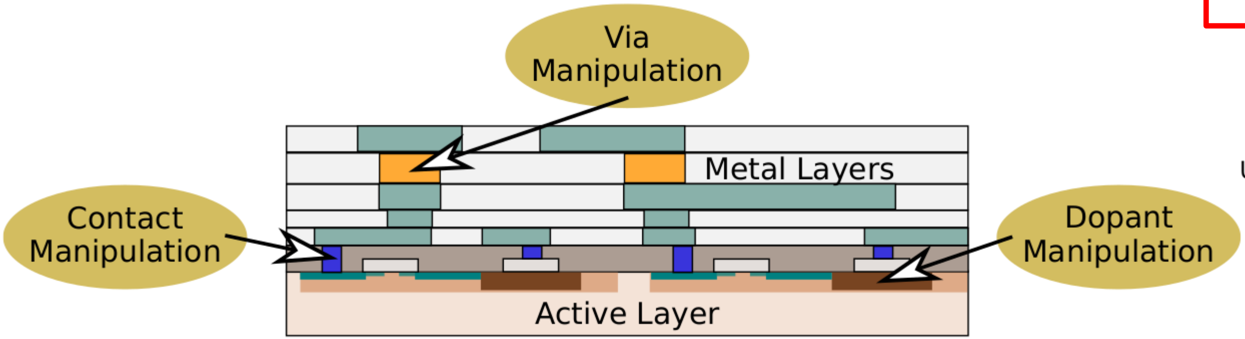


Yasin et al., Provably-Secure Logic Locking: From Theory To Practice, Proc. Comp. Comm. Sec. (CCS), 2017, 1601-1618

Basics of Layout Camouflaging



- Alter the chip's appearance to make it arduous for an attacker to infer the real functionality

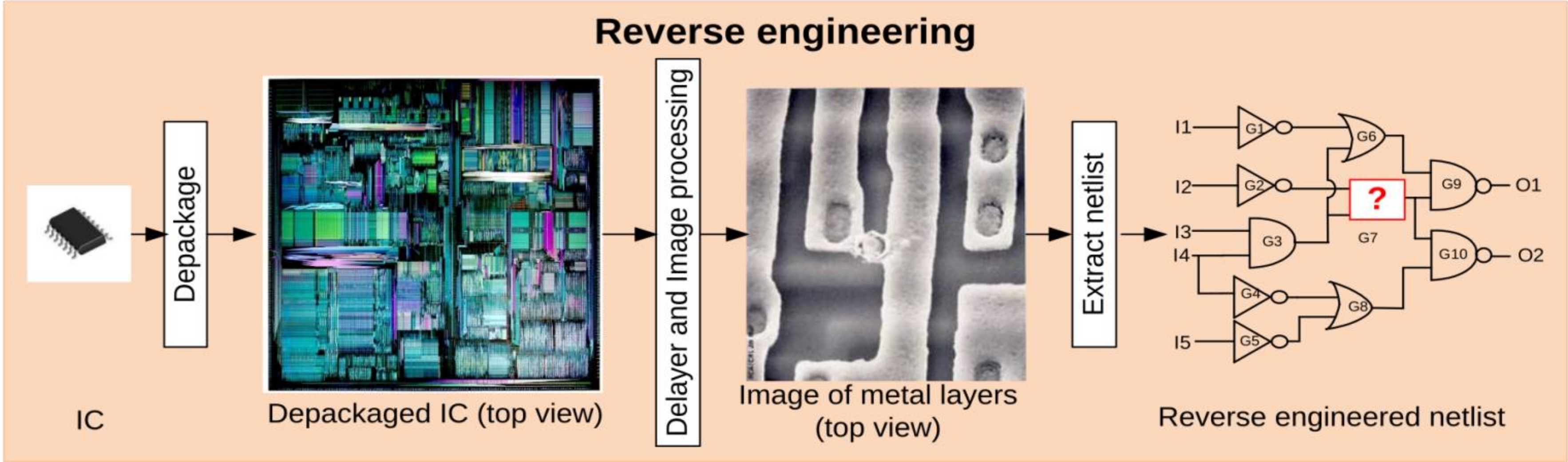


⚠ Trade-offs for security and cost (manufacturing cost, layout cost)

⚠ Prone to invasive and also to analytical attacks

Knechtel et al., Protect Your Chip Design Intellectual Property: An Overview, COINS 2019

Attacks on Layout Camouflaging



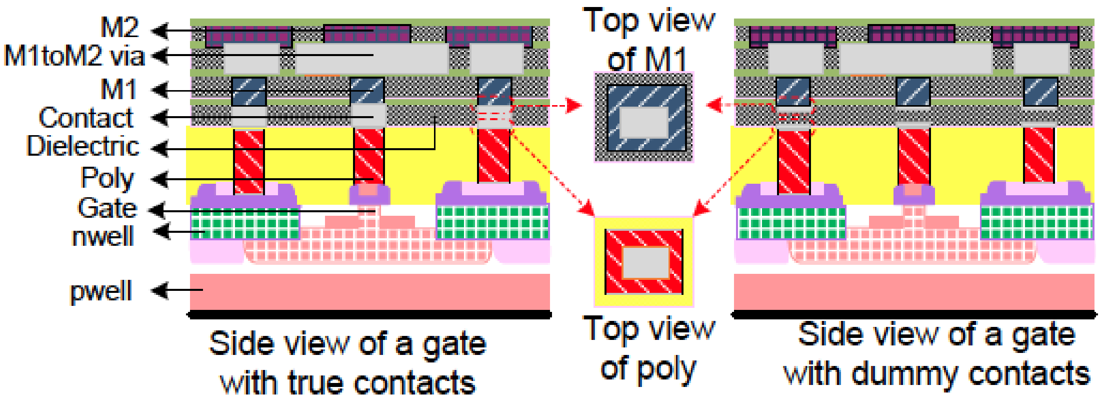
Rajendran et al.: Security Analysis of Integrated Circuit Camouflaging, Proc. Comp. Comm. Sec., 2013, 709-720

1) Modeling of unknown gates as locking problem, using SAT attacks

2) Etching, failure analysis, electron microscopy, photon emission, etc.

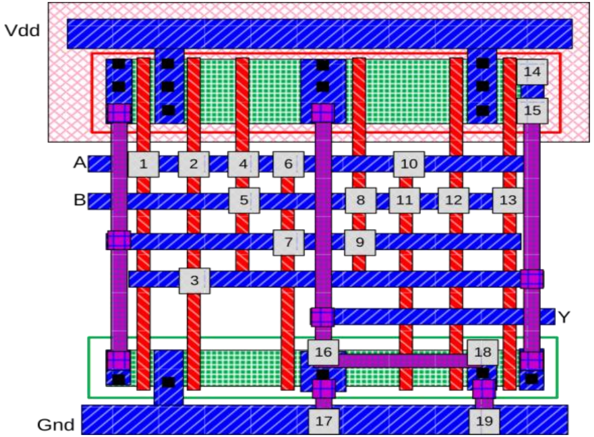
FEOL-Centric Layout Camouflaging

- Dummy contacts, e.g., NAND-NOR-XOR primitive in [Rajendran-CCS13]
  - PPA cost of 5.5X, 1.6X, 4X over 2-input NAND gate
    - Small-scale application, possibly locking-inspired; low error rate
  - Can be reverse-engineered using SEM PVC



Side view of a gate with true contacts

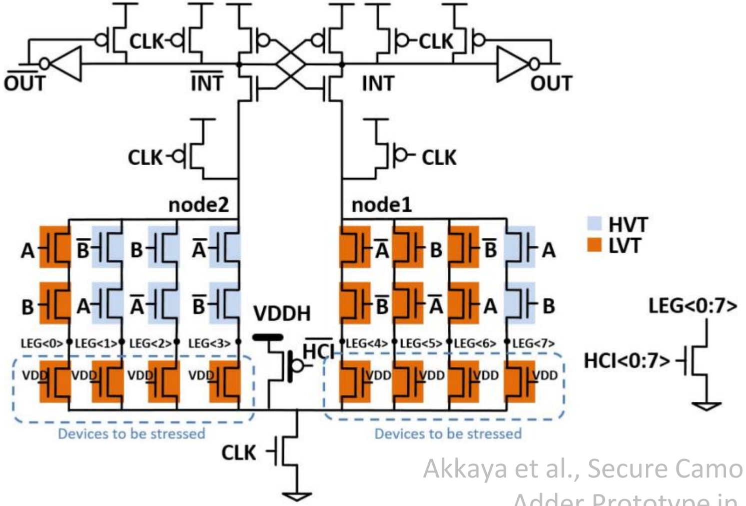
Side view of a gate with dummy contacts

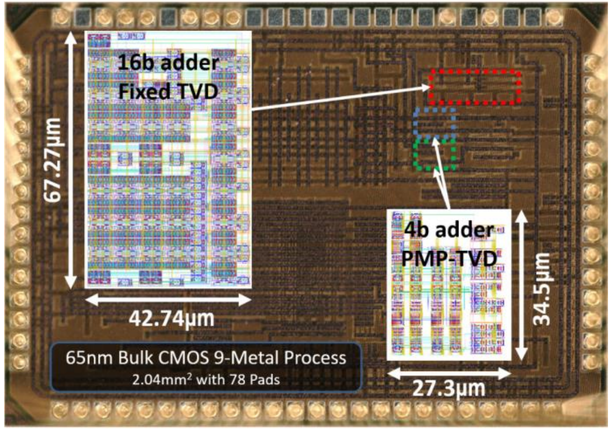


Rajendran et al.: Security Analysis of Integrated Circuit Camouflaging, Proc. Comp. Comm. Sec., 2013, 709-720

FEOL-Centric Layout Camouflaging

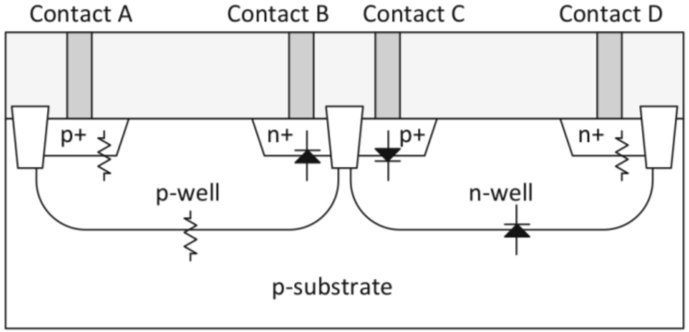
- Threshold-dependent gates, e.g., NAND-NOR-XOR in [Akkaya-ISSCC18]
  - Post-manufacturing configurability, unlike static camouflaging
  - PPA cost of 9.2X, 6.6X, 7.3X over 2-input NAND gate
  - Doping can be reverse-engineered using SEM (PVC) or careful etching

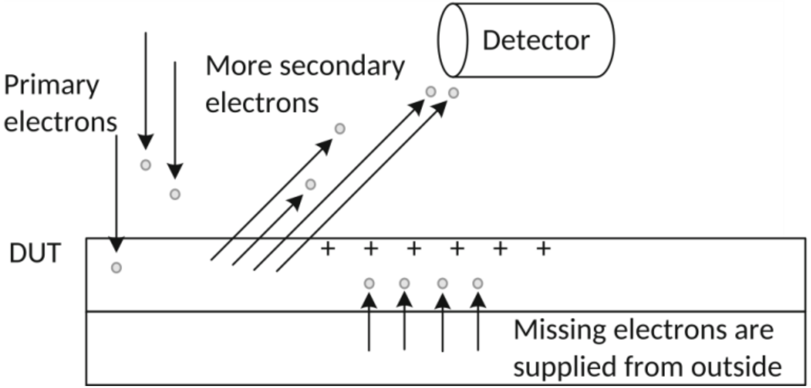


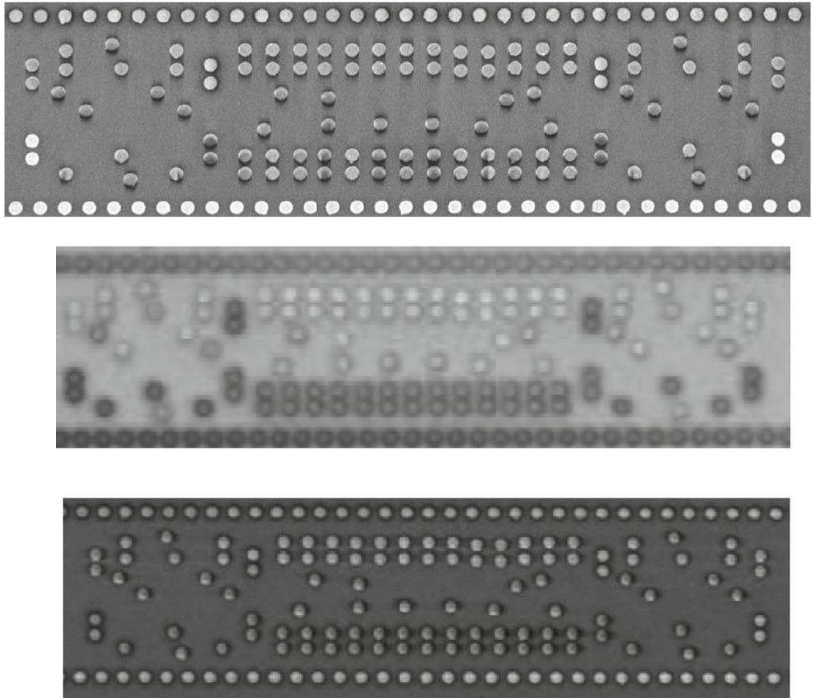


Akkaya et al., Secure Camouflaged Logic Family Using PostManufacturing Programming with a 3.6GHz Adder Prototype in 65nm CMOS at 1V Nominal VDD, Proc. Int. Sol.-St. Circ. Conf., 2018

Scanning Electron Microscopy Passive Voltage Contrast



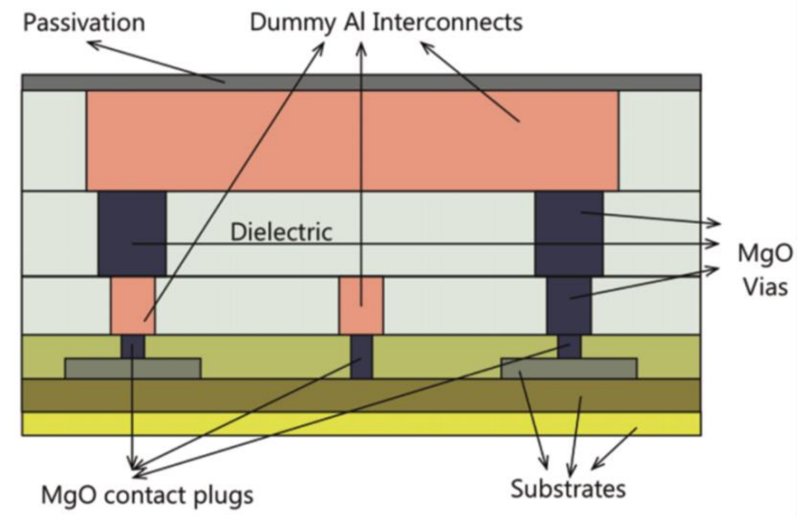




Sugawara et al.: Reversing stealthy dopant-level circuits, J. Cryptogr. Eng., 2015

BEOL-Centric Layout Camouflaging

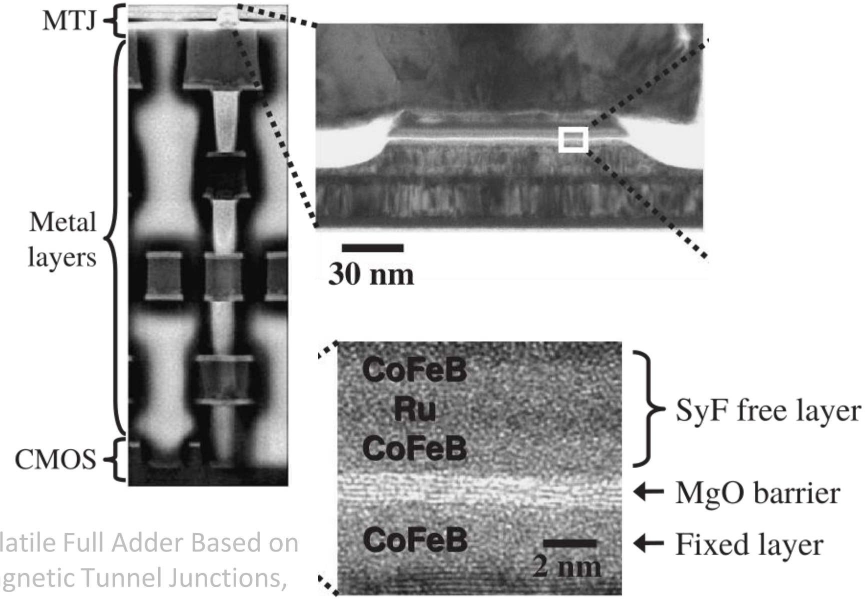
- Dummy vias, wires in [Chen-DFTS15], [Malik-ISVLSI15], [Patnaik-ICCAD17]
- 👍 Simple to manufacture – only BEOL masks affected, any FEOL compatible
- 👍 No inherent gate-level cost
  - 👍 Full-chip camouflaging: SAT attack hindered by scalability issue
- BEOL materials: Mg/MgO vias in [Chen-DFTS15], [Patnaik-ICCAD17]



Chen et al.: Chip-level anti-reverse engineering using transformable interconnects, Proc. Int. Symp. Def. Fault Tol. in VLSI Nanotech. Sys., 2015, 109-114

BEOL-Centric Layout Camouflaging

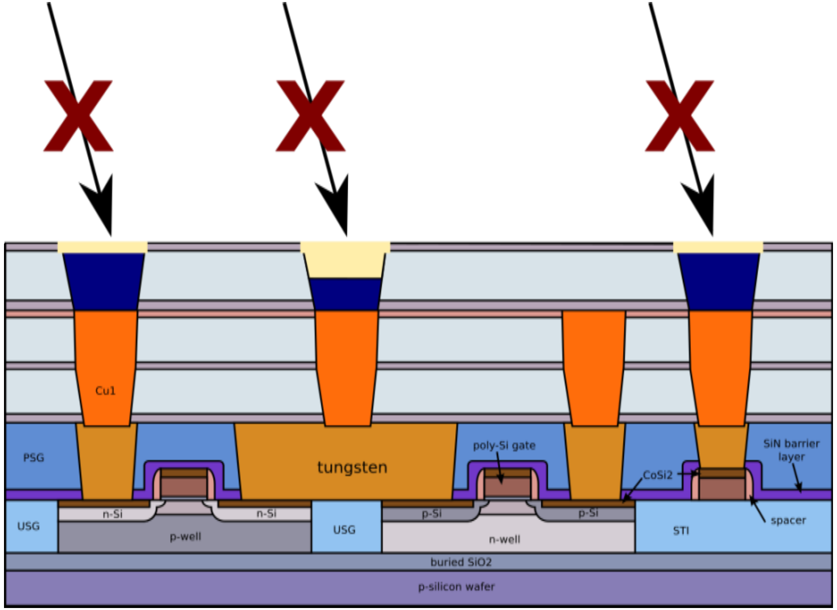
- Dummy vias, wires in [Chen-DFTS15], [Malik-ISVLSI15], [Patnaik-ICCAD17]
- 👍 Simple to manufacture – only BEOL masks affected, any FEOL compatible
- 👍 No inherent gate-level cost
  - 👍 Full-chip camouflaging: SAT attack hindered by scalability issue
- BEOL materials: Mg/MgO vias in [Chen-DFTS15], [Patnaik-ICCAD17]
  - 👍 Mg/MgO used in CMOS processes (for MTJs, Damascene process, …)



Matsunaga et al.: Fabrication of a Nonvolatile Full Adder Based on Logic-in-Memory Architecture Using Magnetic Tunnel Junctions, Applied Physics Express, 2008, 1, 091301

BEOL-Centric Layout Camouflaging

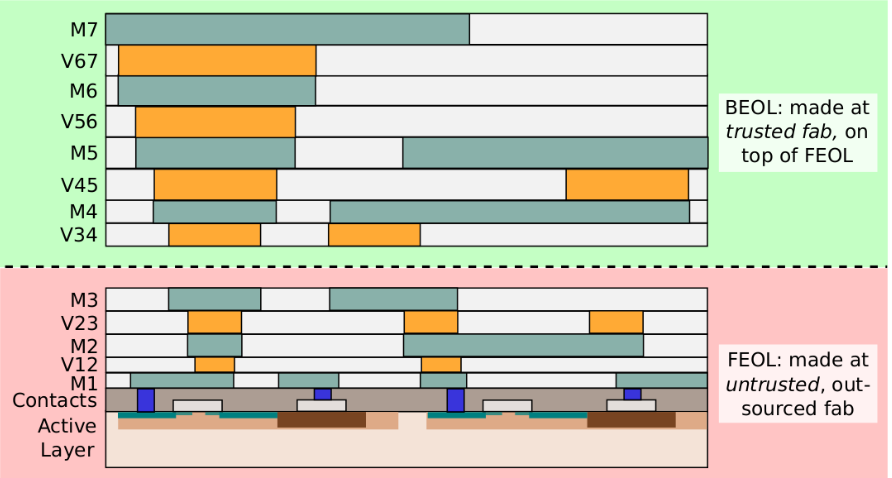
- Dummy vias, wires in [Chen-DFTS15], [Malik-ISVLSI15], [Patnaik-ICCAD17]
- 👍 Simple to manufacture – only BEOL masks affected, any FEOL compatible
- 👍 No inherent gate-level cost
  - 👍 Full-chip camouflaging: SAT attack hindered by scalability issue
- BEOL materials: Mg/MgO vias in [Chen-DFTS15], [Patnaik-ICCAD17]
  - 👍 Mg/MgO used in CMOS processes (for MTJs, Damascene process, ...)
  - 👍 Difficult to reverse engineer: Mg oxidizes
  - 👍 Charge-based SEM may fail as well

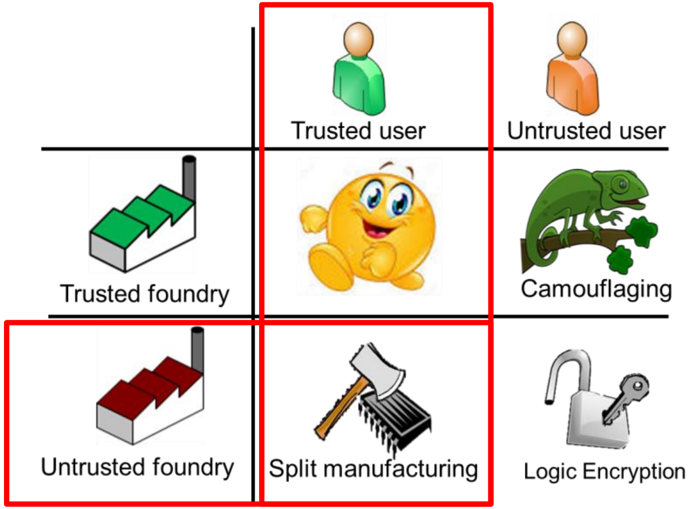


Derived from https://commons.wikimedia.org/wiki/File:Cmos-chip_structure_in_2000s_(en).svg

Basics of Split Manufacturing

- Split the design process into multiple stages
  - Typically split into FEOL and BEOL
  - Good support of economics-driven supply chain


M7
V67
M6
V56
M5
V45
M4
V34
BEOL: made at *trusted fab*, on top of FEOL
M3
V23
M2
V12
M1
Contacts
Active Layer
FEOL: made at *untrusted*, out-sourced fab

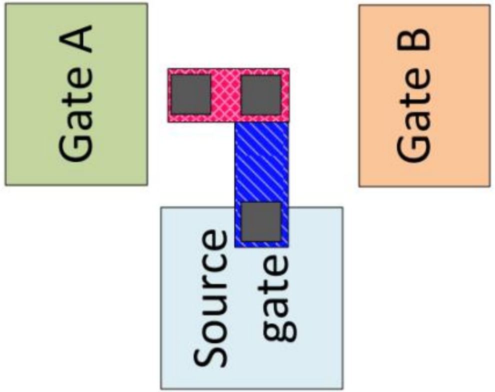


⚠ Trade-off for security and practicability (split layer, BEOL requirements, wafer handling)

⚠ Prone to analytical attacks

Knechtel et al., Protect Your Chip Design Intellectual Property: An Overview, COINS 2019

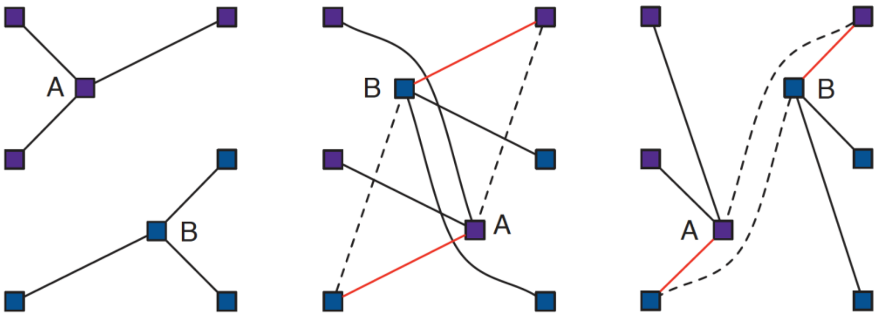
Attacks on Split Manufacturing – Proximity Attacks



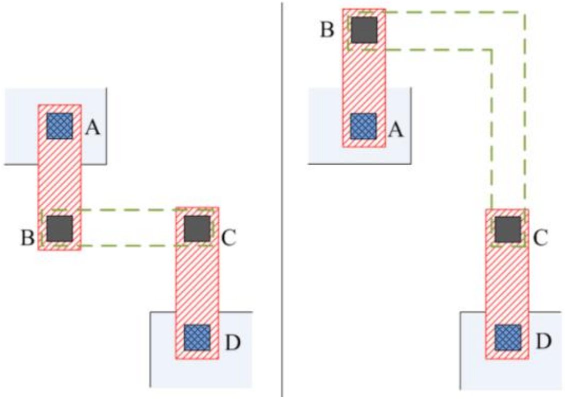
- CAD tools work holistically on FEOL and BEOL
- Infer missing BEOL connections from FEOL layout [Rajendran-DATE13]
  - Placement proximity, direction of dangling wires
- Additional hints, various attack implementations
  - Load capacitance, no combinatorial loops, timing constraints [Wang-DAC16]
  - Routing proximity, estimated routing congestion [Magana-ICCAD16]
  - Machine-learning based attack [Wang17-ICCAD, Zhang18-DAC, Li19-DAC]

Defense Schemes

- Placement perturbation [Wang-DAC16]
  - ⚠ Selective, small-scale use – proximity attack rate at 92%
- Routing perturbation [Wang-ASPDAC17], [Magana-ICCAD16], [Feng-ICCAD17], [Patnaik-ASPDAC18]



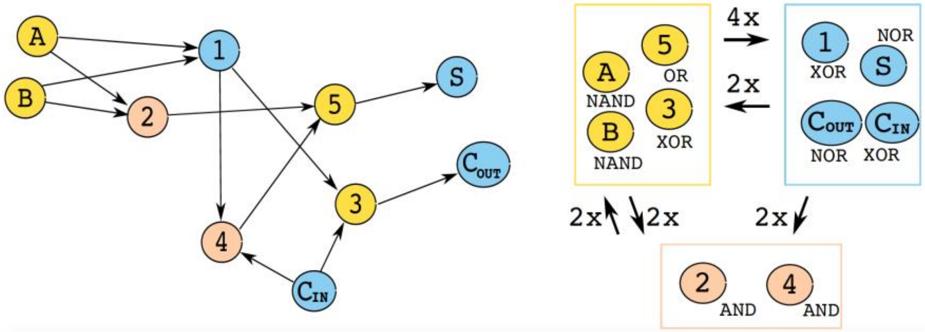
Wang et al.: The Cat and Mouse in Split Manufacturing, Proc. DAC, 2016



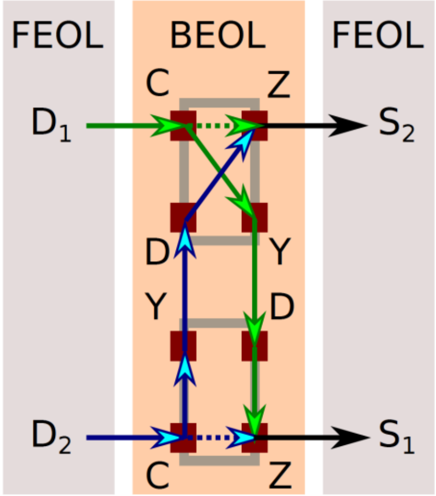
Wang et al.: Routing Perturbation for Enhanced Security in Split Manufacturing, Proc. ASP-DAC, 2017

Defense Schemes

- Placement and routing pertubation – “netlist restructuring” [Sengupta-ICCAD17, Patnaik-DAC18]
  - 👍 Better security, proximity attack success rate as low as 0%
  - ⚠ PPA for large-scale application



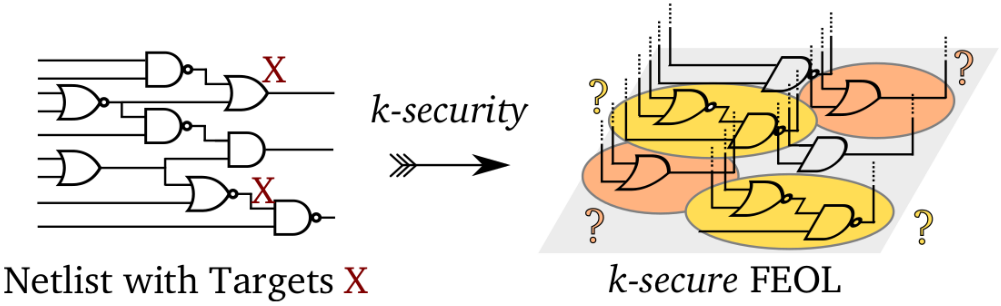
Sengupta et al.: Rethinking Split Manufacturing: An Information-Theoretic Approach with Secure Layout Techniques, Proc. ICCAD, 2017

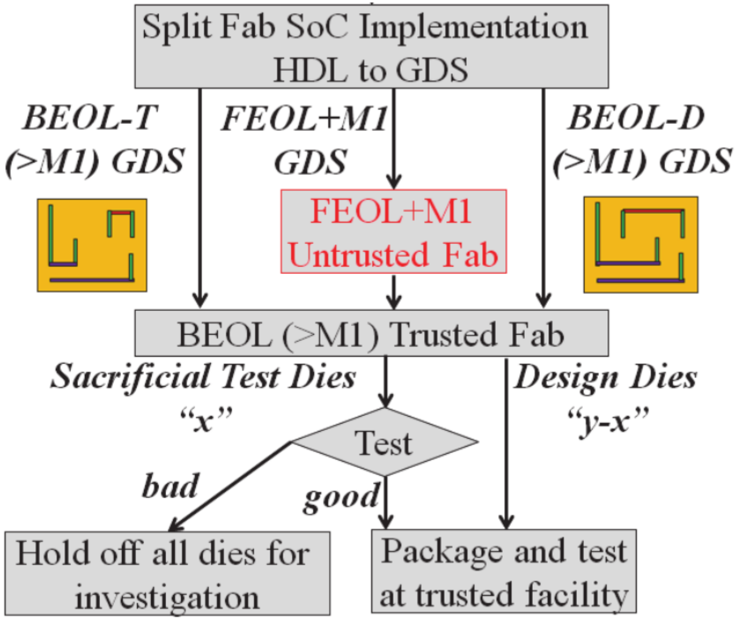


Patnaik et al.: Raise Your Game for Split Manufacturing: Restoring the True Functionality Through BEOL, Proc. DAC, 2018

Split Manufacturing for Protection Against Hardware Trojans

- When the fab attacker already knows the netlist, how to prevent Trojans? [Imeson13]
  - Layout cost
- When the fab attacker inserted some Trojan, how to test for? [Vaidyanathan14]
  - Commercial cost

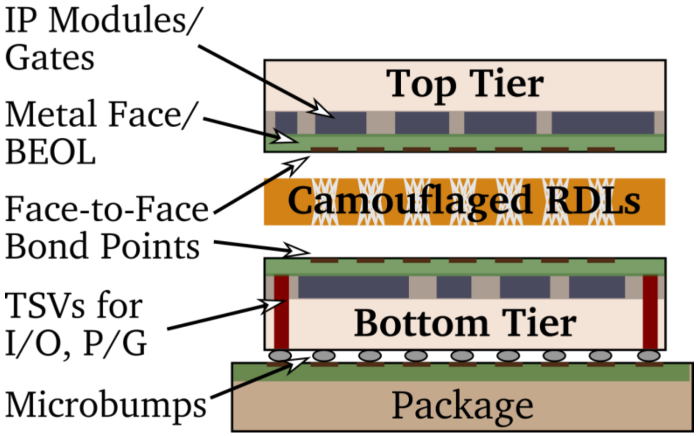


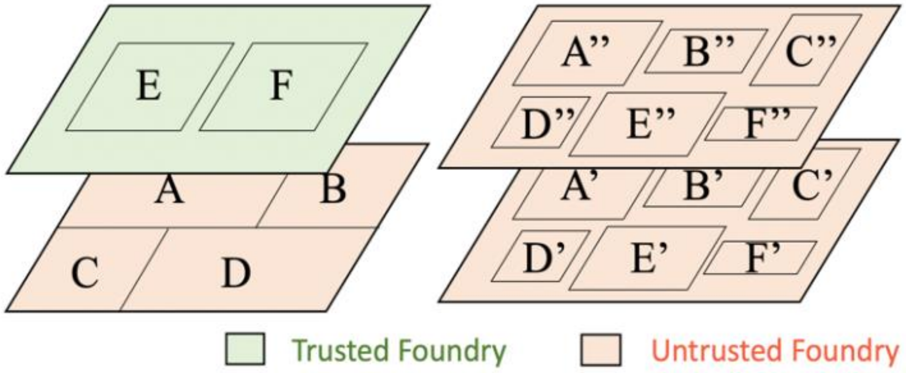


Vaidyanathan et al., Detecting Reliability Attacks During Split Fabrication Using Test-only BEOL Stack, DAC 2014, 156:1-156:6

Extending Split Manufacturing by 3D Integration

- Prior art: high layout cost, commercial cost, protect only against fab
- “Best of both worlds”: split manufacturing and BEOL camouflaging
  - Security-driven “3D split” into two (or more) tiers

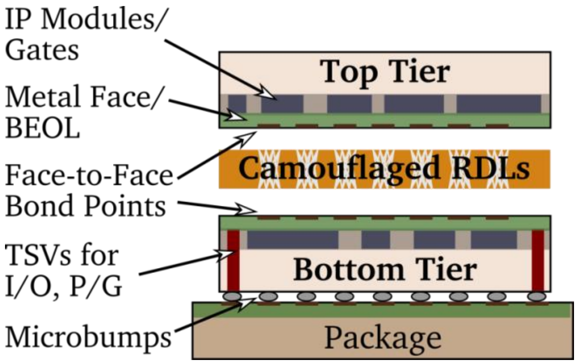


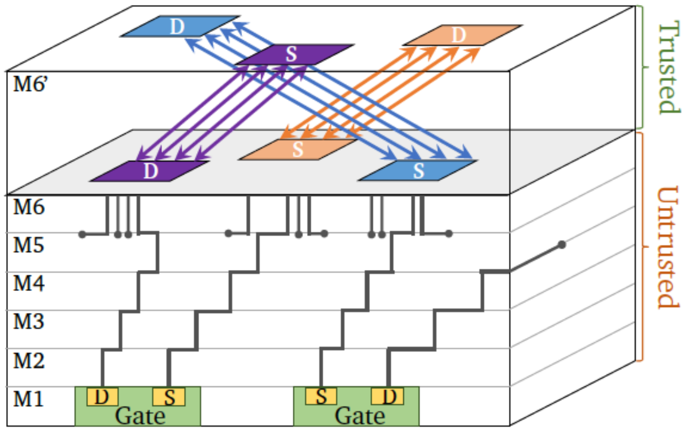


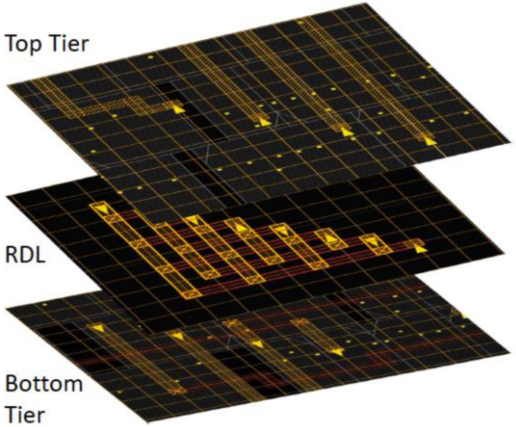
Patnaik et al., Best of Both Worlds: Integration of Split Manufacturing and Camouflaging into a Security-Driven CAD Flow for 3D ICs
Proc. IEEE/ACM Int. Conf. on Computer-Aided Design (ICCAD), 2018, 8:1-8:8

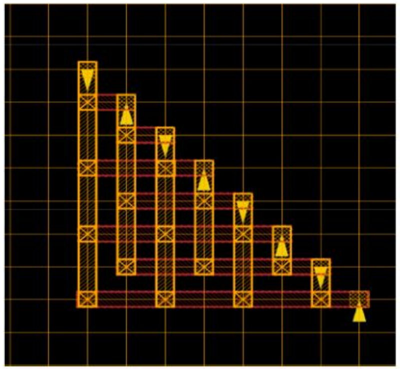
Extending Split Manufacturing by 3D Integration

- Split manufacturing and BEOL camouflaging
  - Security-driven “3D split” into two (or more) tiers
  - Randomize and camouflage interconnects (RDLs)
  - Only trusted BEOL facility is required
  - Thwarts both malicious FEOL fabs and end-user







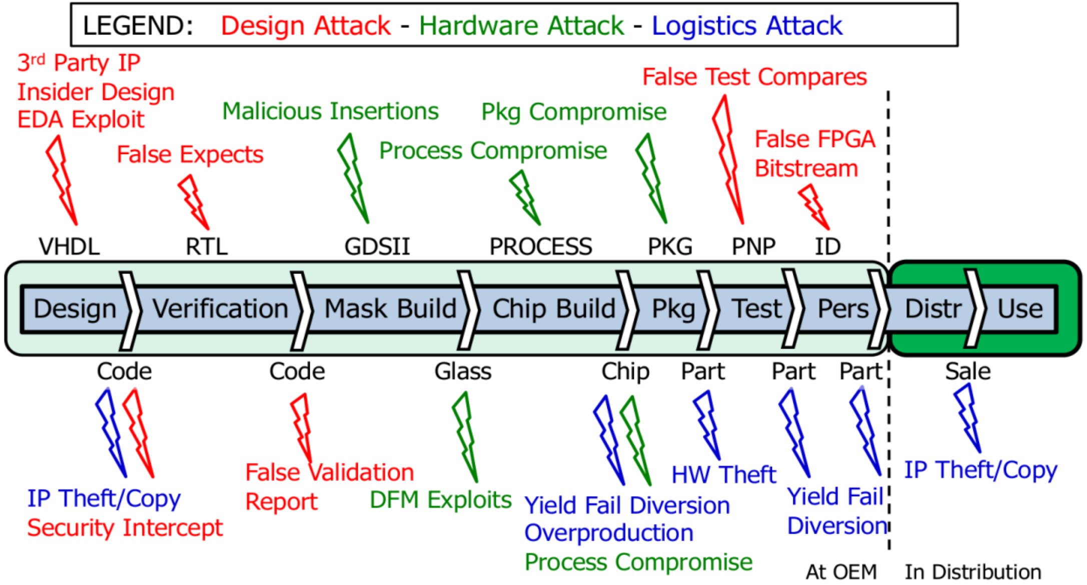


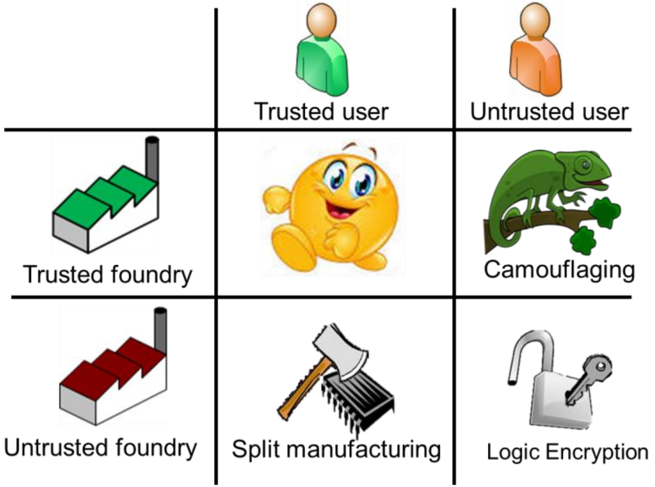
Obfuscated switchbox in RDL

Patnaik et al., Best of Both Worlds: Integration of Split Manufacturing and Camouflaging into a Security-Driven CAD Flow for 3D ICs
Proc. IEEE/ACM Int. Conf. on Computer-Aided Design (ICCAD), 2018, 8:1-8:8

Protect Your Chip Design Intellectual Property : An Overview

- Complex and globalized, outsourced IC supply chain
  - Need for protection of chip design IP
- Logic locking, layout camouflaging, and split manufacturing

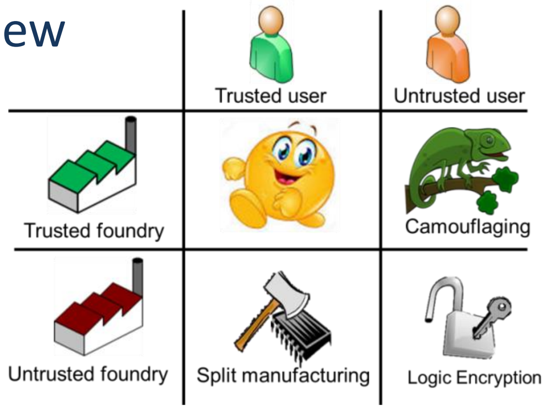


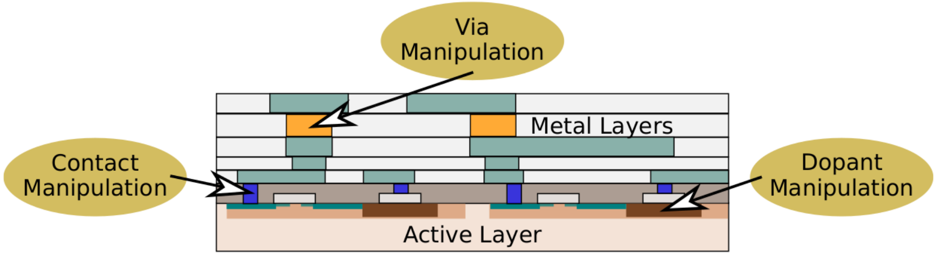


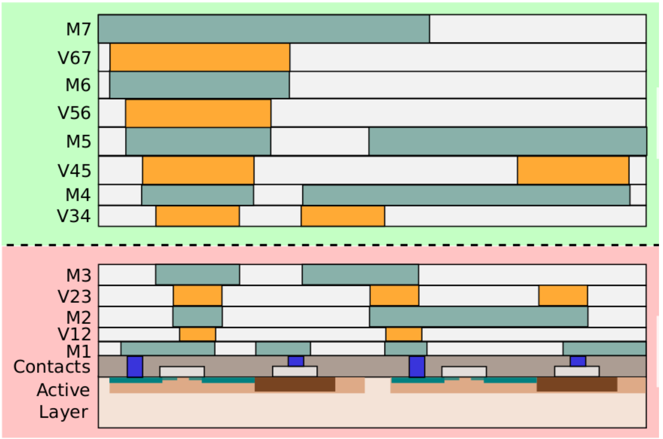
Knechtel et al., Protect Your Chip Design Intellectual Property: An Overview, COINS 2019

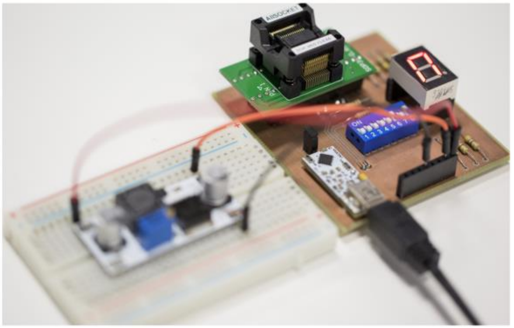
Protect Your Chip Design Intellectual Property : An Overview

- Complex and globalized, outsourced IC supply chain
  - Need for protection of chip design IP
- Logic locking, layout camouflaging, and split manufacturing

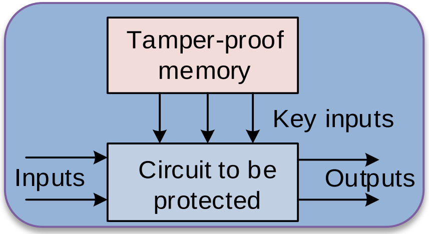








👍 Thank you!


Tamper-proof memory
Key inputs
Inputs
Circuit to be protected
Outputs