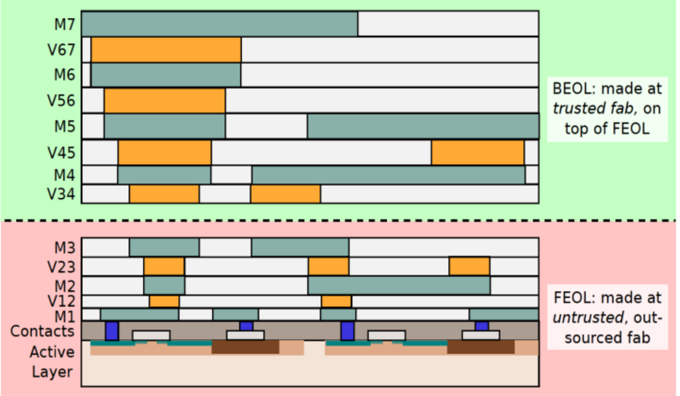
Concerted Wire Lifting: Enabling Secure and Cost-Effective Split Manufacturing

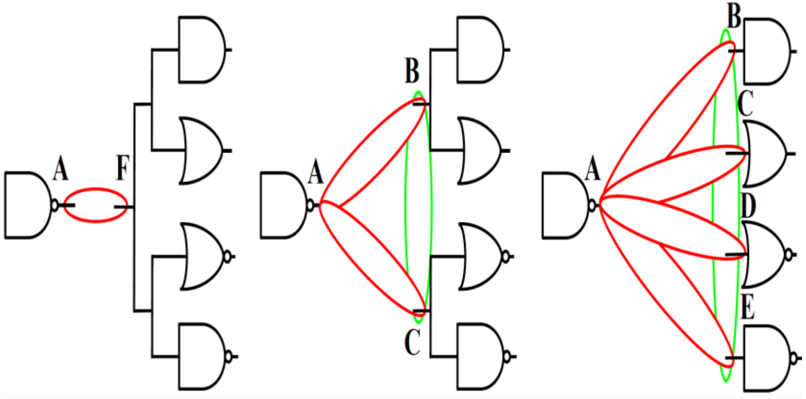
Satwik Patnaik, Johann Knechtel, Mohammed Ashraf, and Ozgur Sinanoglu
{sp4012, johann, ma199, ozgursin}@nyu.edu

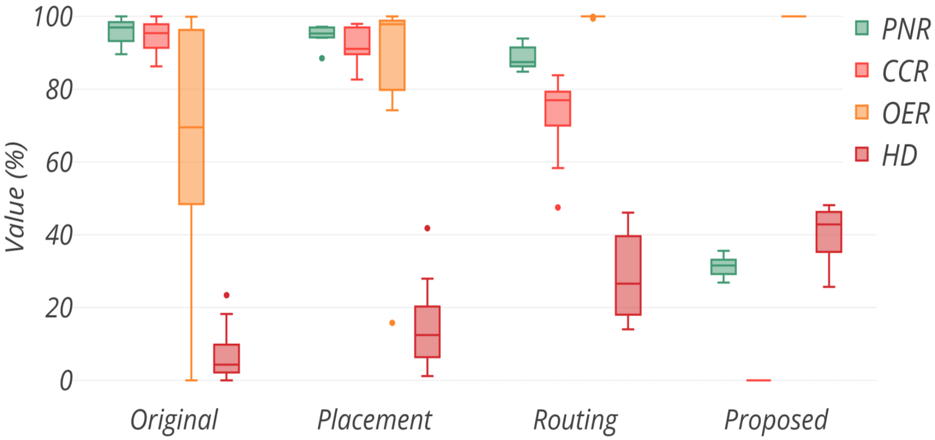
ASP-DAC 2018, January 23, Jeju Island, South Korea
Session 3D: Split Manufacturing, Logic Obfuscation and Camouflaging

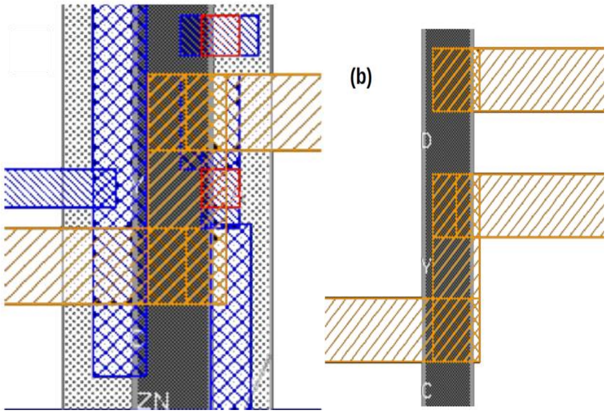
Outline

1. Background
2. Concept
3. Methodology
4. Evaluation
5. Summary

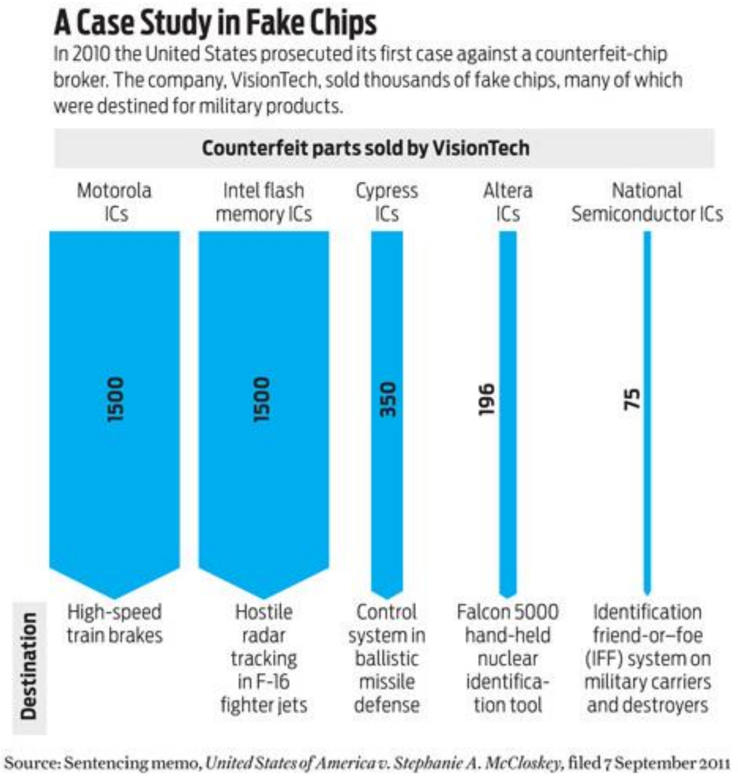


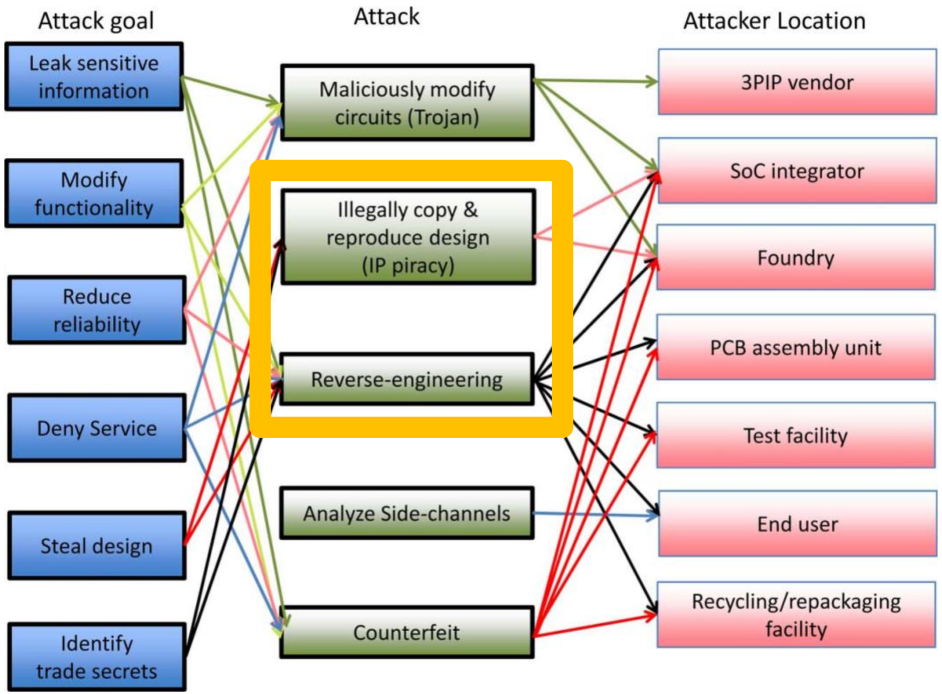






Growing Demand for Protection of Design IP and Chips

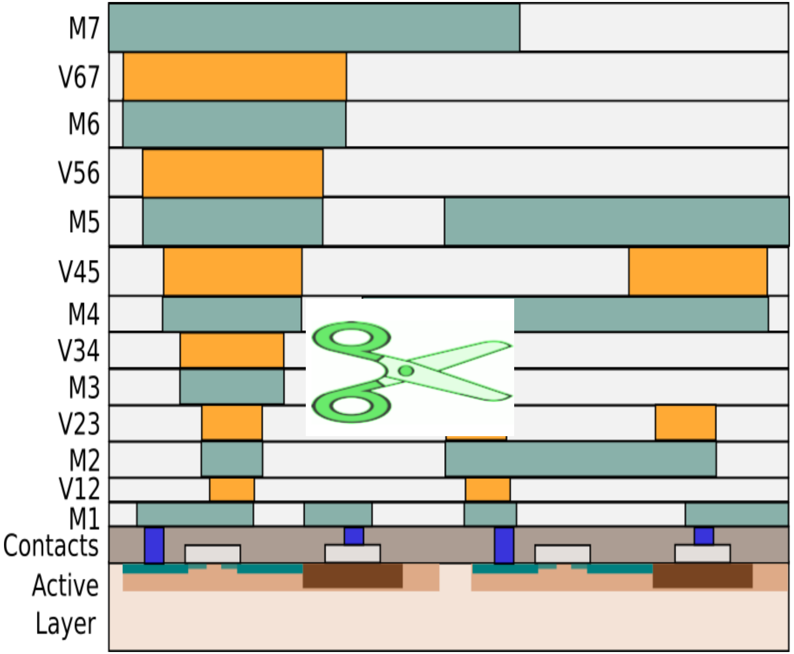


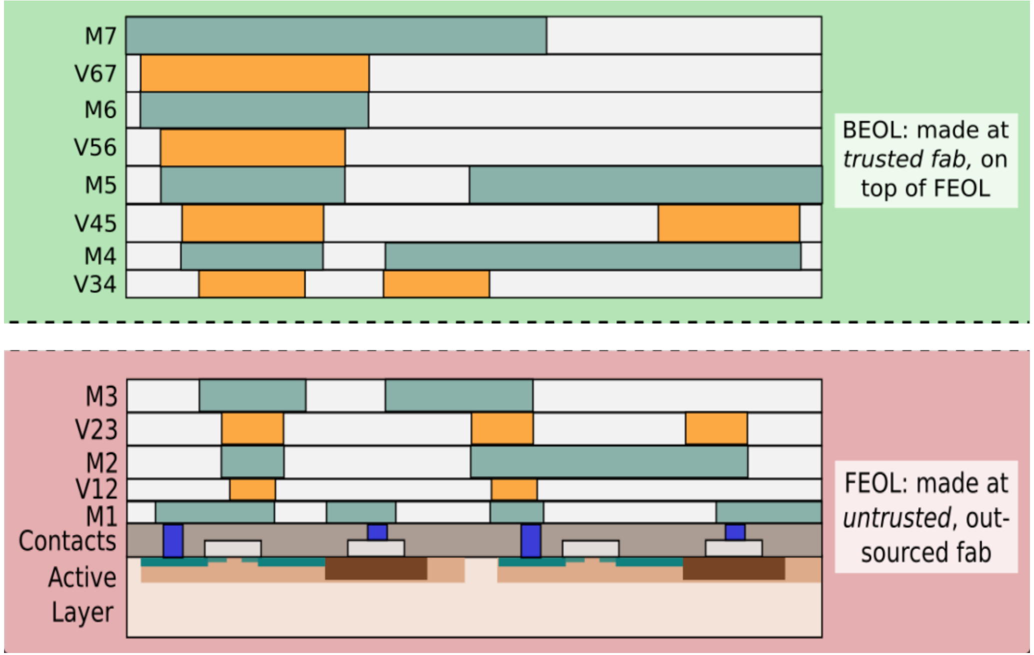


Left: IEEE Spectrum; Top: Rostami et al.: A Primer on Hardware Security: Models, Methods, and Metrics, Proc. IEEE, 2014, 102, 1283-1295

Protecting IP at chip level -- Split Manufacturing

- *Split the design into multiple parts*
  - Protects against IP piracy, unauthorized over-production, insertion of hardware Trojans
  - Most common embodiment – FEOL (Front-end-of-Line) and BEOL (Back-end-of-Line)

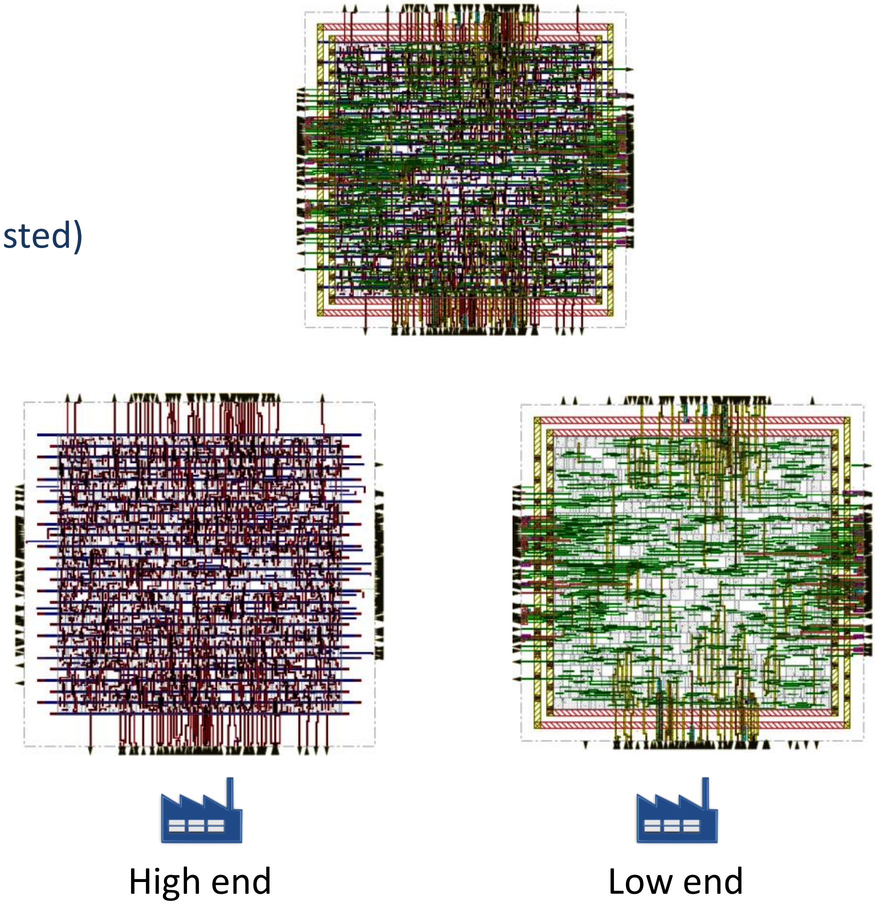




S. Patnaik et al., "Concerted Wire Lifting: Enabling Secure and Cost-Effective Split Manufacturing," ASP-DAC 2018

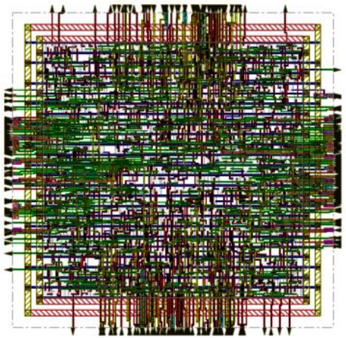
Split Manufacturing

- Based on the *asymmetry* of the metal layers
  - Typically M1-M3 (FEOL), M4 onwards (BEOL)
  - FEOL (high-end, untrusted) & BEOL (low-end, trusted)

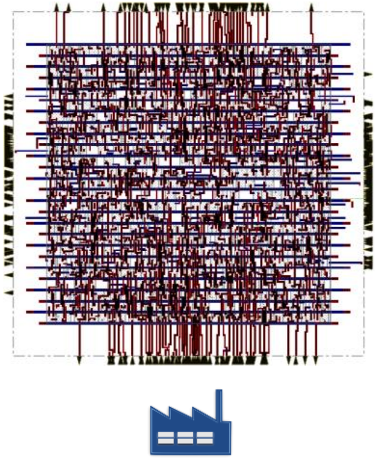


Split Manufacturing

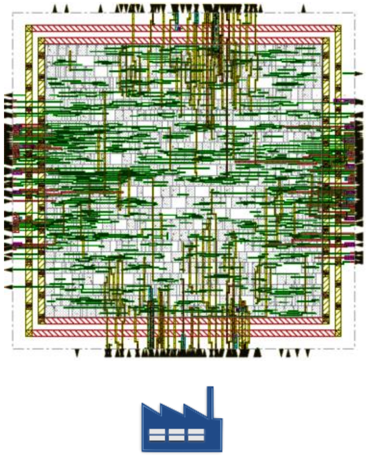
- Based on the *asymmetry* of the metal layers
  - Typically M1-M3 (FEOL), M4 onwards (BEOL)
  - FEOL (high-end, untrusted) & BEOL (low-end, trusted)



- Where to split?
  - Financial cost – security tradeoff
  - Lower metal layer split
    - ⚠ High financial cost
    - 👍 Attacks difficult -- Better security

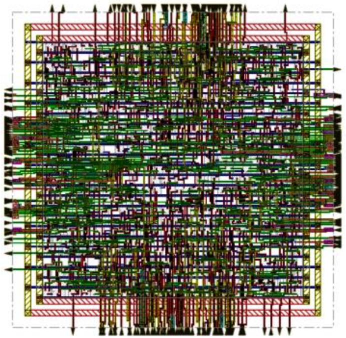


High end



Low end

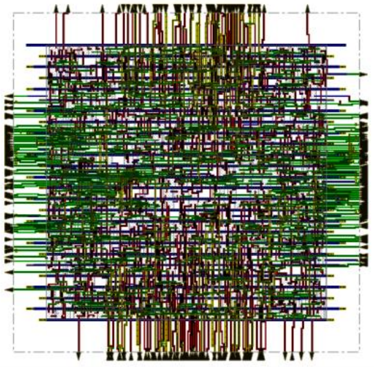
Split Manufacturing

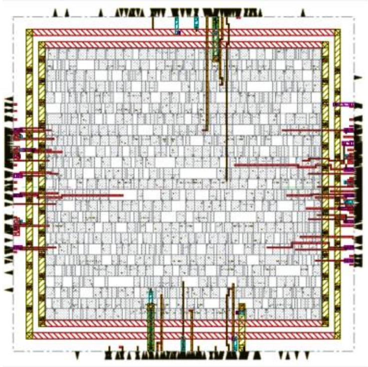


- Based on the *asymmetry* of the metal layers
  - Typically M1-M3 (FEOL), M4 onwards (BEOL)
  - FEOL (high-end, untrusted) & BEOL (low-end, trusted)

- Where to split?
  - Financial cost – security tradeoff
  - Lower metal layer split
    - ⚠ High financial cost
    - 👍 Attacks difficult -- Better security
  - Higher metal layer split
    - 👍 Less financial cost
    - ⚠ Attacks easier -- Lesser security

👍 *Higher split and better security?*



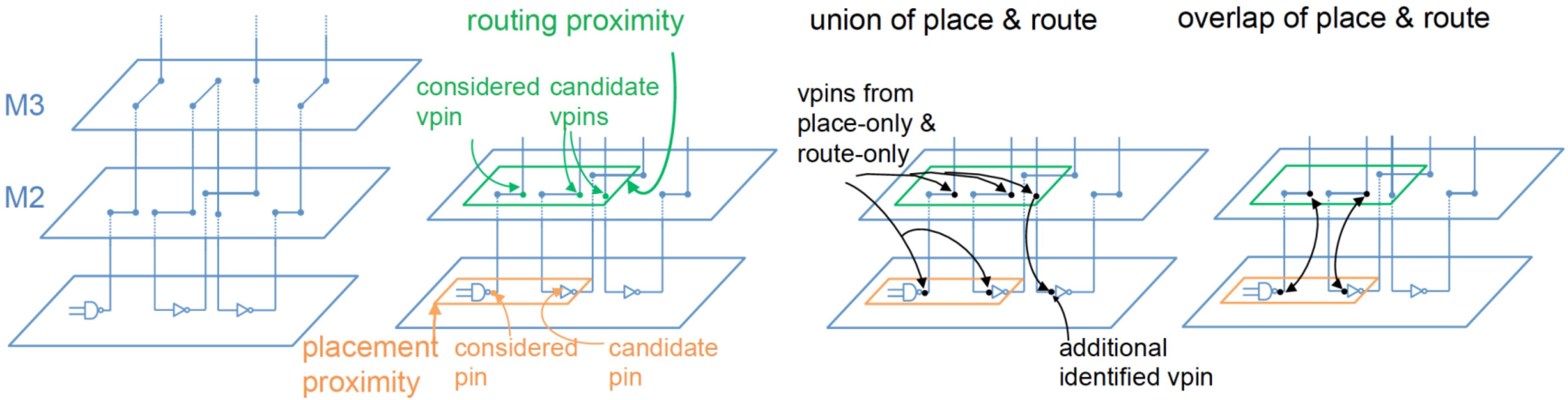


High end

Low end

Proximity Attack

- Infer missing BEOL connections from FEOL layout [Rajendran-DATE13]
  - Hints include placement proximity, direction of dangling wires [Wang-DAC16]
  - Load capacitance, non-formation of combinatorial loops, timing constraints
- Additional hints were explored by [Magana-ICCAD16]
  - Routing proximity, estimate routing congestion



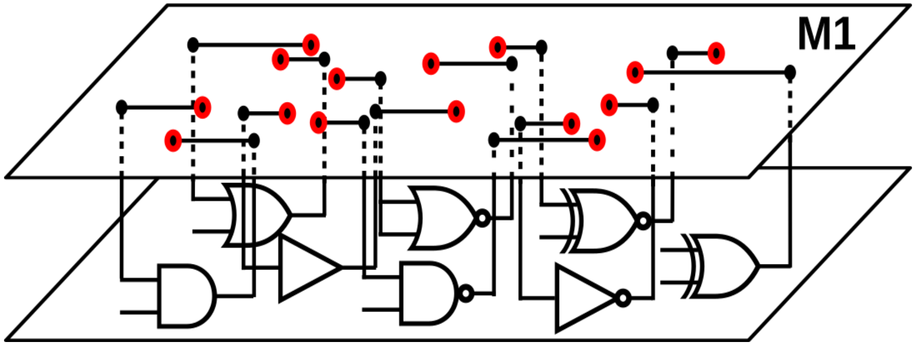
Magana et al.: Are Proximity Attacks a Threat to the Security of Split Manufacturing of Integrated Circuits?, Proc. ICCAD, 2016

Open Pins and Open Pin Pair (OPP)

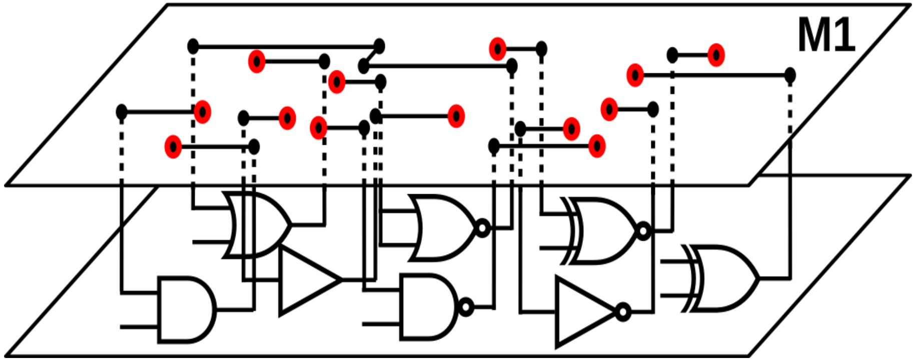
- Metal segment cut across FEOL/BEOL
  - Dangling wires unconnected *at least* from one end
  - Open ends indicate location of vias – open pins
  - Pairs of open pins – open pin pair (OPP)

Split after M1

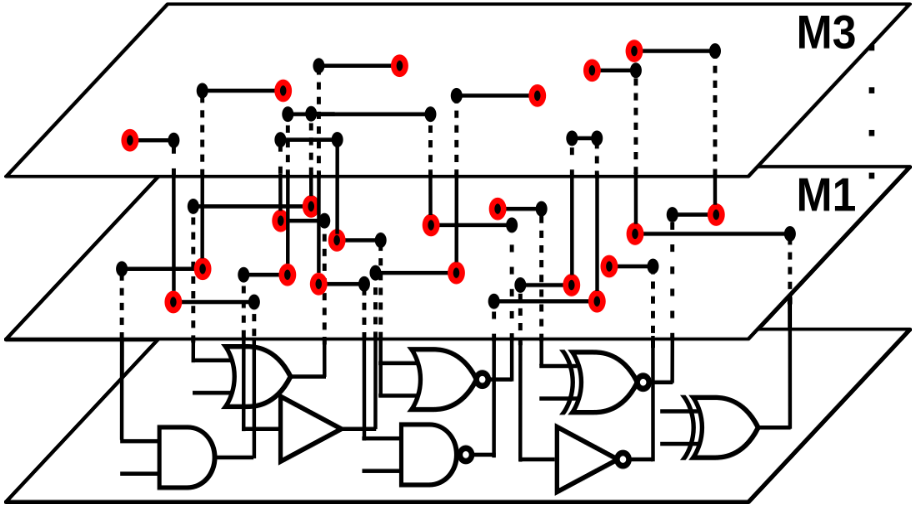
Original

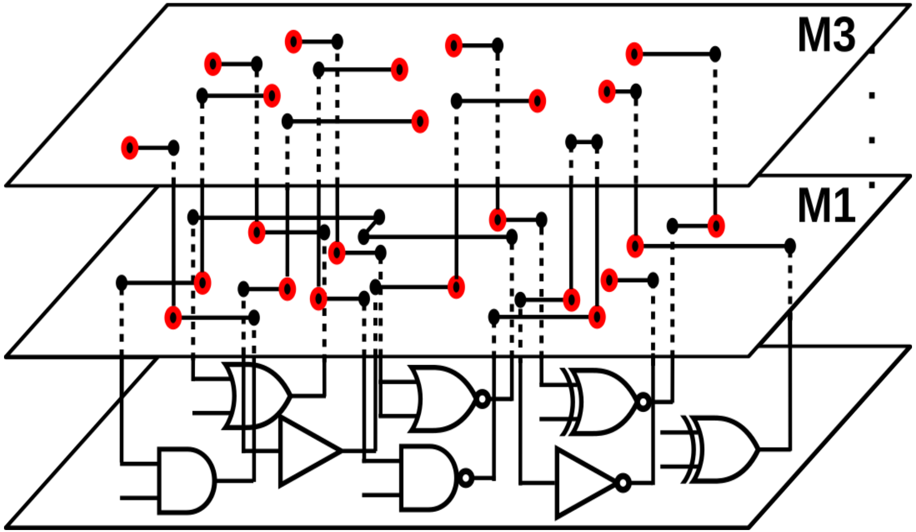


Naïve lifting



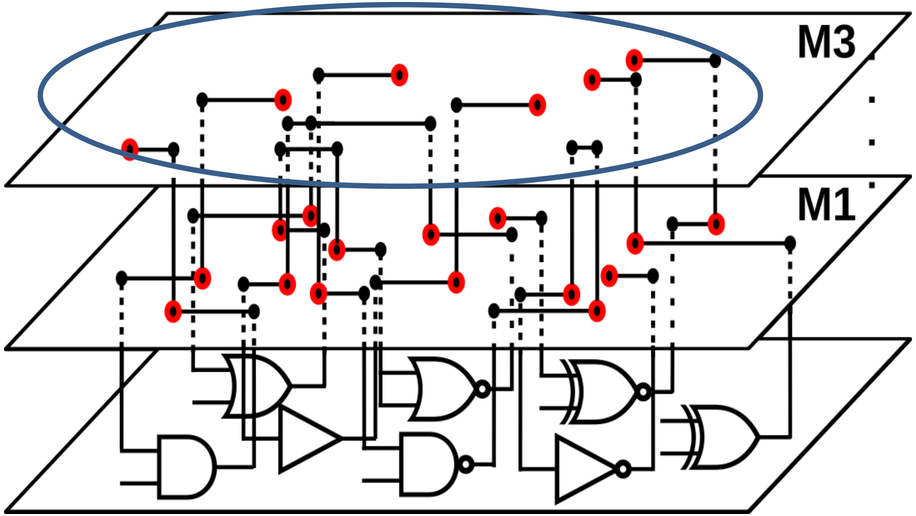
Split after M3

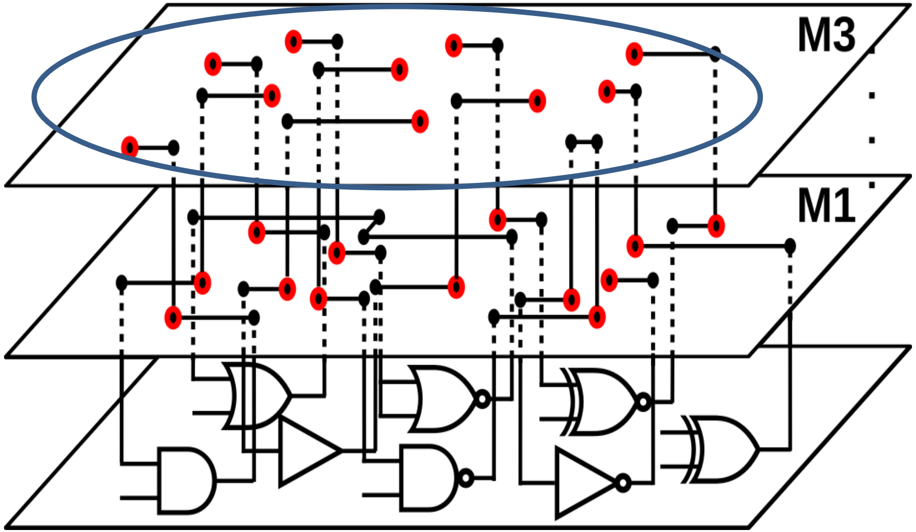




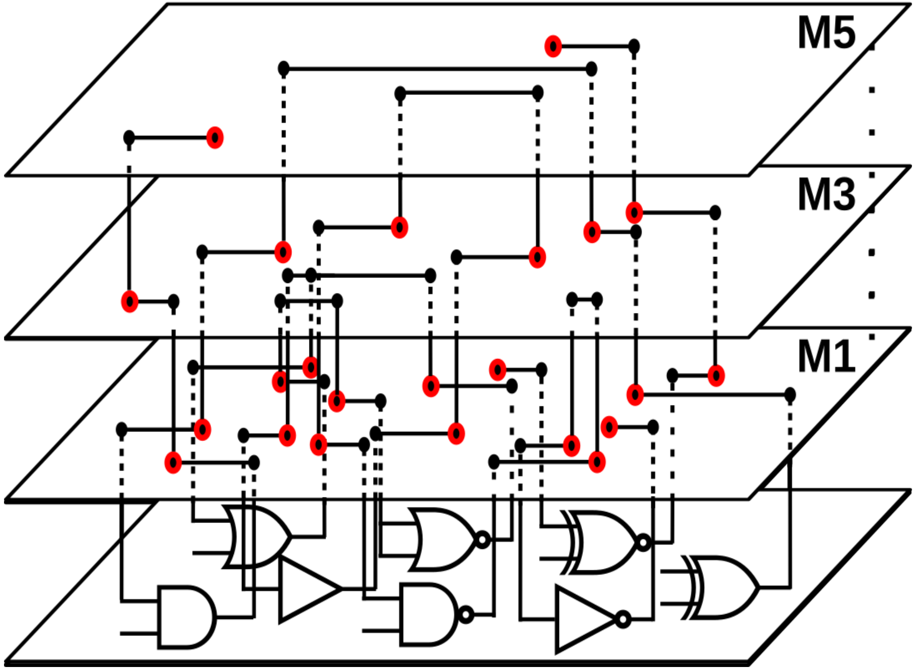
S. Patnaik et al., “Concerted Wire Lifting: Enabling Secure and Cost-Effective Split Manufacturing,” ASP-DAC 2018

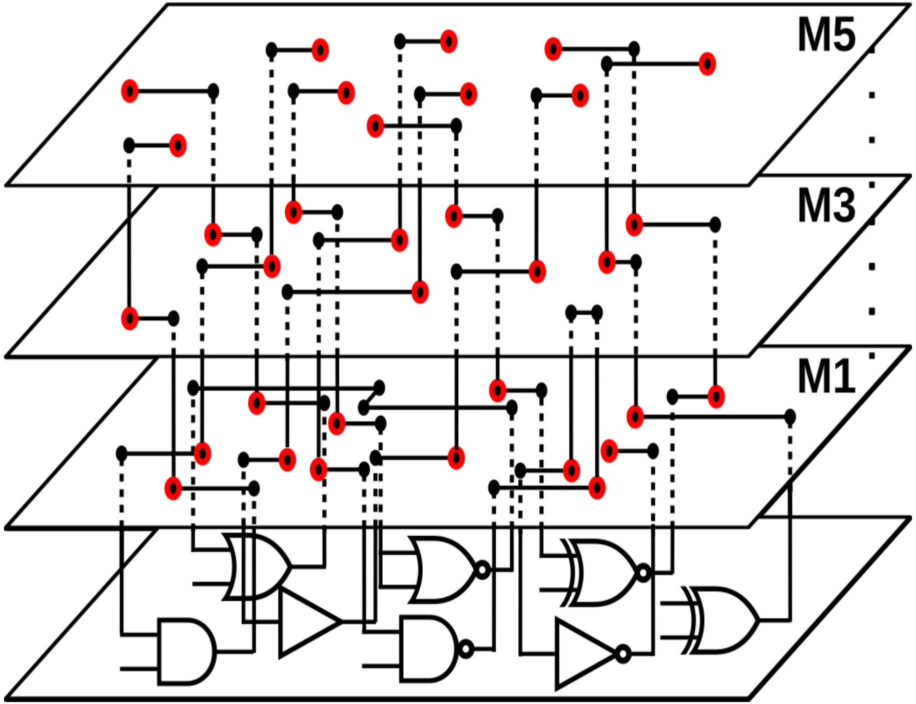
Split after M3



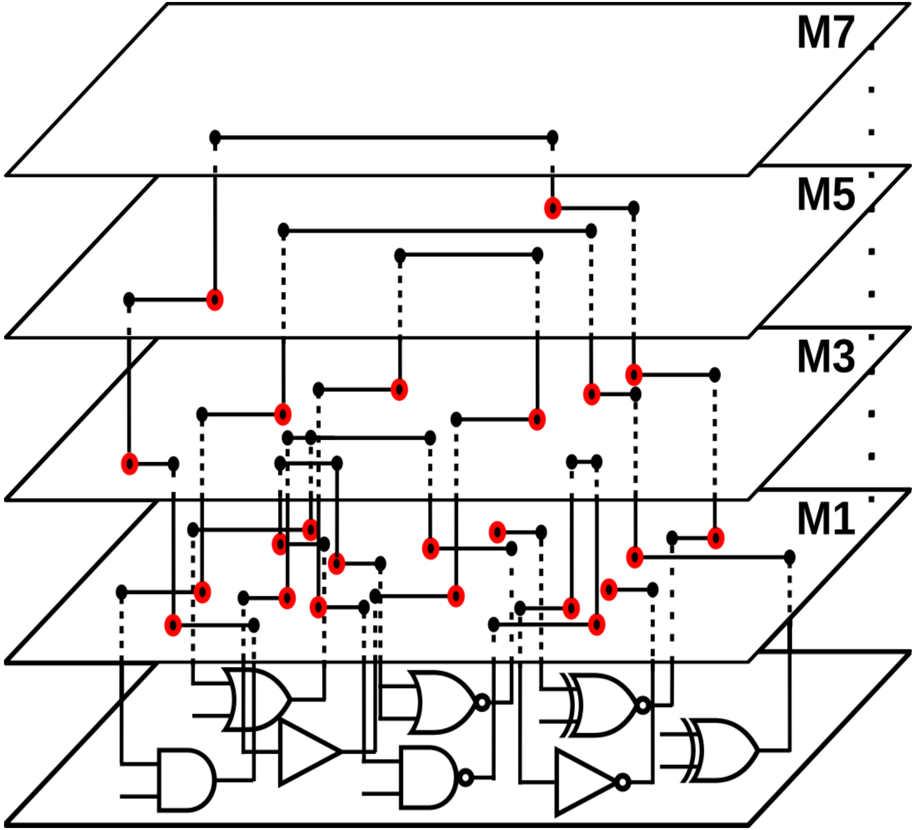


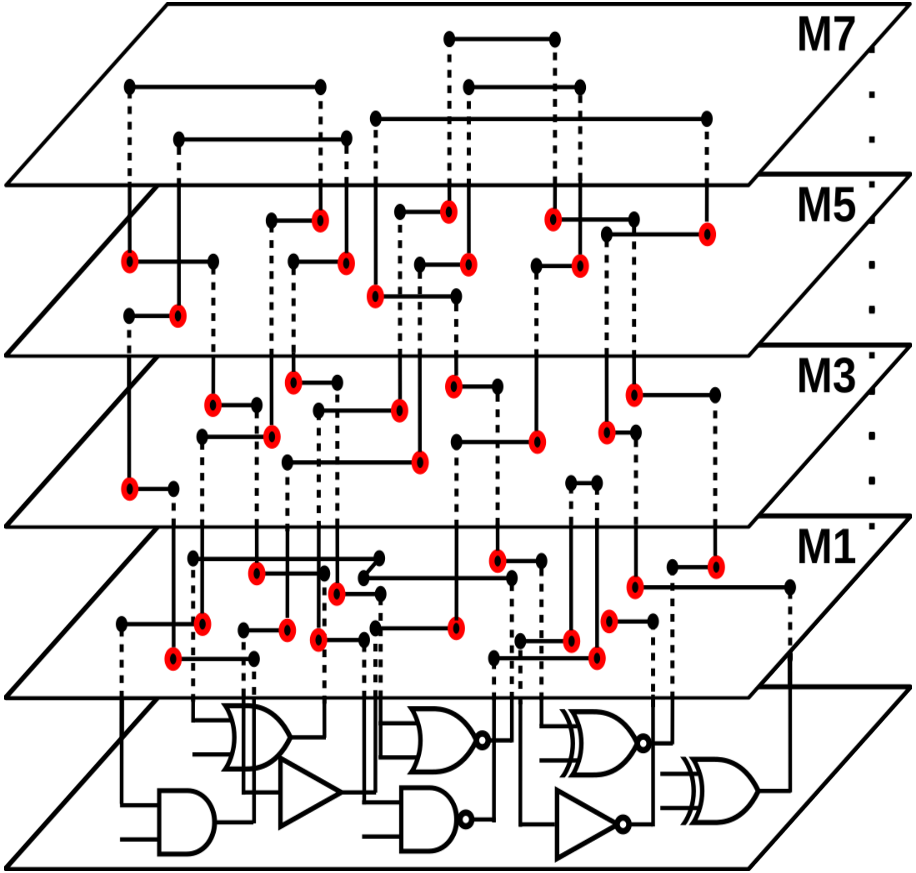
Split after M5





Final Layouts





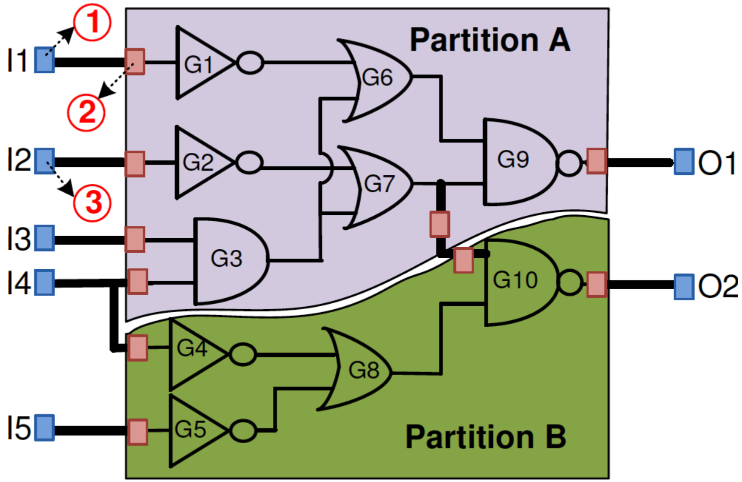
Evaluation of Attack Success

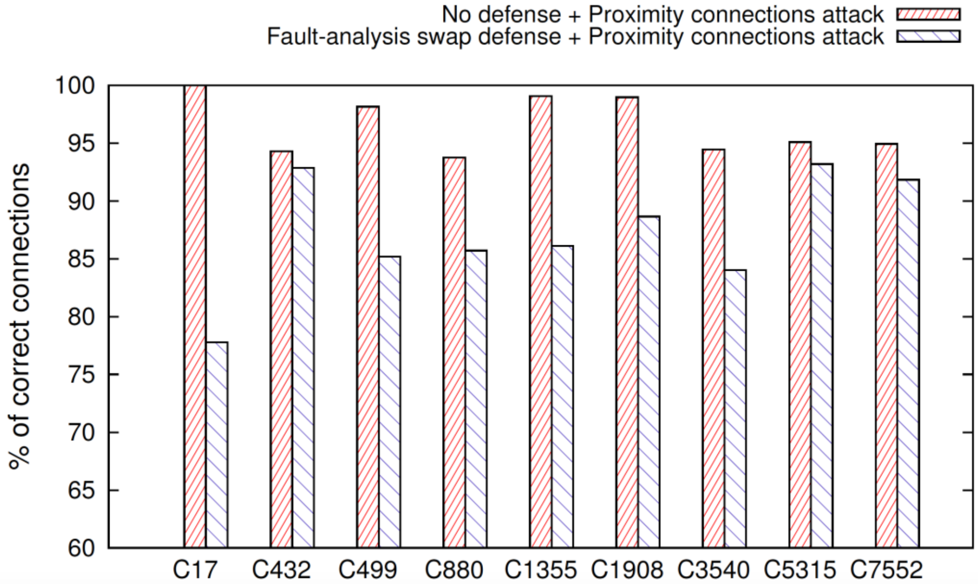
- Existing metrics
  - Correct Connection Rate (CCR) [Rajendran-DATE13]
  - Output Error Rate (OER) [Wang-DAC16]
  - Hamming Distance (HD)
  - ⚠ Do not quantify IP theft

- Proposed metric: Percentage of Netlist Recovery (PNR)
  - Correctly inferred connections over total nets
  - Quantifies structural similarity, accounts whole netlist
  - 100 protected nets, total 1000 nets, 20 nets inferred
    - CCR is 20%
  - 100 protected nets, total 1000 nets, *400 FEOL nets*, 20 nets inferred
    - CCR is 20% *but* PNR is 42%

Making Split Manufacturing Secure: Some Prior Art and Shortcomings

- Pin swapping
  - ⚠ Applicable only to hierarchical designs [Rajendran-DATE13]
  - ⚠ Performance overhead of 25%
  - ⚠ 87% CCR

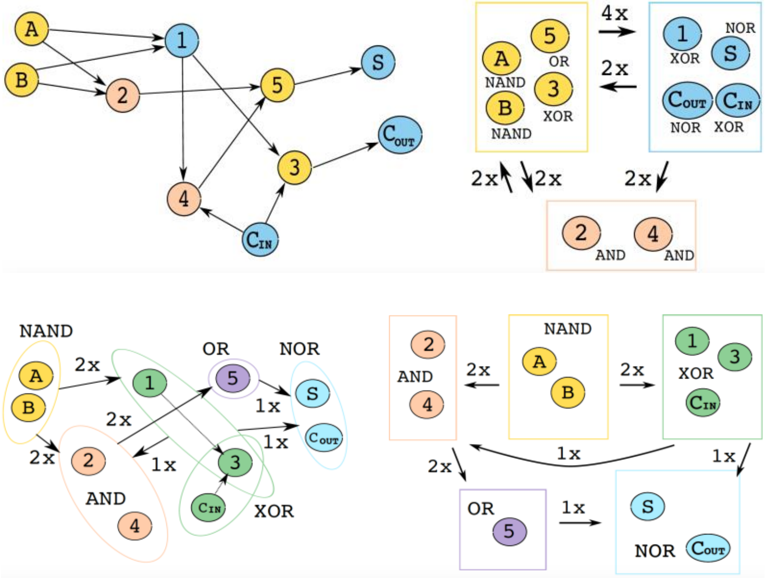




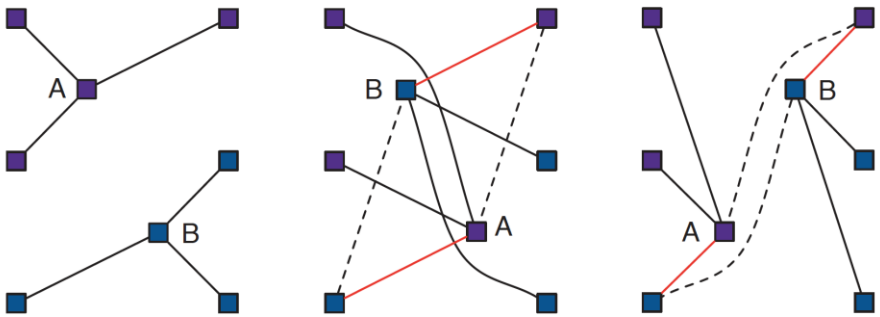
Rajendran et al.: Is Split Manufacturing Secure?, Proc. DATE, 2013

Making Split Manufacturing Secure: Some Prior Art and Shortcomings

- Placement perturbation
  - ⚠ Local movement of gates in [Wang-DAC16]
    - ⚠ Selective, small-scale use → eases proximity attacks
    - ⚠ CCR at 92%, PNR at 95%
  - ⚠ Netlist restructuring in [Sengupta-ICCAD17]
    - 👍 Better security than [Wang-DAC16], more OPPs
    - ⚠ High PPA costs, esp. large designs



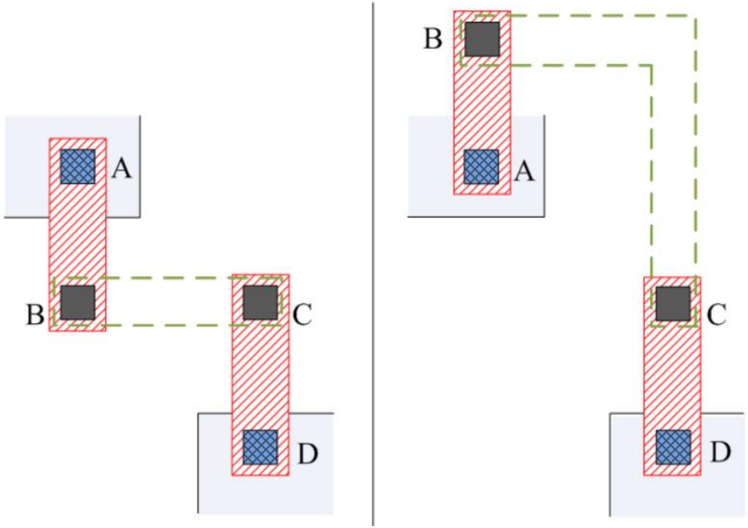
Sengupta et al.: Rethinking Split Manufacturing: An Information-Theoretic Approach with Secure Layout Techniques, Proc. ICCAD, 2017



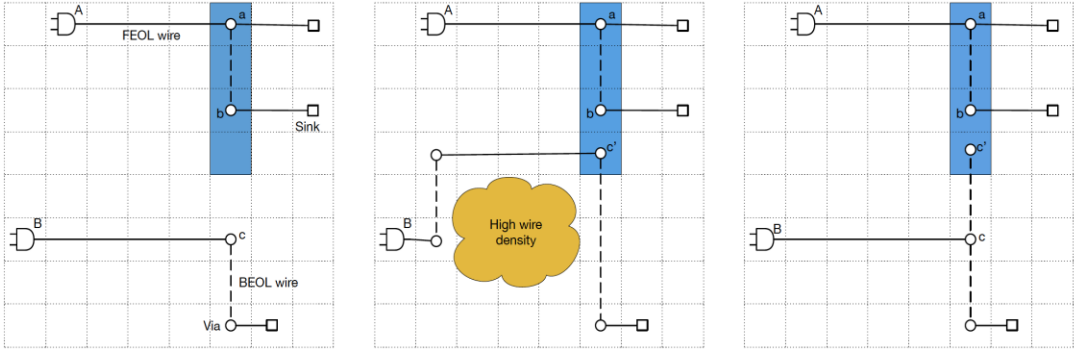
Wang et al.: The Cat and Mouse in Split Manufacturing, Proc. DAC, 2016

Making Split Manufacturing Secure: Some Prior Art and Shortcomings

- Routing perturbation in [Wang-ASPDAC17], [Magana-ICCAD16] and [Feng-ICCAD17]
  - ⚠ Few nets detoured in [Wang-ASPDAC17]
    - ⚠ Selective, small-scale use, less OPPs → eases proximity attacks
    - ⚠ CCR at 72%, PNR at 88%



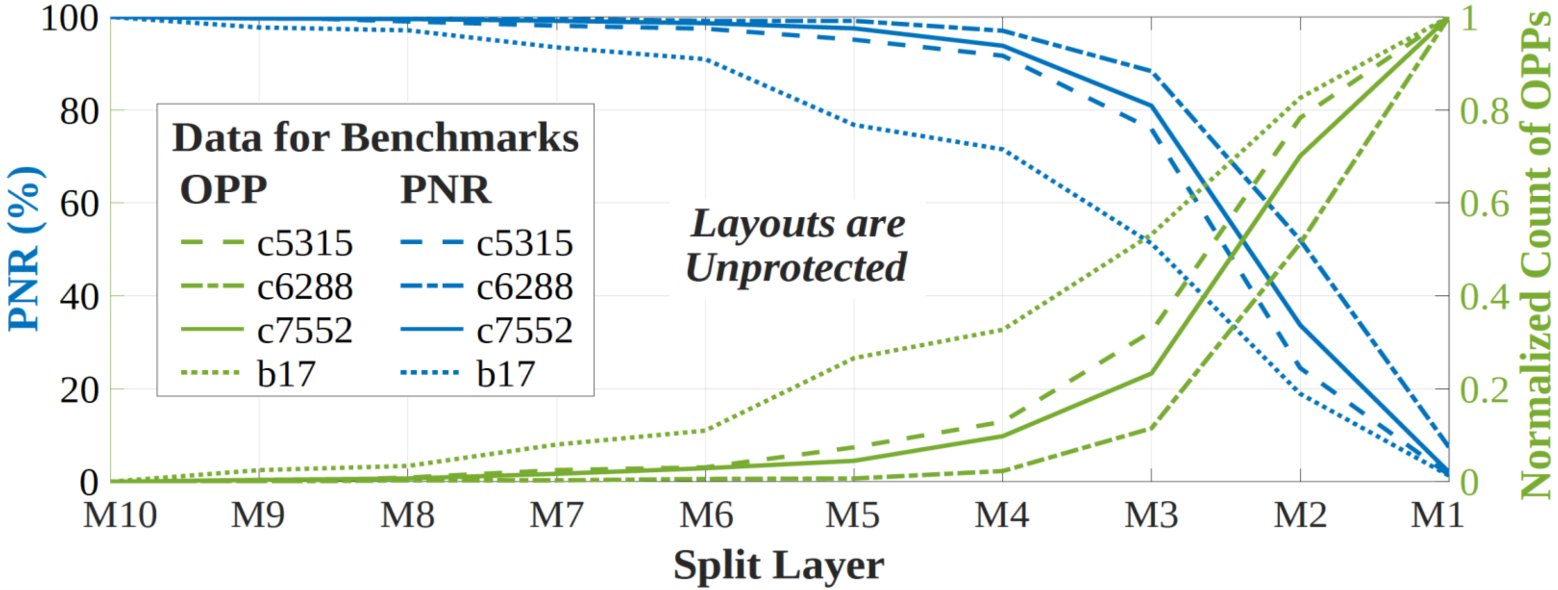
Wang et al.: Routing Perturbation for Enhanced Security in Split Manufacturing, Proc. ASP-DAC, 2017



Feng et al.: Making Split Fabrication Synergistically Secure and Manufacturable, Proc. ICCAD, 2017

Exploratory Experiments on Split Layers

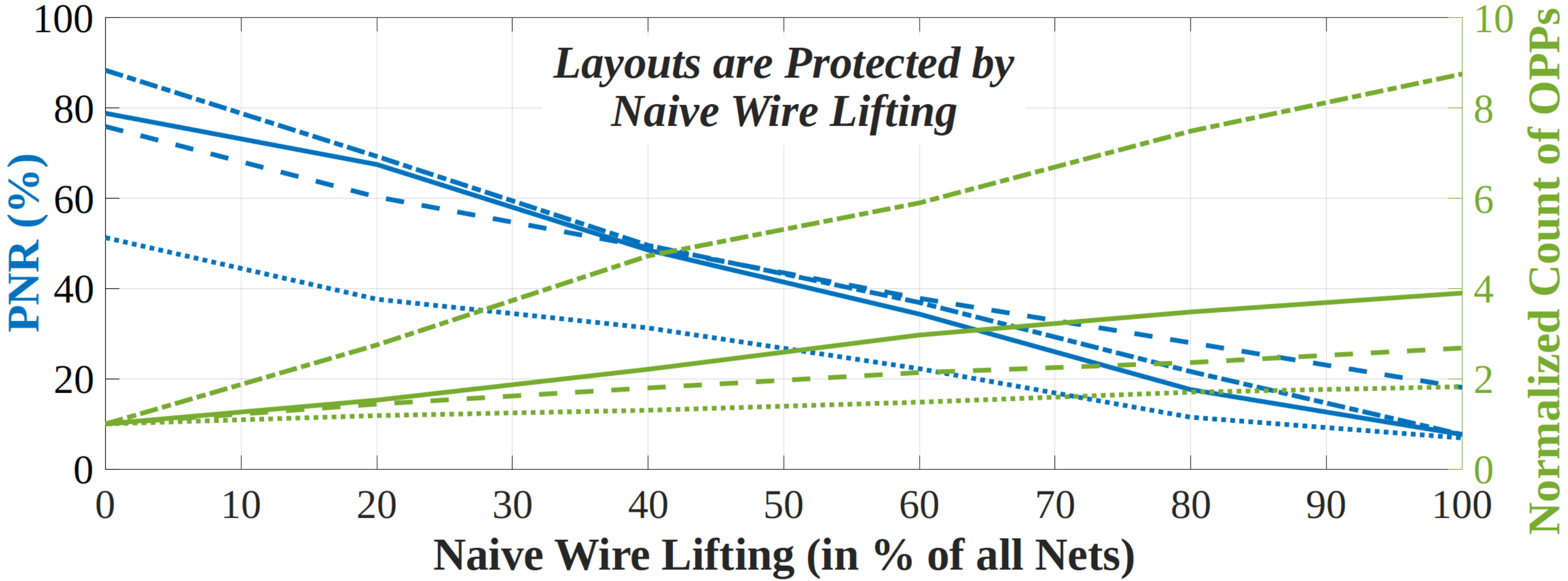
- Attacker observing fewer OPPs at FEOL
  - ⚠ Reduced search space
  - ⚠ Strongly reciprocal relations → Layouts split after higher layers, easier to attack



S. Patnaik et al., “Concerted Wire Lifting: Enabling Secure and Cost-Effective Split Manufacturing,” ASP-DAC 2018

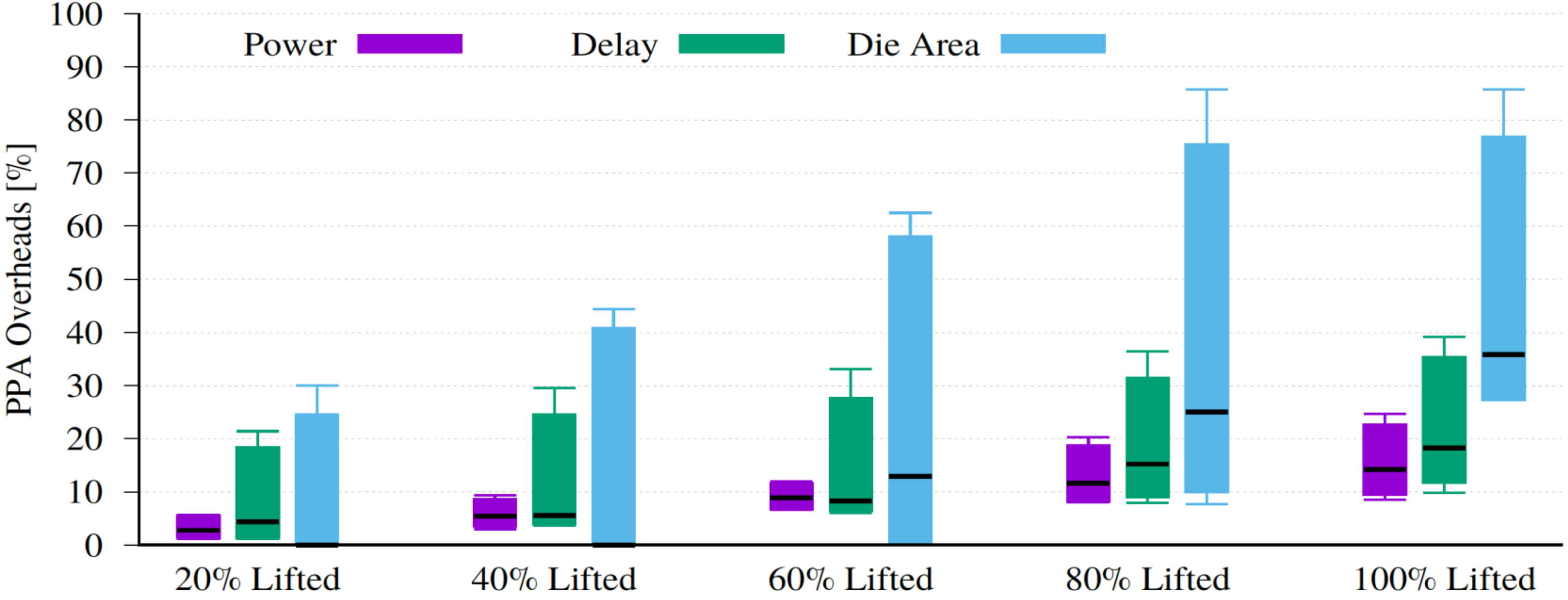
Exploratory Experiments on Naïve lifting

- Attacker observing large # of OPPs at FEOL
  - Increased search space
  - Layouts split at higher layers → difficult to attack



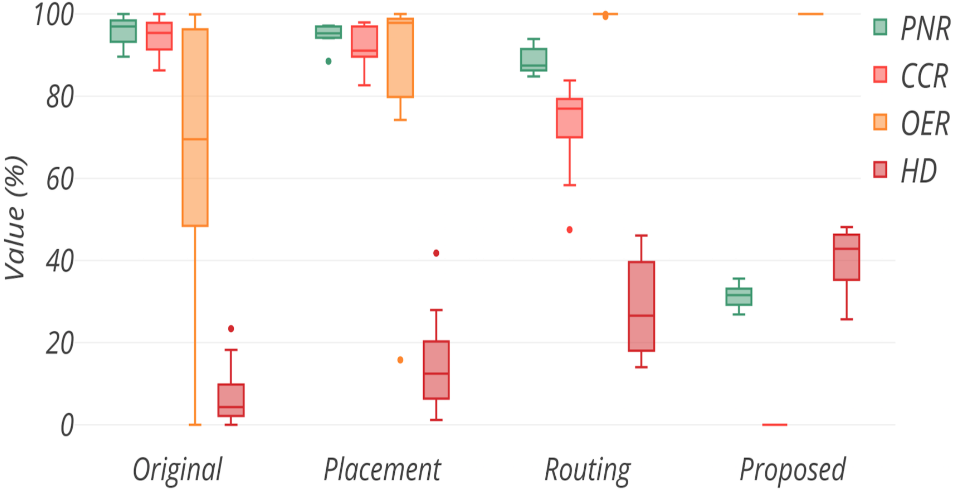
Exploratory Experiments on Security vs Layout Cost

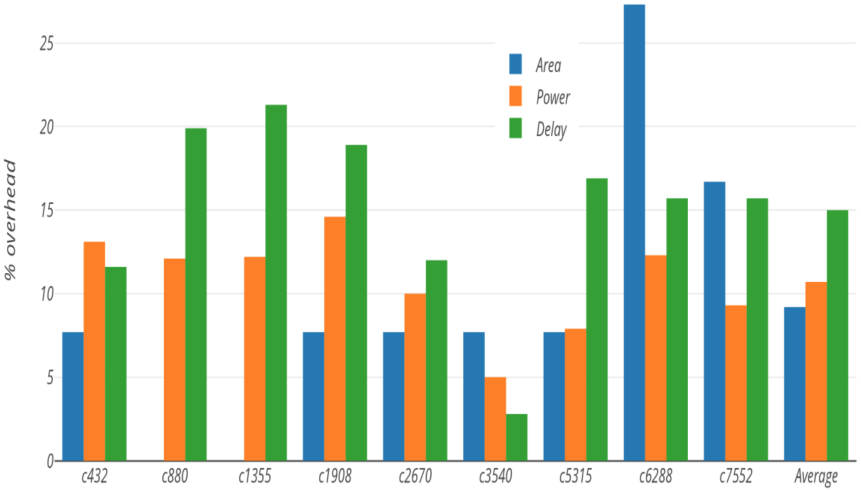
- Naïve lifting of randomly selected nets
  - ⚠ Increase in Power, performance and area (PPA)
  - ⚠ Area overheads are more drastic



Scope of Work

- More OPPs, while splitting at higher layers, yet at low commercial cost
- Routing – and hence PPA overhead – can become a challenge
- Scope of this work: Cost-effective and Secure Split Manufacturing

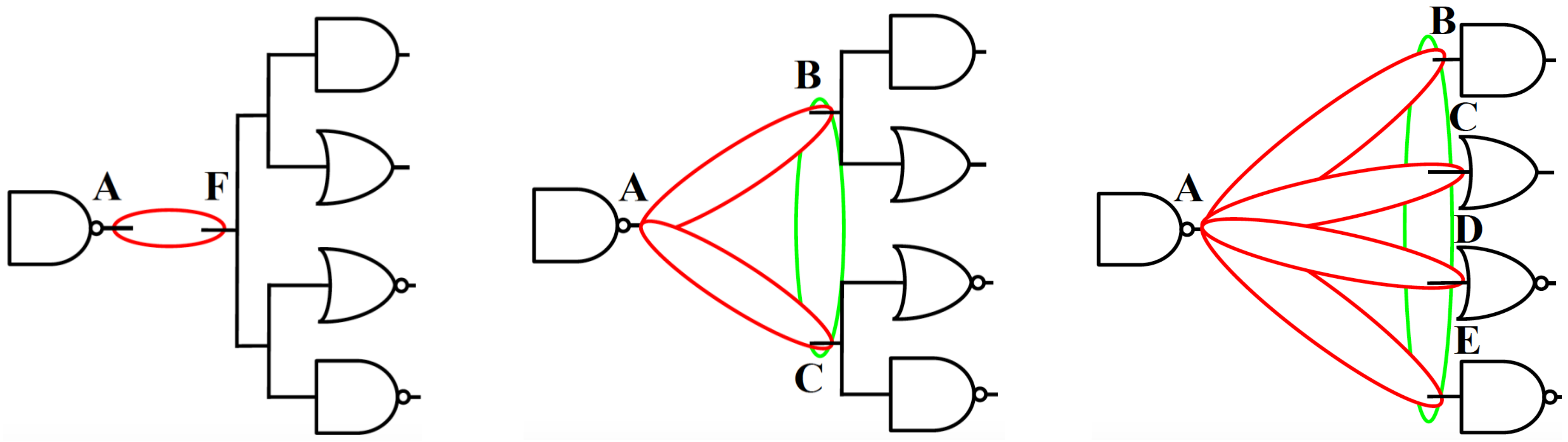




S. Patnaik et al., "Concerted Wire Lifting: Enabling Secure and Cost-Effective Split Manufacturing," ASP-DAC 2018

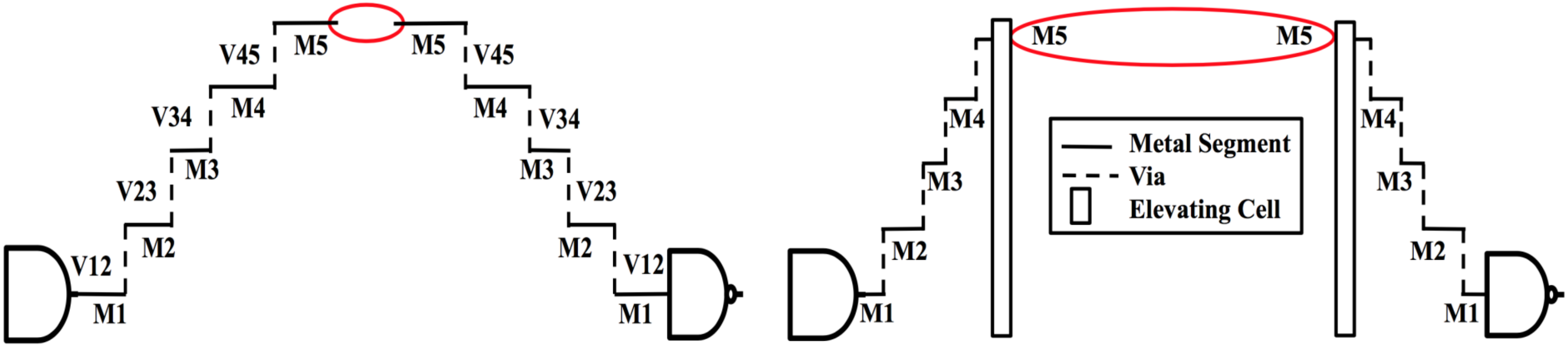
Strategy 1: Lifting High-fan-out Nets

- *Lifting HiFONs*
  - Incorrect connection propagates to multiple places
  - Introduces more *OPPs*



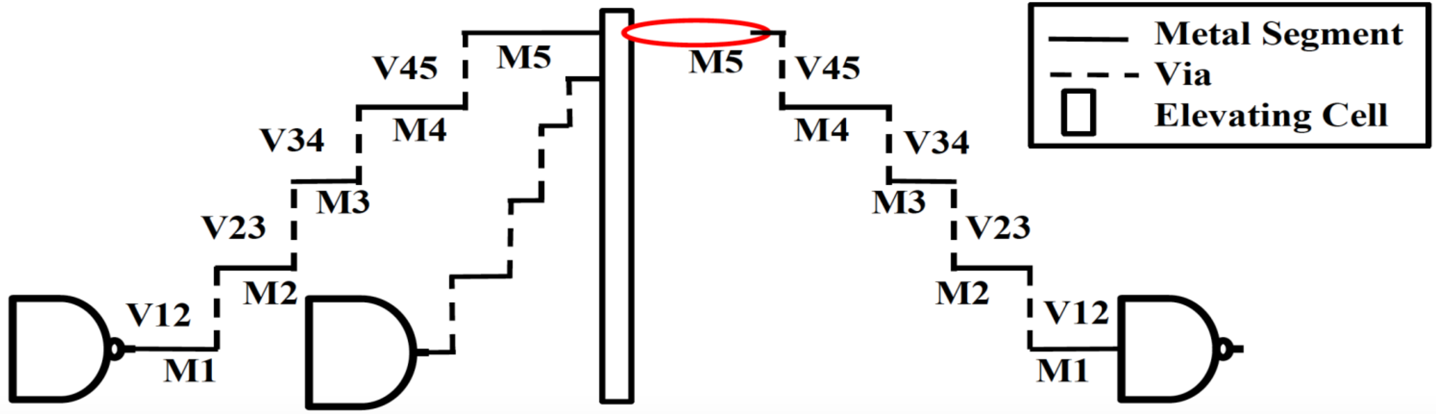
Strategy 2: Controlling Distances for OPPs

- Implicit wire lifting [Magana-ICCAD16] or short local detours [Wang-ASPDAC17]
  - ⚠ Shorter distance between open metal segments
  - ⚠ Proximity attack successful
- Increase distance between OPPs
  - 👍 Controllable distance
  - 👍 CCR reduces -- Attacker effort increases



Strategy 3: Obfuscating Short Nets

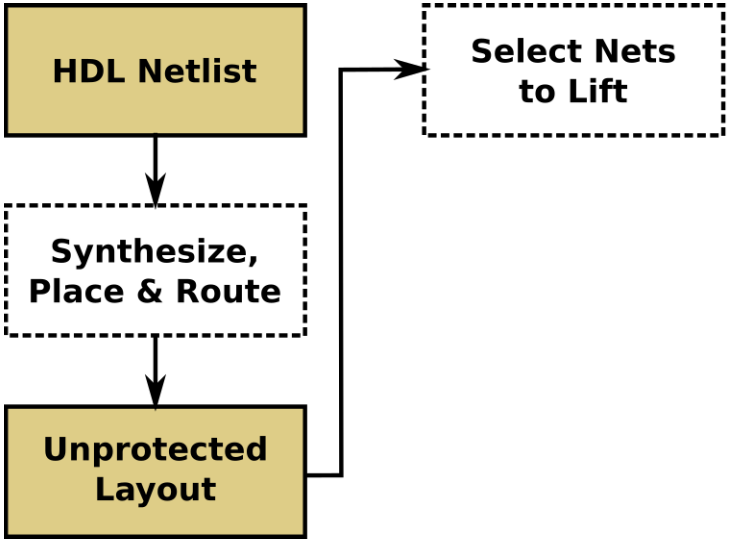
- Short nets
  - ⚠ Identification simpler, low driving strength of drivers, attack successful
- Need to increase ambiguity for an attacker
  - 👍 Addition of dummy net(s) & dummy driver
    - 👍 No combinatorial loops
    - 👍 Driving strength adapted
    - 👍 Increase in OPPs



S. Patnaik et al., "Concerted Wire Lifting: Enabling Secure and Cost-Effective Split Manufacturing," ASP-DAC 2018

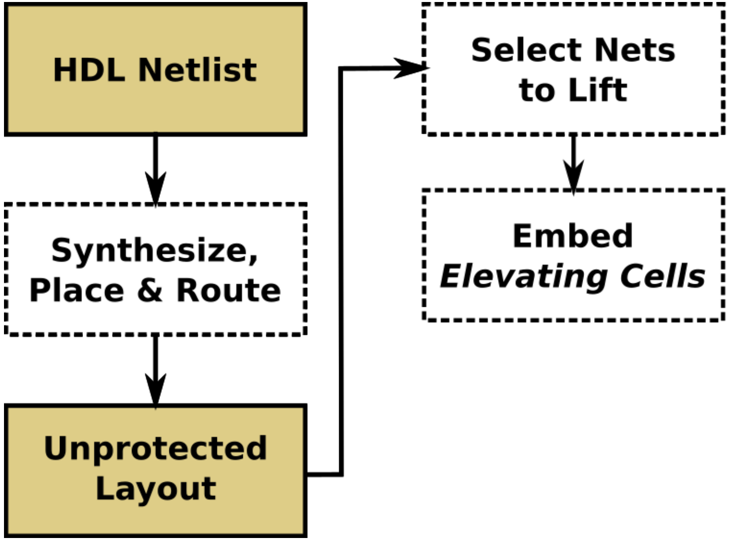
Protection Flow

- Automated flow, implemented for *Cadence Innovus*



Protection Flow

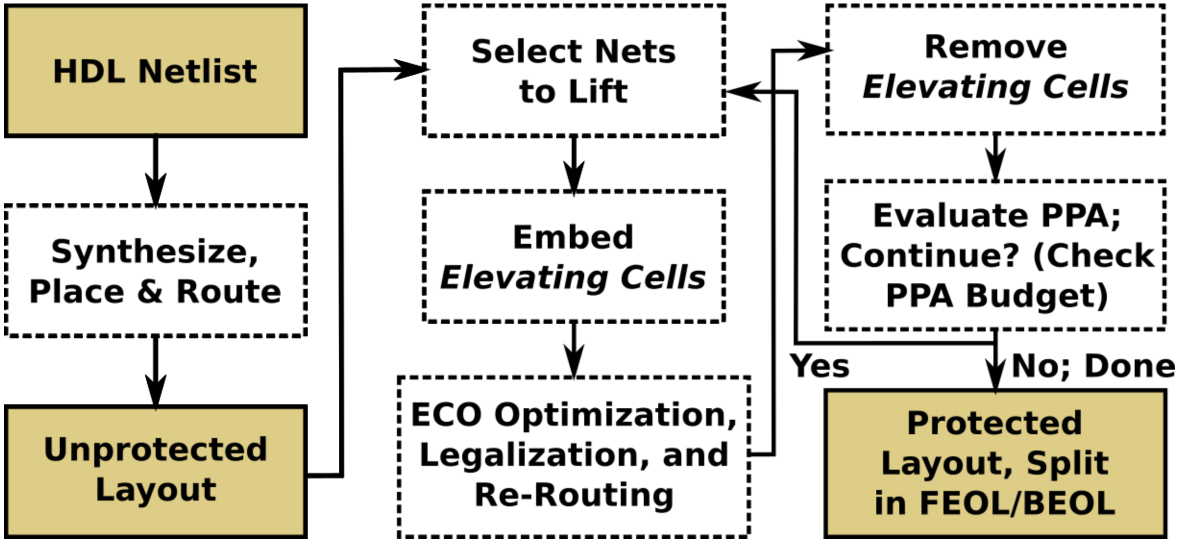
- Automated flow, implemented for *Cadence Innovus*



Customized *elevating cells* do not impact FEOL – only for routing of BEOL wires

Protection Flow

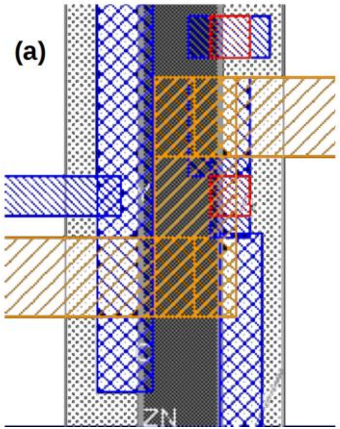
- Automated flow, implemented for *Cadence Innovus*

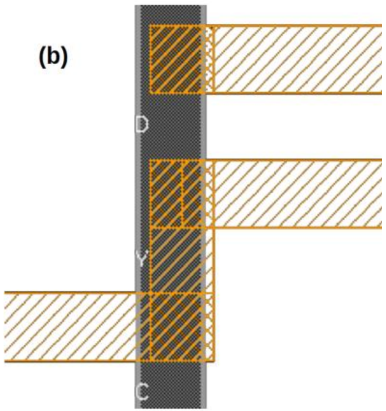


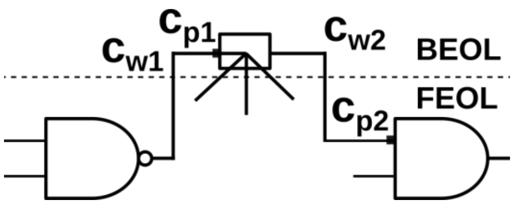
- Customized *elevating cells* do not impact FEOL – only for routing of BEOL wires

Physical Design of Elevating Cell

- 2/3 pins in M6
  - Lowers cost for split manufacturing
- Dimensions such that pins can “snap” onto routing tracks
- Customized constraint rules to allow overlap with regular cells
- Modeled as BUFX2
- Annotation of input capacitances, to account for load of “masked” sink pin and wire







Setup for Layout and Security Evaluation

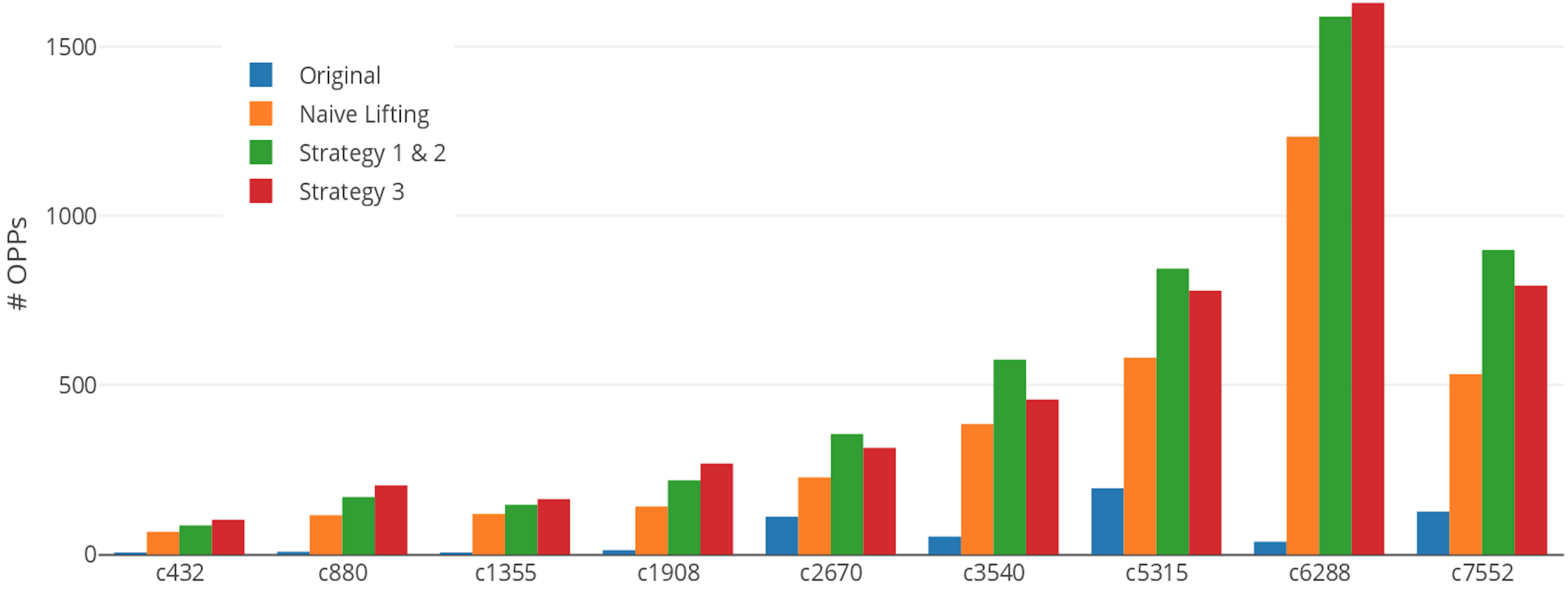
- *Cadence Innovus* 16.15
  - *NanGate 45nm Open Cell Library*, 10 metal layers
  - Conservative PPA setup: 0.95 V, 125 C, slow process corner, switching activity 0.2
  - Utilization rates for original layout such that <1% routing congestion

- Proximity attack based on [Wang-DAC16]
  - Layouts split after M3, M4, and M5
  - Functional equivalence using *Synopsys Formality*
  - OER and HD calculated using *Synopsys VCS*

- Total 28 benchmarks
  - Traditional ISCAS, MCNC and ITC-99
  - 1st time, large-scale industrial *IBM-superblue benchmarks*

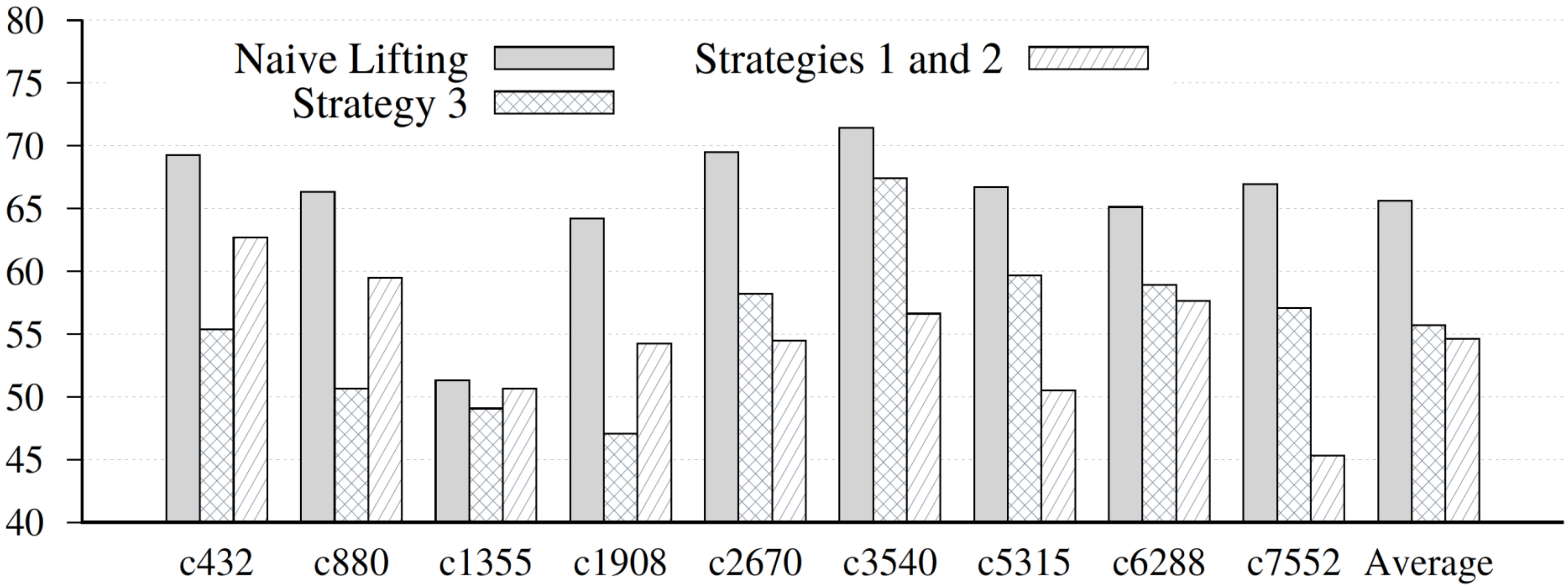
Name	Nets*
superblue1	879,168
superblue5	764,445
superblue10	1,158,282
superblue12	1,523,108
superblue18	672,084

Security Evaluation – Increase in OPPs



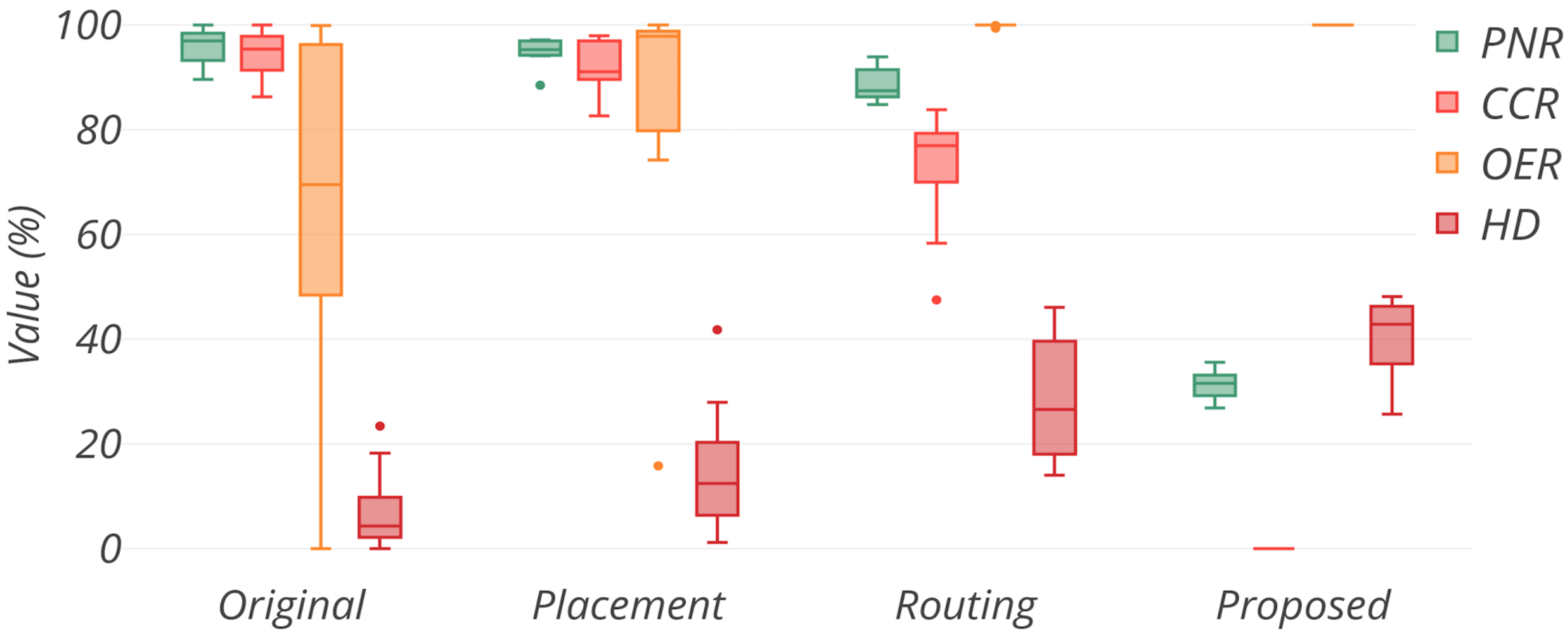
- More OPPs compared to Naïve lifting
  - Better security

Security Evaluation – Comparison of PNR (Percentage of Netlist Recovery)



- Less PNR compared to naïve lifting
  - Attacker learns less about the design

Security Evaluation – Comparison among Metrics

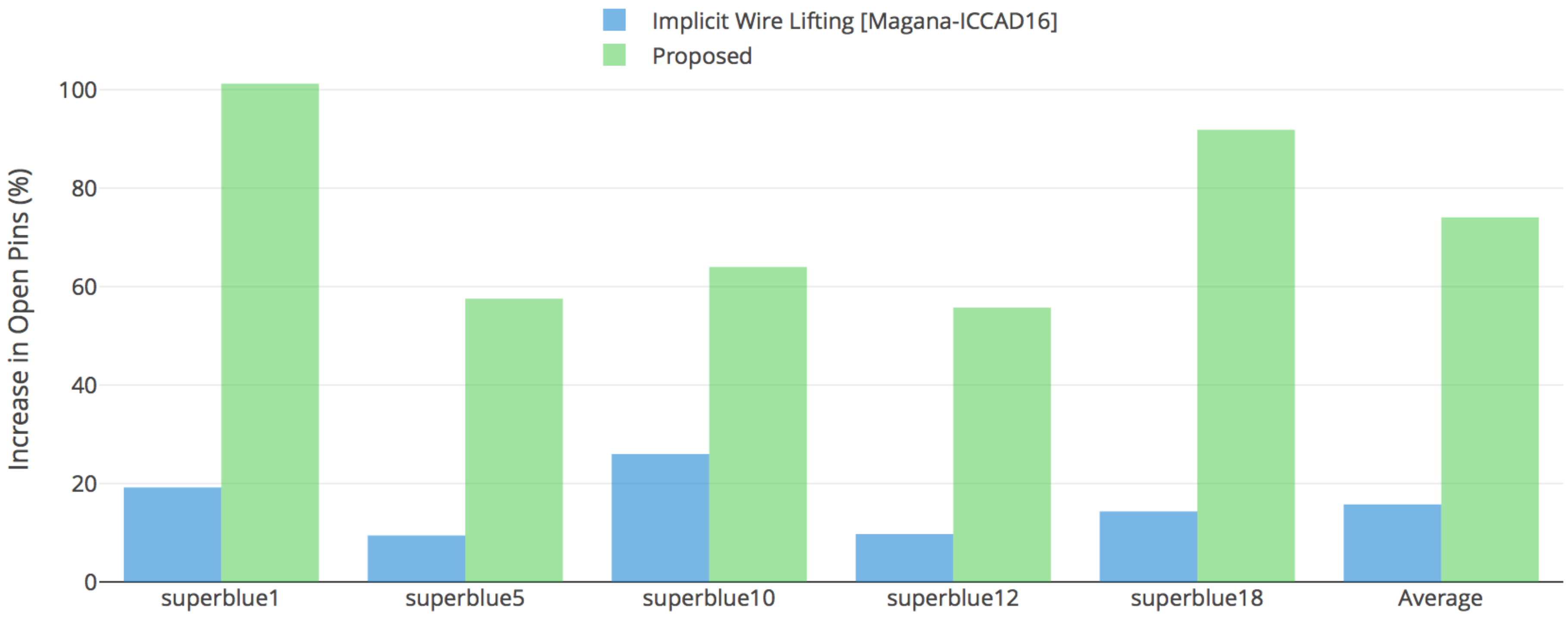


Placement: Wang et al.: The Cat and Mouse in Split Manufacturing, Proc. DAC, 2016

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

- CCR = 0%, OER = 100%
  - PNR is lowest among all schemes, HD is 40%

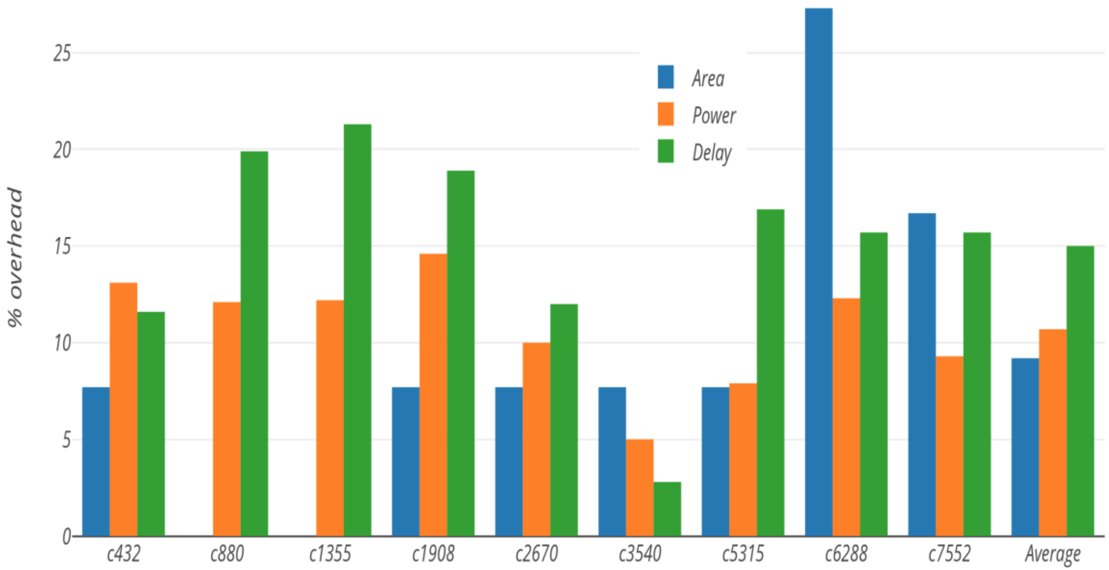
Security Evaluation – Increase in Open pins

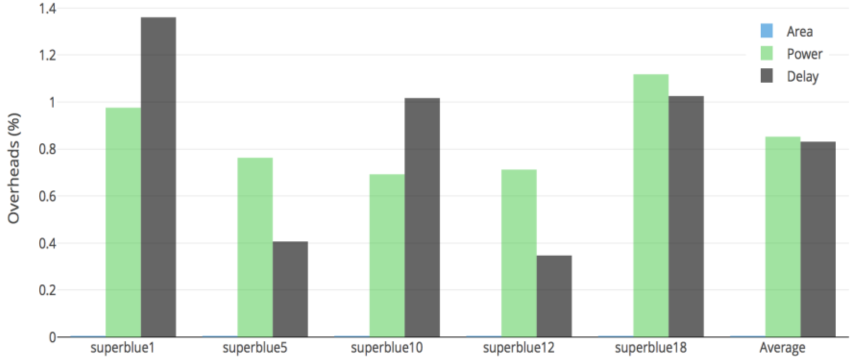


- On an average, 58.74% increase in open pins
  - More open pins above split layer – nets routed in higher layers

Layout Evaluation – PPA

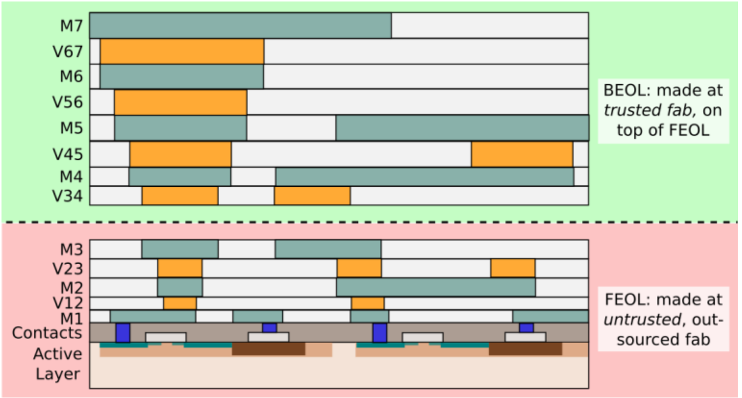
- Avg. overheads for PPA:
  - 10.7%, 15%, & 9.2%
- Avg. overheads (*IBM-superblue)*
  - 0.85%, 0.83%, & 0%
- Area: Die outline
  - Scale up die outlines to avoid any routing/DRC errors
- Power and performance
  - Increase of wirelength as nets are lifted
  - Relatively low resistance of higher metal layers
  - Positive effects are offset by routing congestion





On Use of Additional Metal Layers

- PPA and PNR can be further improved
  - Scarcity of routing resources

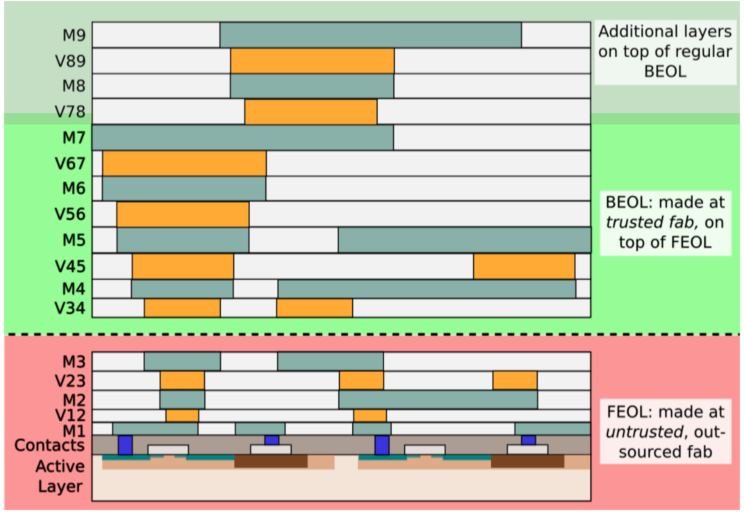


S. Patnaik et al., "Concerted Wire Lifting: Enabling Secure and Cost-Effective Split Manufacturing," ASP-DAC 2018

On Use of Additional Metal Layers

- PPA and PNR can be further improved
  - Scarcity of routing resources
  - Advocate use of additional metal layers
  - Less commercial cost, at trusted foundry

- Study on addition of 2 extra layers
  - Duplicated M6 twice

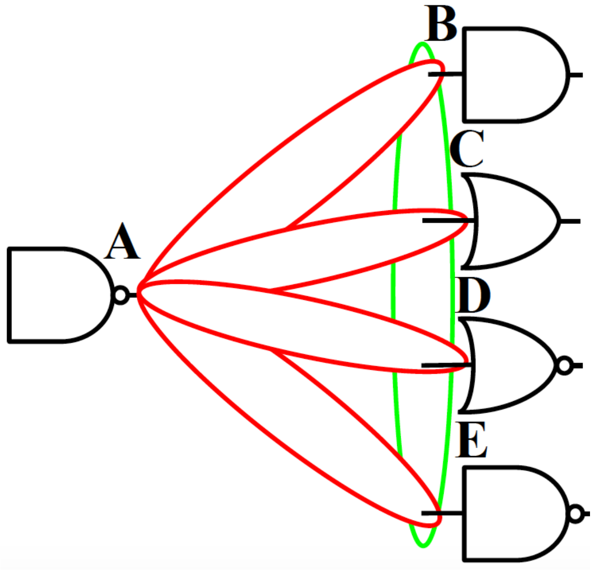


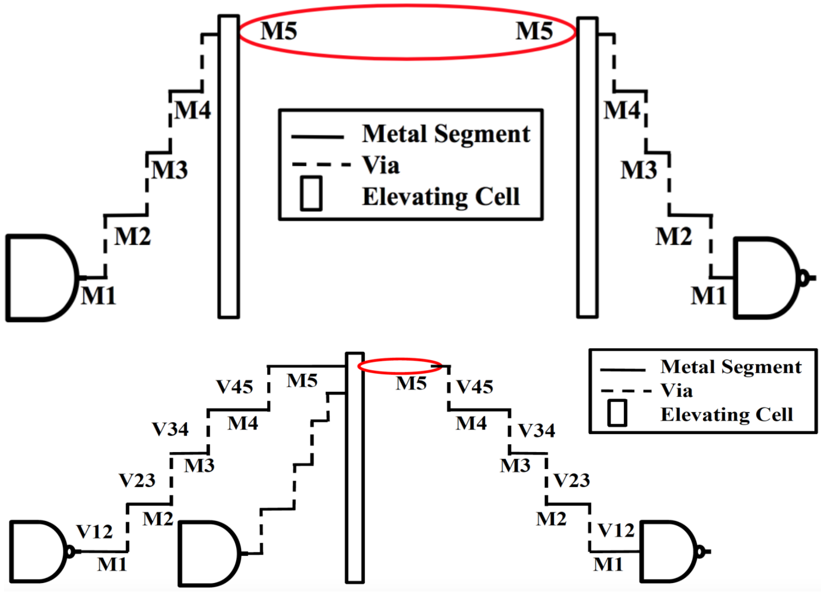
Benchmark	*PNR*	Die-Area Cost	Power Cost	Delay Cost
c5315	28.1	0	2.9	3.3
c6288	34.5	0	7.2	5.6
c7552	24.6	0	3.5	4.3
Average	29.1	0	4.5	4.4

S. Patnaik et al., "Concerted Wire Lifting: Enabling Secure and Cost-Effective Split Manufacturing," ASP-DAC 2018

Secure and Cost-Effective Split Manufacturing

- Strategies for Concerted wire lifting, more OPPs

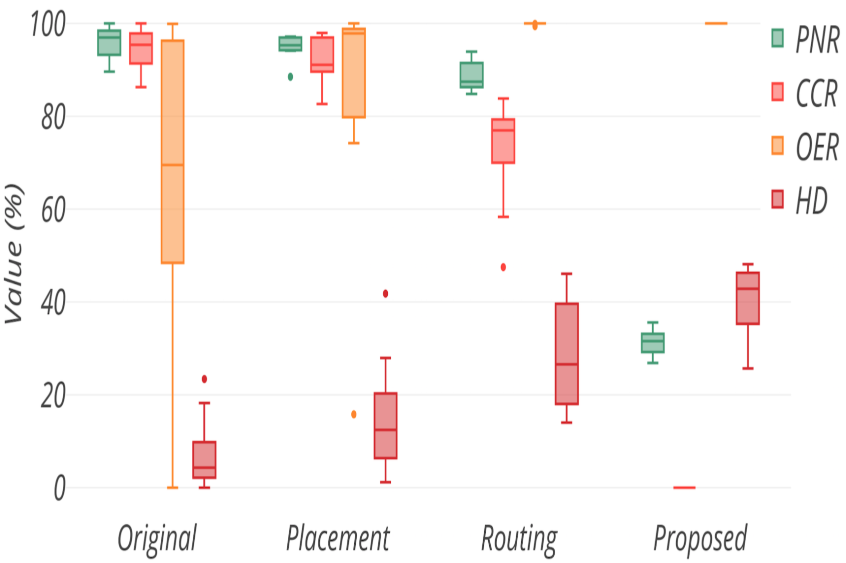


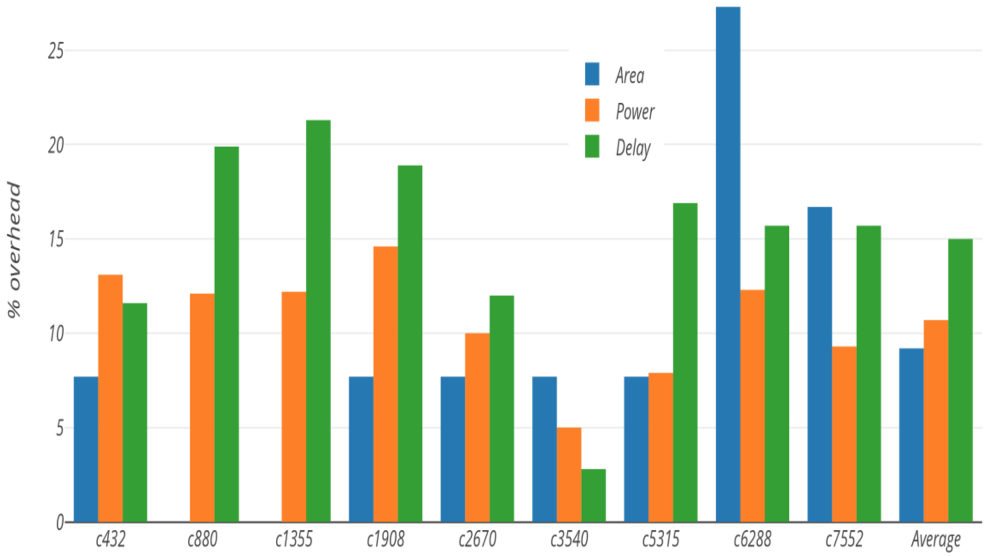


S. Patnaik et al., “Concerted Wire Lifting: Enabling Secure and Cost-Effective Split Manufacturing,” ASP-DAC 2018

Secure and Cost-Effective Split Manufacturing

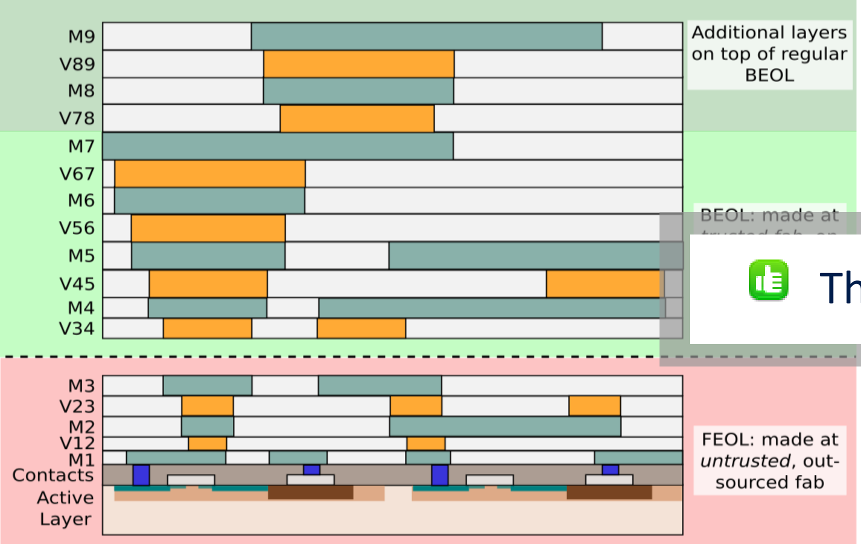
- Strategies for Concerted wire lifting, more OPPs
- Thorough evaluation of scheme – **superior considering security, $ cost, and PPA overheads**
- Resilient against proximity attacks, e.g., CCR 0%.

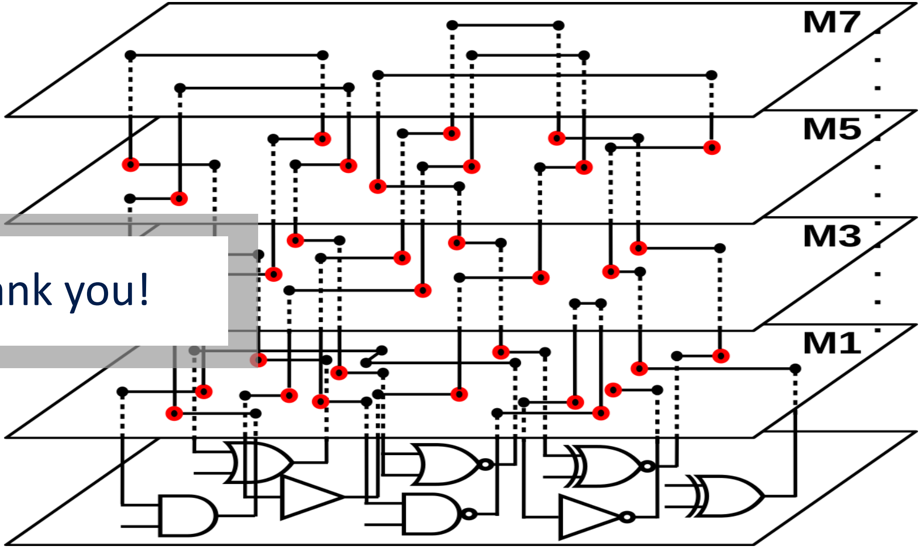




Secure and Cost-Effective Split Manufacturing

- Strategies for Concerted wire lifting, more OPPs
- Thorough evaluation of scheme – **superior considering security, $ cost, and PPA overheads**
- Resilient against proximity attacks, e.g., CCR 0%.
- Additional metal layers – aid in security, less overhead





Thank you!