Routing Perturbation for Enhanced Security in Split Manufacturing

Yujie Wang [*‡], Pu Chen [*], Jiang Hu[*] and Jeyavijayan (JV) Rajendran[†]

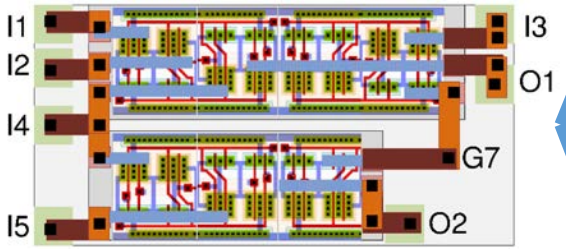
[*] Department of Electrical & Computer Engineering, Texas A&M University
[†] Department of Electrical Engineering, The University of Texas at Dallas
[‡] College of Electronic Information and Optical Engineering, Nankai University

TEXAS A&M UNIVERSITY | UT DALLAS

OVERVIEW

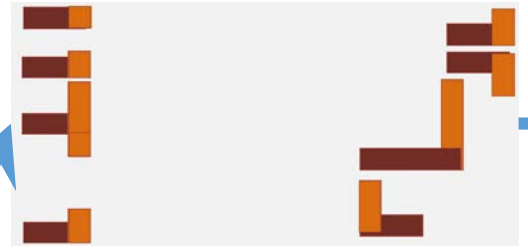
- Introduction
- Defense
- Experiments
- Conclusion

INTRODUCTION

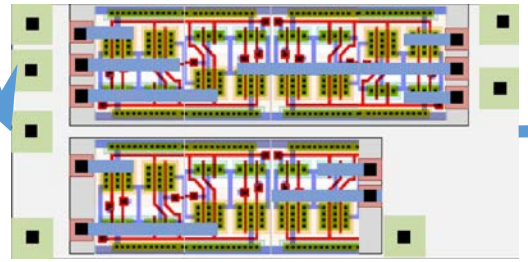


Layout*

Defender†



BEOL*
(Back End Of Line)



FEOL*
(Front End Of Line)

Fabricated in TRUSTED foundry

Fabricated in UNTRUSTED foundry

Align and integrated BEOL and FEOL part

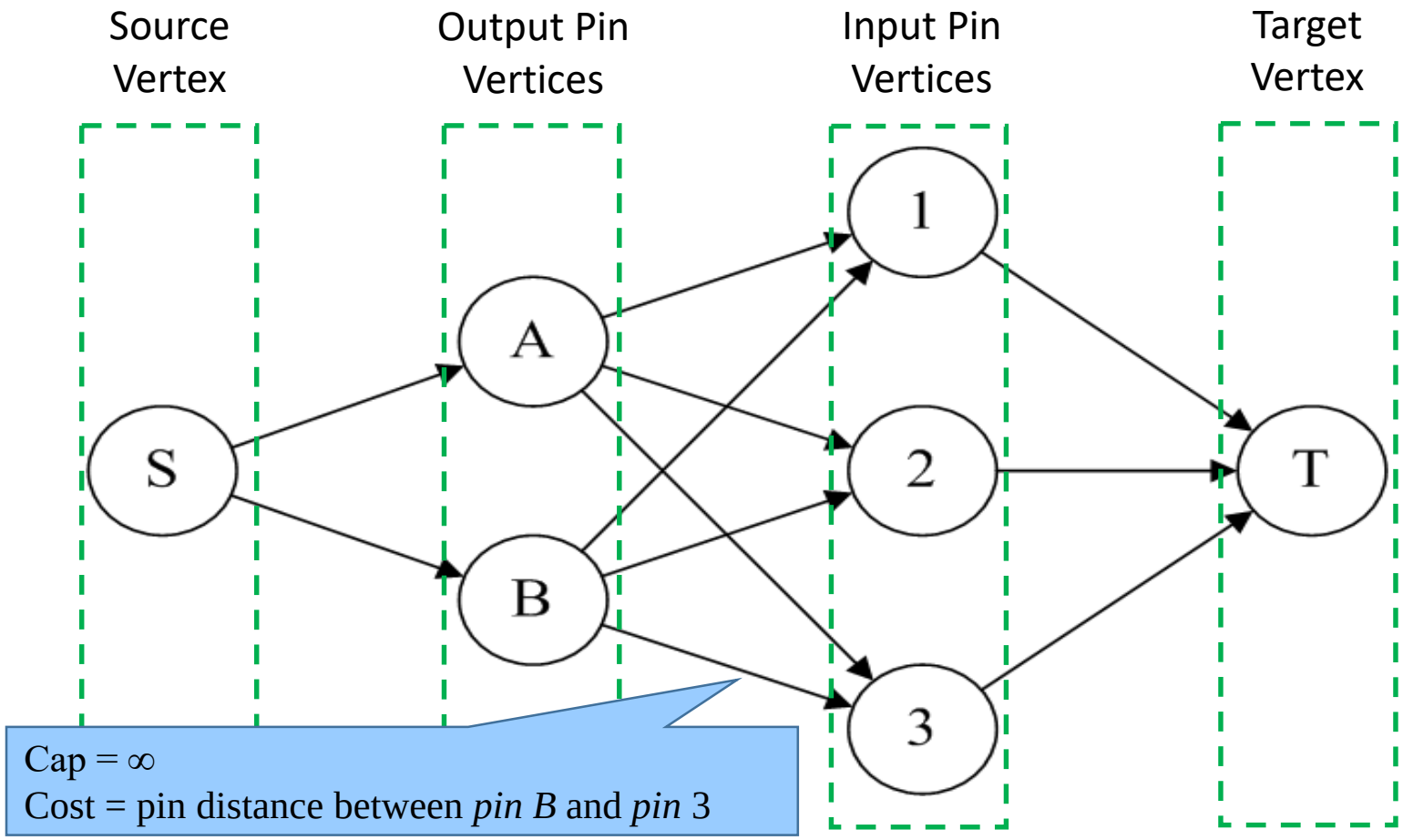
Attacker†

* JV, et.al, “Is split manufacturing secure?,” IEEE/ACM DATE2013
† From internet

Proximity Attack

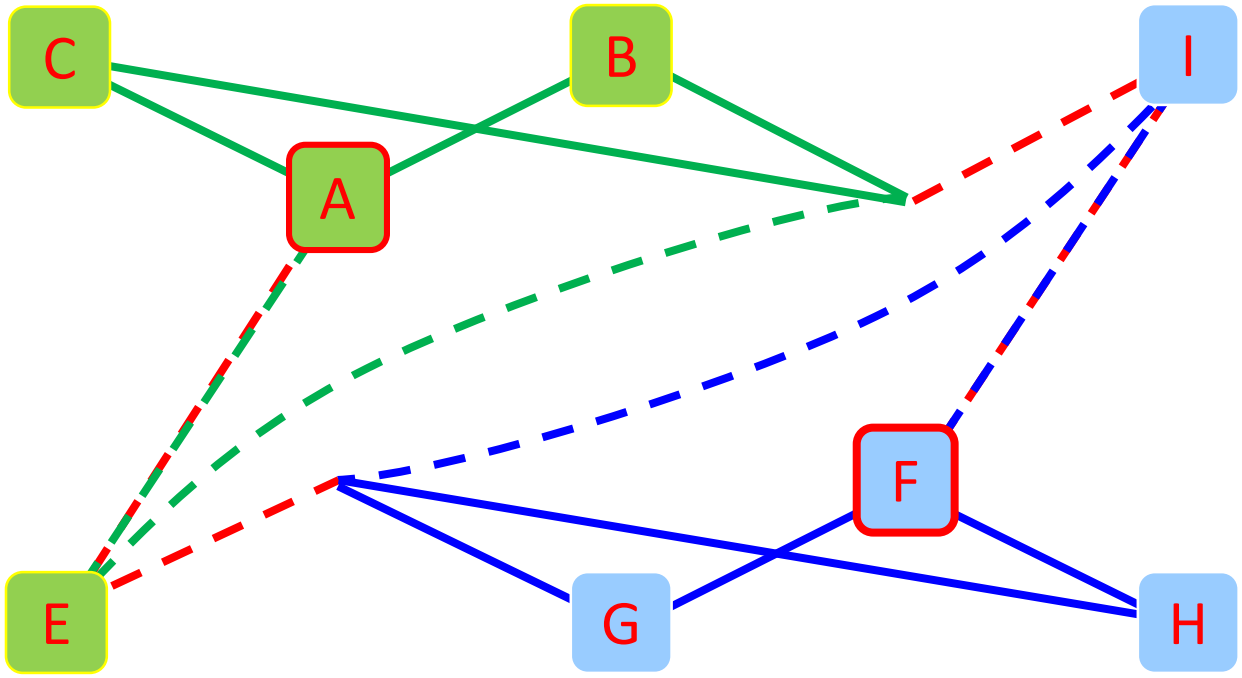
--JV, et.al, “Is split manufacturing secure?”, IEEE/ACM DATE2013
--J.Magana, “ Are proximity attacks a threat to the security of split manufacturing of integrated circuits?” ICCAD2016

Network-flow Attack Model *



* Y. Wang, The Cat and Mouse in Split Manufacturing. DAC 2016

Placement Perturbation Based Defense Model*(Previous Work)



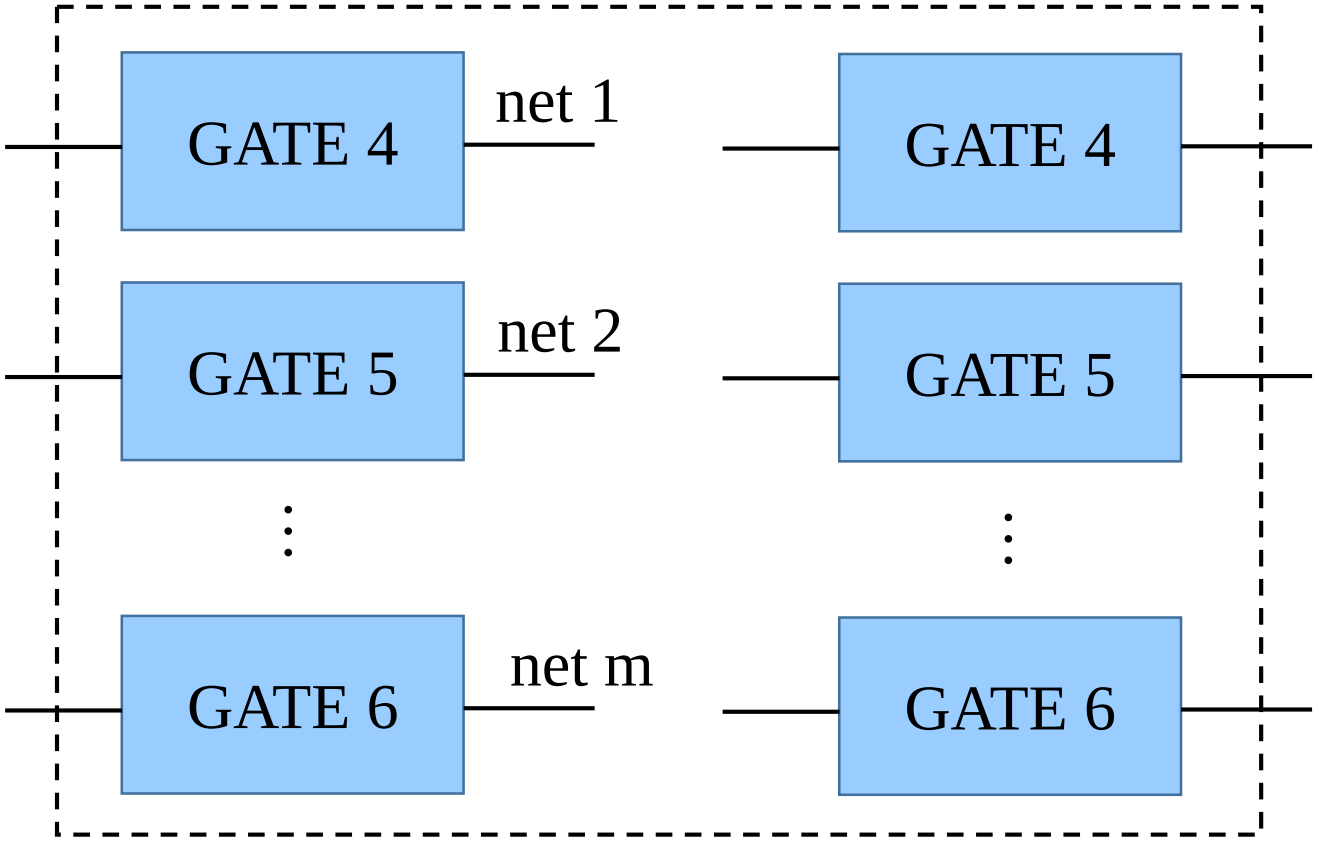
* Y. Wang, The Cat and Mouse in Split Manufacturing. DAC'16

Routing Perturbation Based Defense Method

OVERVIEW

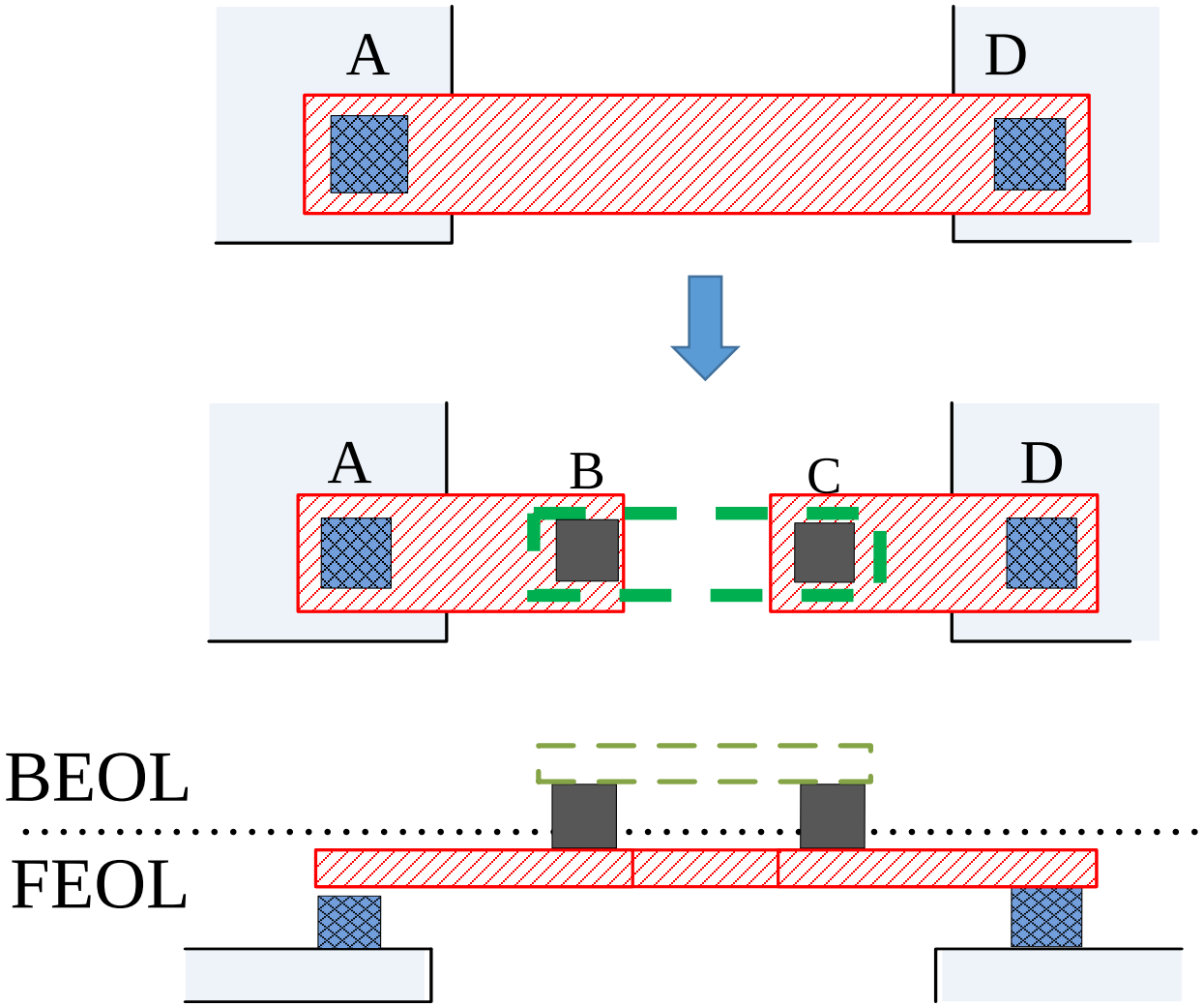
- Introduction
- Defense
- Experiments
- Conclusion

- Layer Elevation
- Routing Detour
- Decoy
- Test Principle



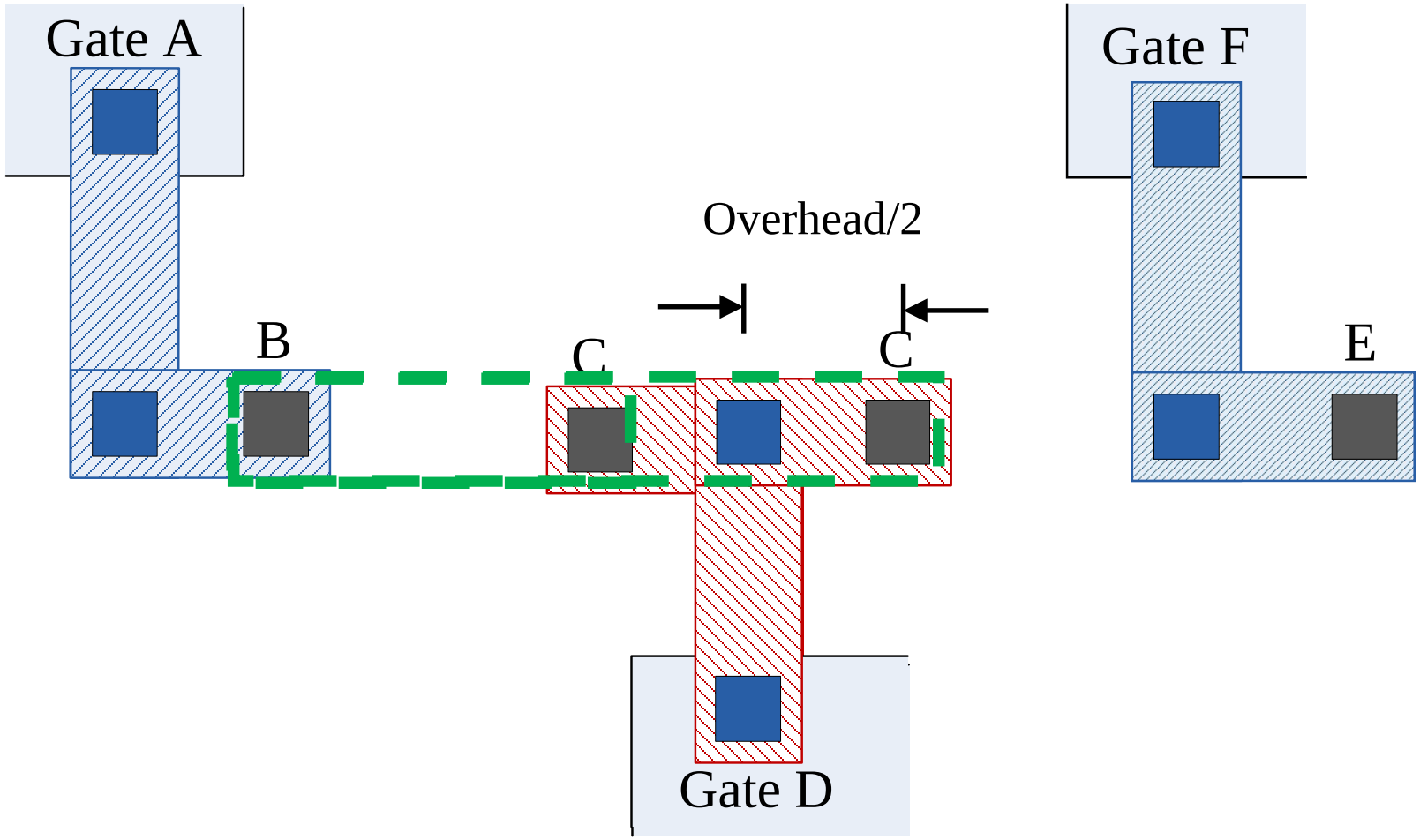
M 2-pin nets in BEOL ⟶ M! solution space

DEFENSE – LAYER ELEVATION



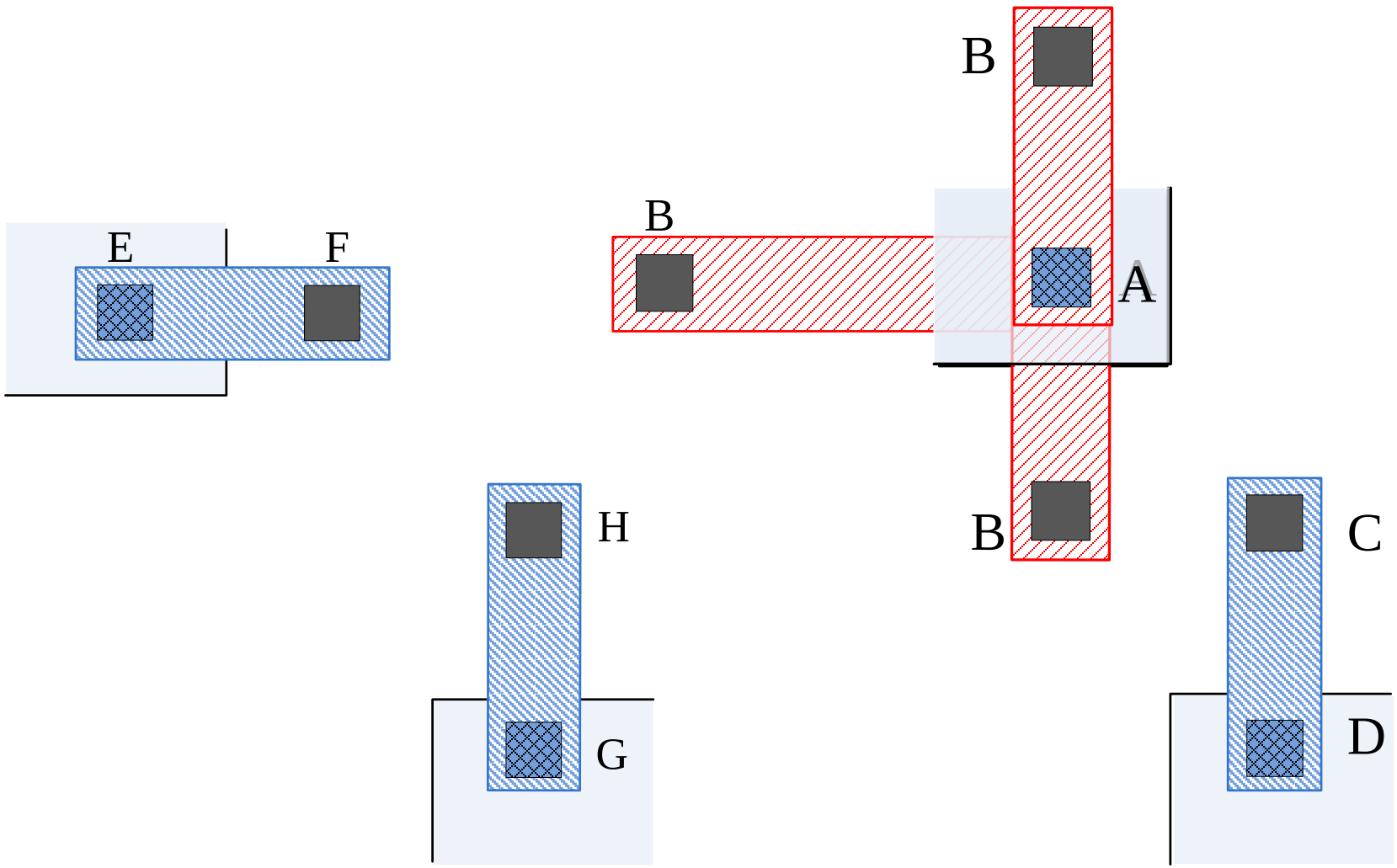
- Layer Elevation
- Routing Detour
- Decoy
- Test Principle

Directionality of dangling wires

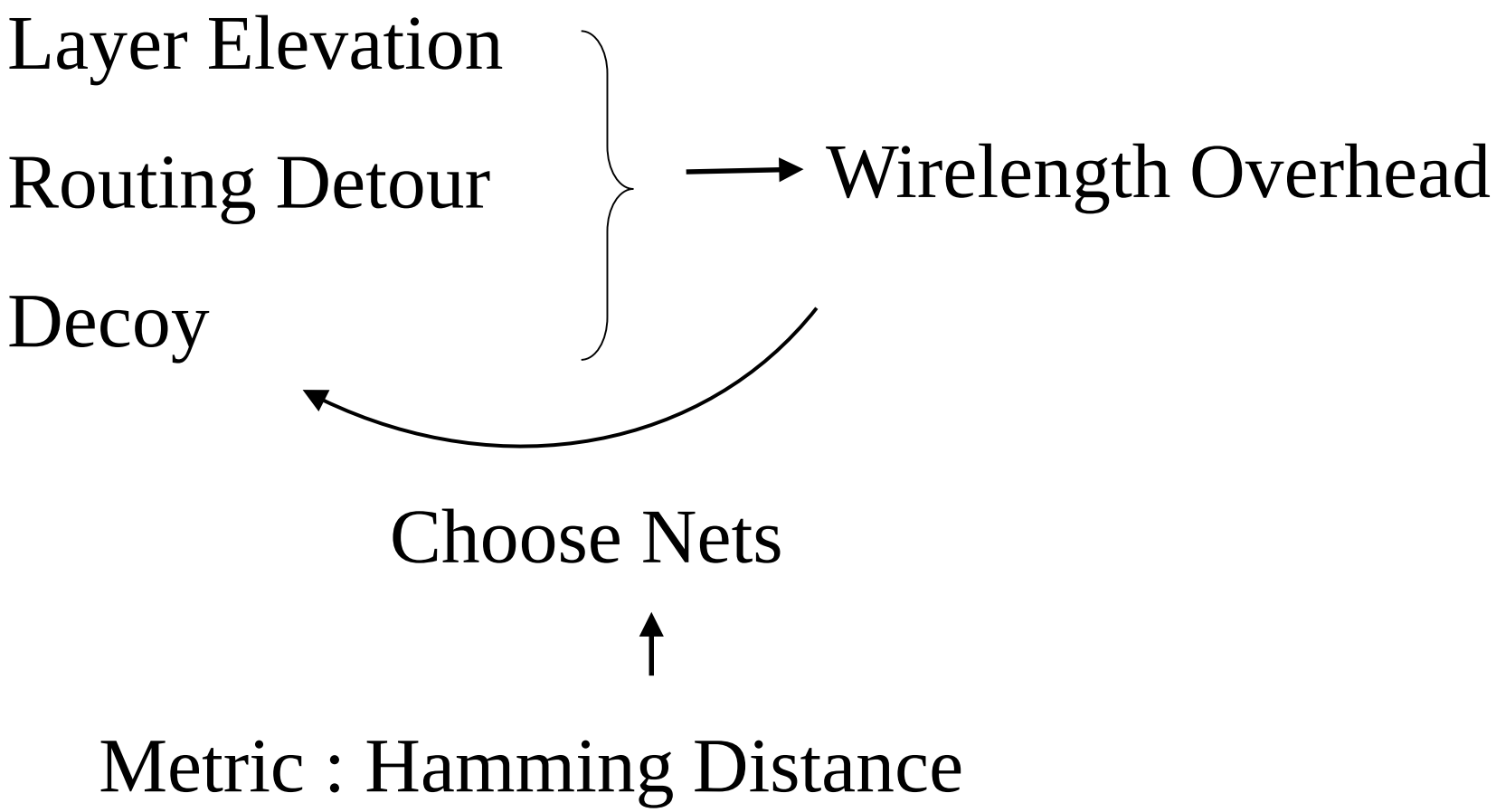


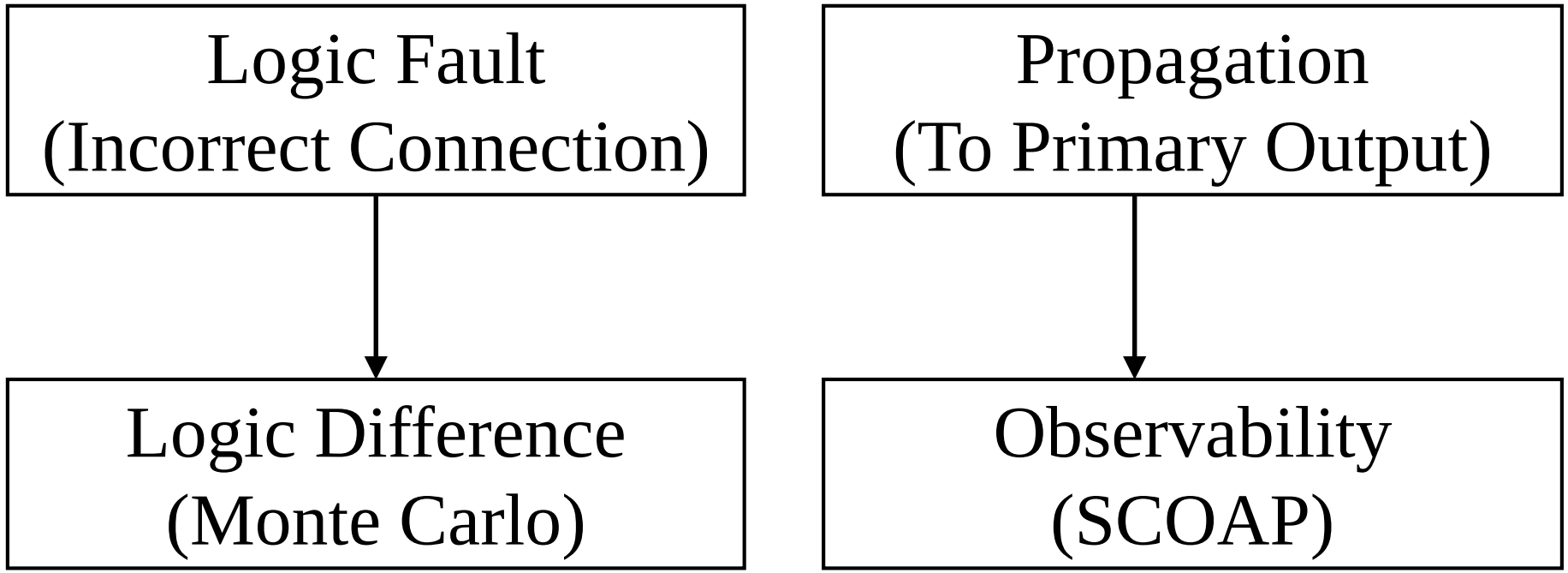
- Layer Elevation
- Routing Detour
- Decoy
- Test Principle

DEFENSE – DECOY

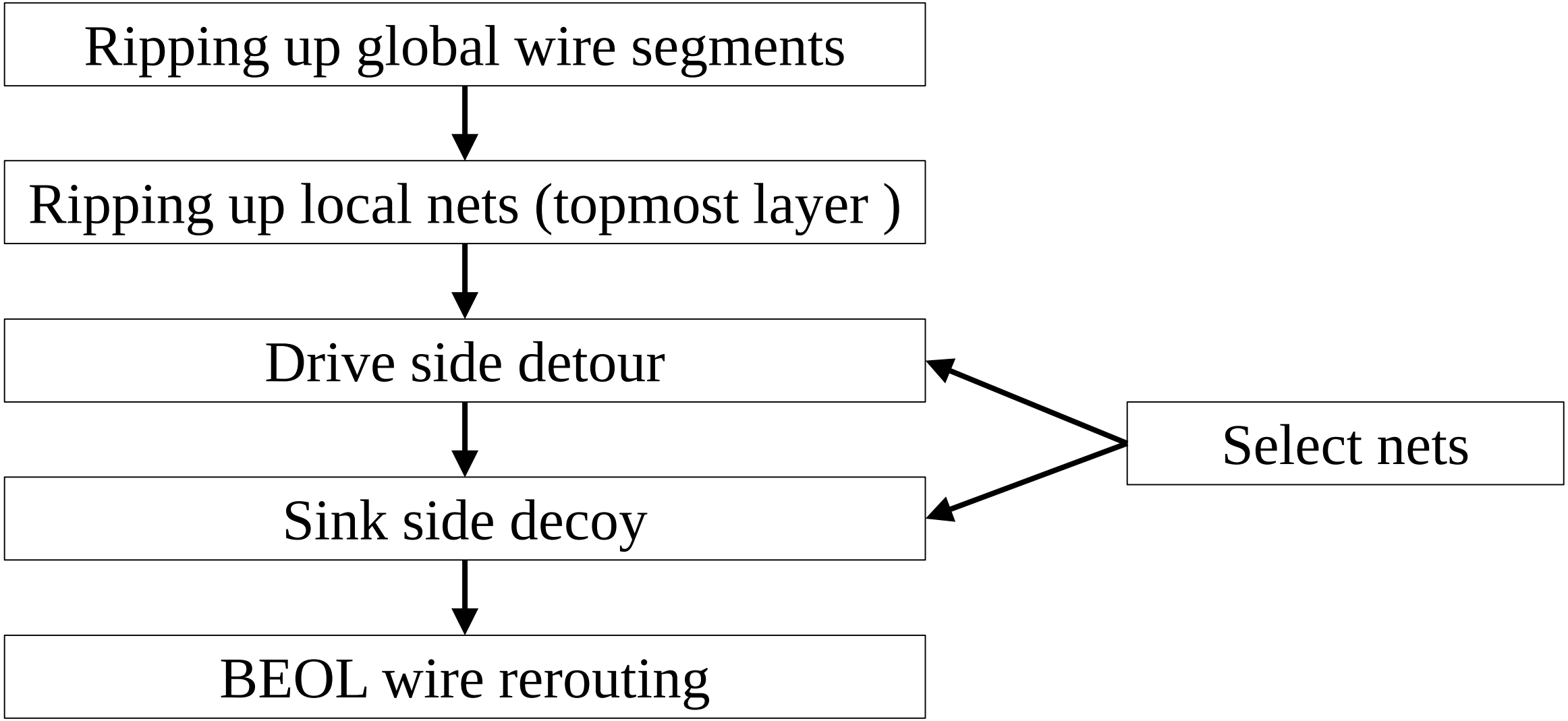


- Layer Elevation
- Routing Detour
- Decoy
- Test Principle


Layer Elevation
Routing Detour
Decoy
Wirelength Overhead
Choose Nets
Metric : Hamming Distance


Logic Fault
(Incorrect Connection)
Propagation
(To Primary Output)
Logic Difference
(Monte Carlo)
Observability
(SCOAP)

DEFENSE – OVERALL ALGORITHM



OVERVIEW

- Introduction
- Defense
- Experiments
- Conclusion

ISCAS'85 + ITC'99 + Network-flow Attack Model

Incorrect Conection Rate : 10.7% → 36%

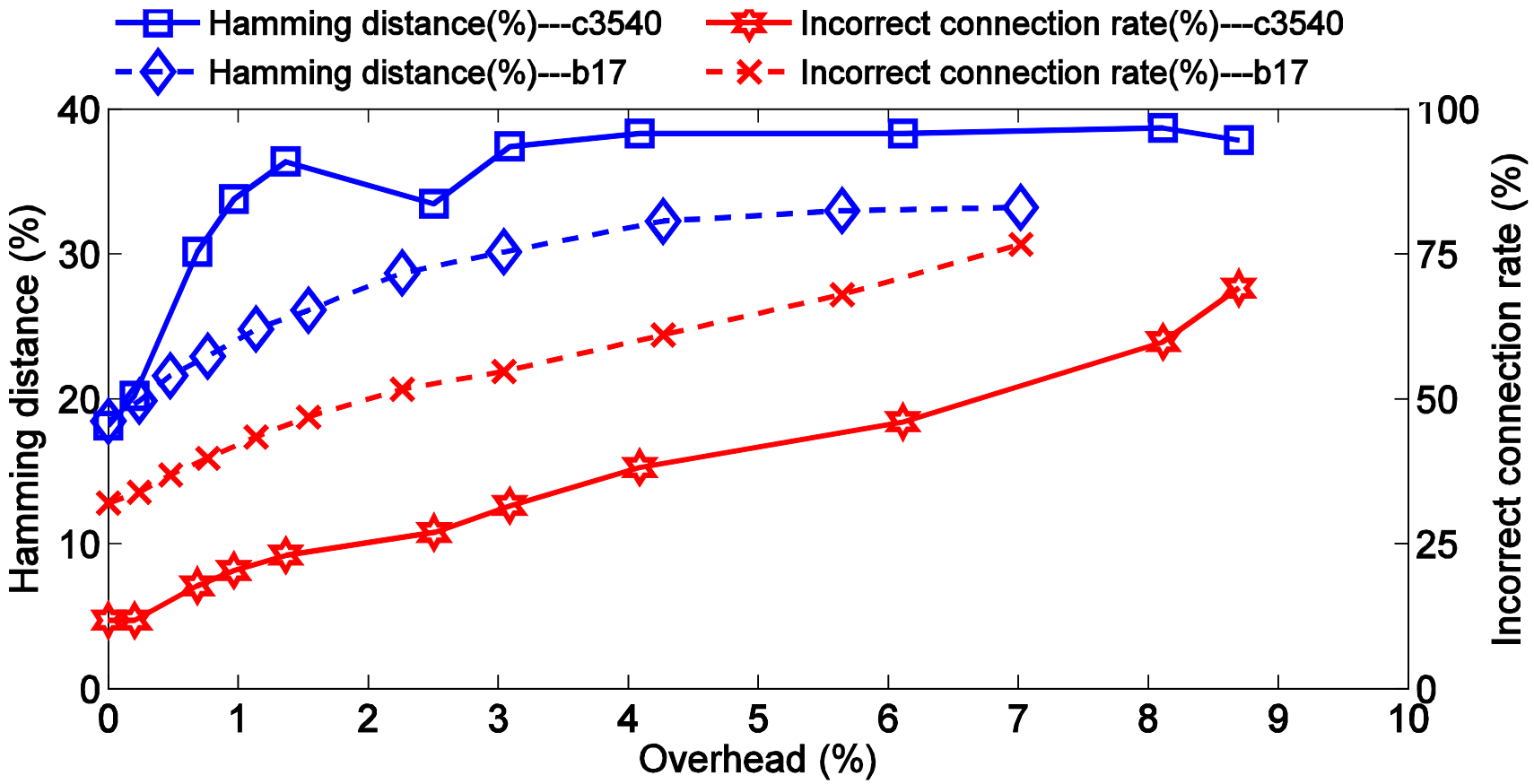
Hamming Distance : 8.1% → 27%

Wirelength Overhead : 2.9%

Timing Overhead :0.23%

$$Incorrect\ Connection\ Rate = \frac{\#\ incorrect\ connections}{\#\ nets\ in\ BEOL + \#\ nets\ in\ topmost\ FEOL\ layer}$$

EXPERIMENTS – SECURITY VERSUS OVERHEAD TRADE-OFF



Wirelength overhead ↑ Inorrect connections ↑

Hamming distance ↑ Defense effectiveness ↑

- Introduction
- Attack
- Defense
- Experiments
- Conclusion

- Three routing perturbation techniques
- Test principle to trade off overhead and security
- Effectiveness : 8.1% → 27% (Hamming distance)
- Overhead : about 6%[1] → 2.9% (wirelength)

[1] Y. Wang, The Cat and Mouse in Split Manufacturing. DAC'16

Thank you!