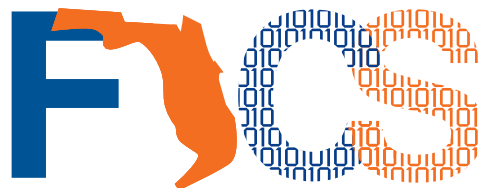


A Layout-driven Framework to Asses Vulnerability of ICs to Microprobing Attacks

Qihang Shi¹, Navid Asadizanjani², Domenic Forte², Mark M. Tehranipoor²

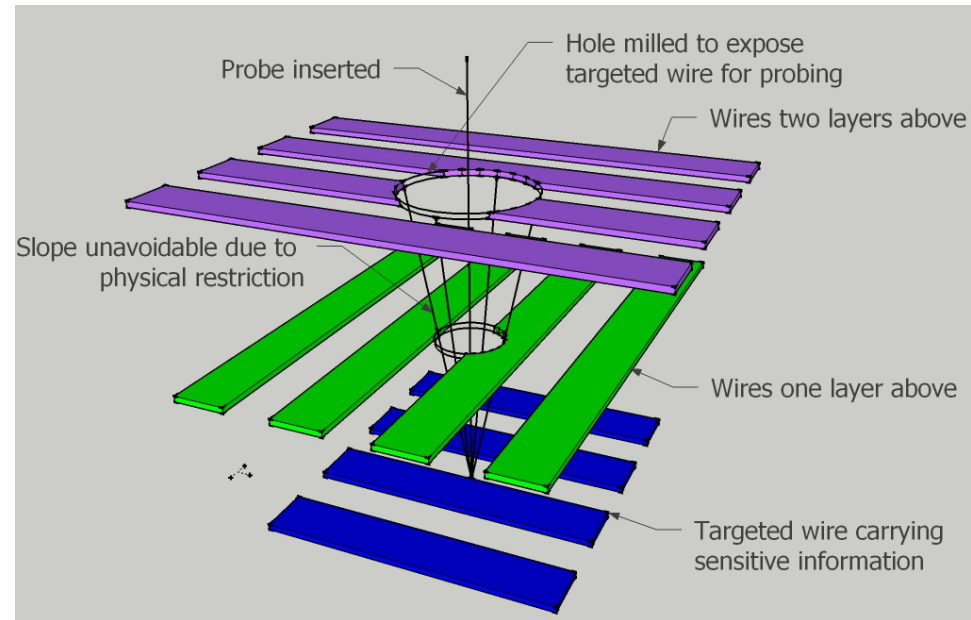
¹ University of Connecticut

² University of Florida

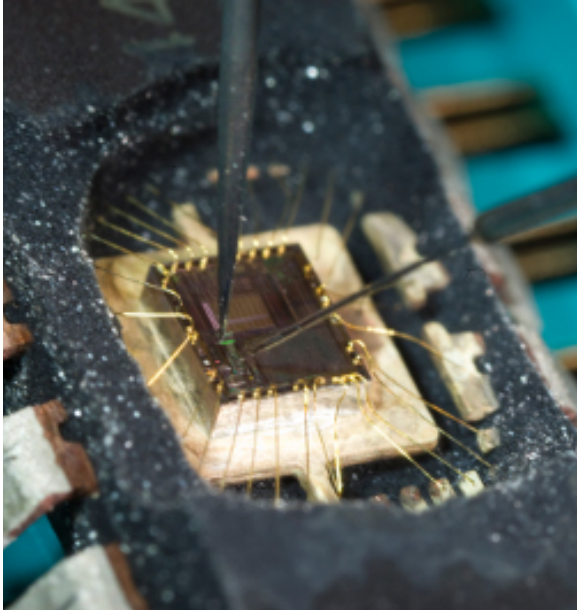


Microprobing Attacks

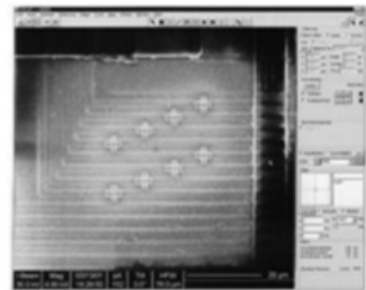
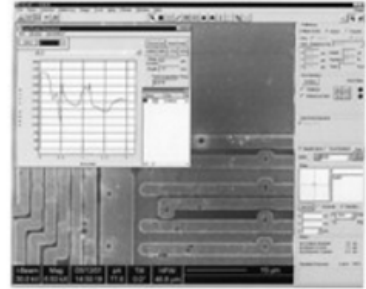
- **Definition:** circumvent encryption by probing at signal wires to extract security sensitive information
- **Reality:** any given wire in IC is likely buried under layers of wires
- Either mill through, or perform backside attack
 - **Focused Ion Beam (FIB)** can reach nanometer level accuracy
 - **Aspect Ratio (R_{FIB})** defined as milling depth divided by hole diameter
 - Backside attack (from substrate) not likely to replace frontside due to resolution limits and back-to-back 3D IC



Physical Microprobing Examples



Picture courtesy of Semiresearch Ltd

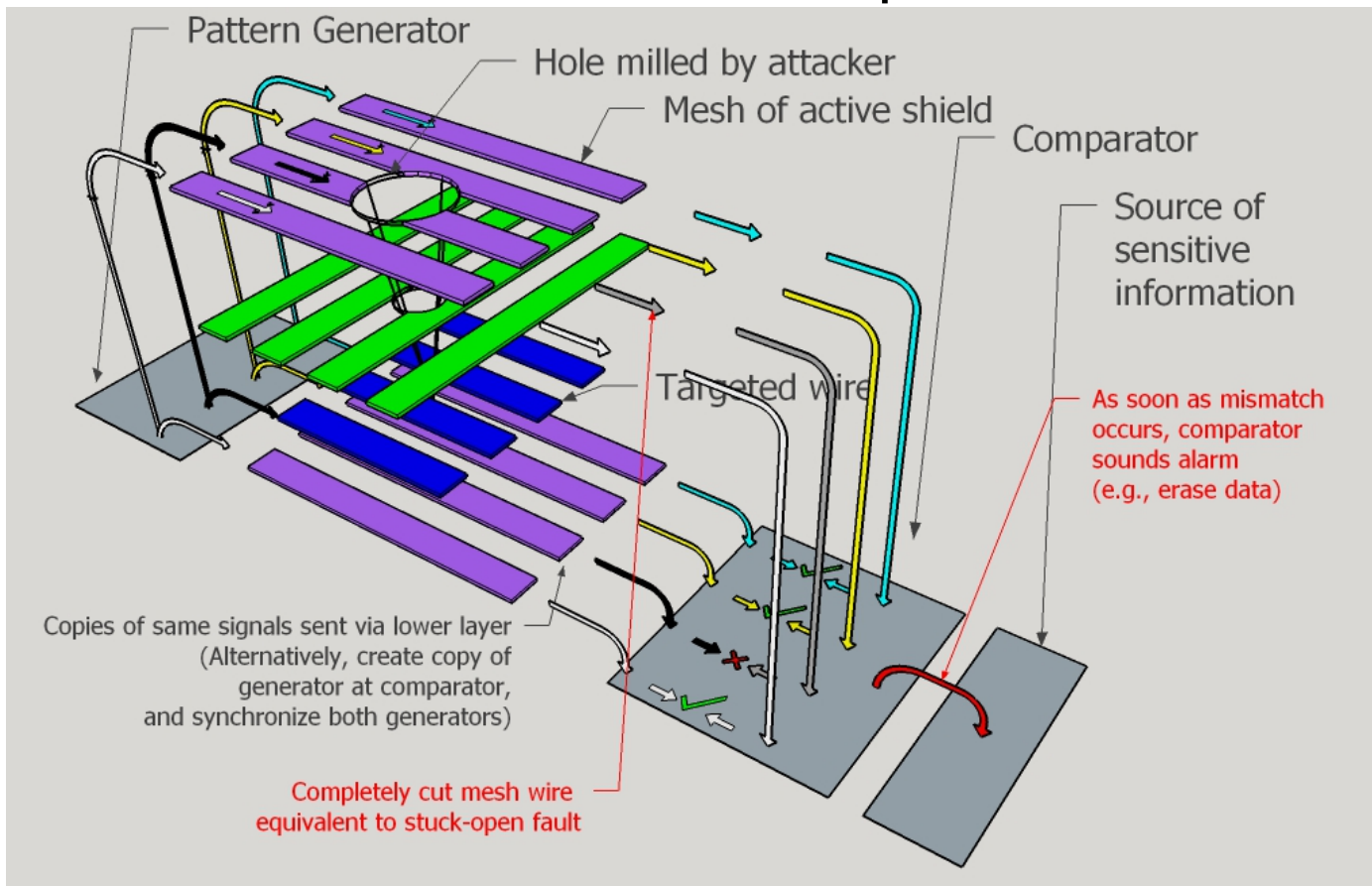


<https://www.sec.ei.tum.de/en/research/invasive-attacks/>

<http://slideplayer.com/slide/9006291/>

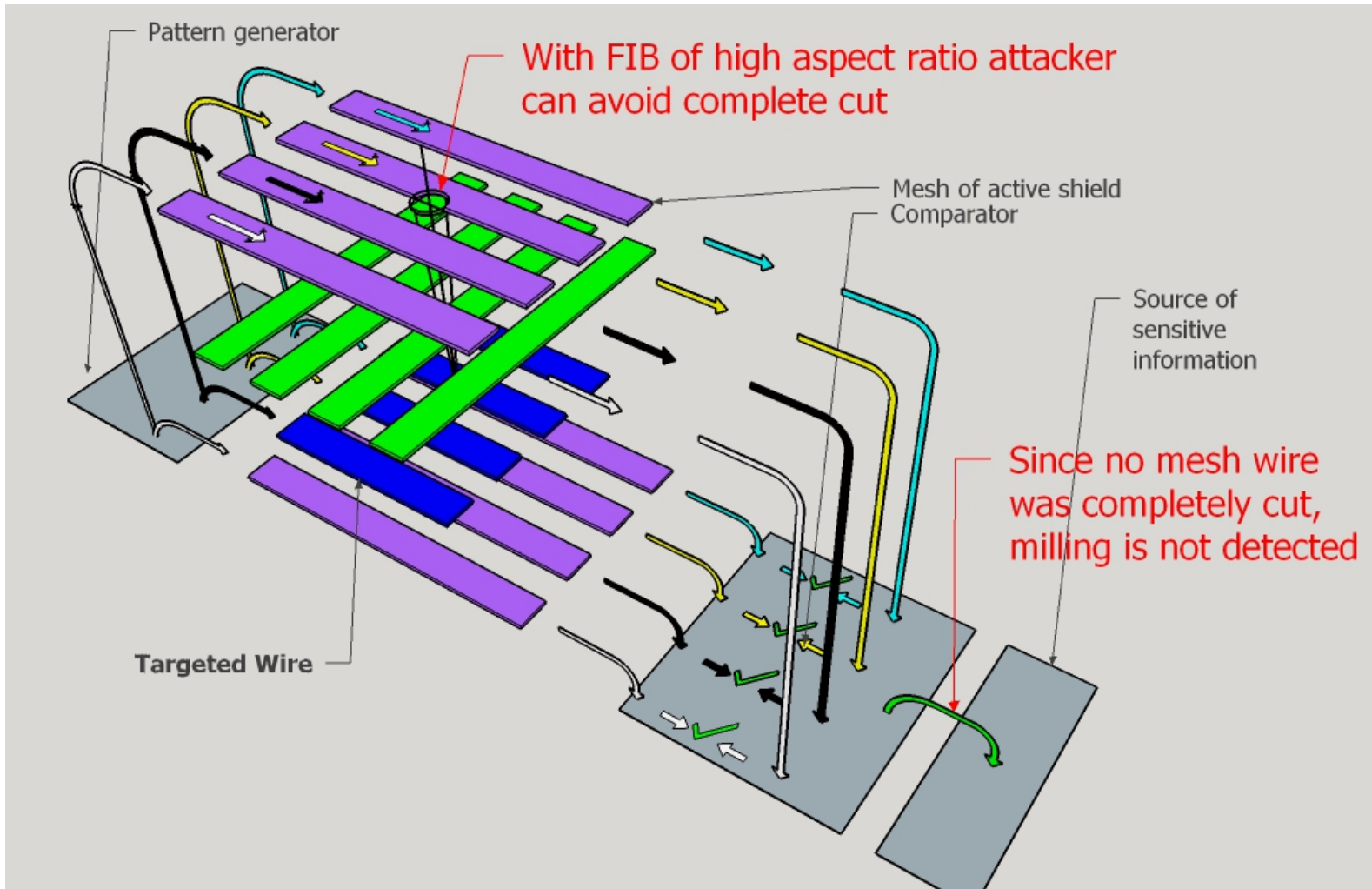
Antiprobing Designs: Active Shields

- **Digital active shields:** detect complete cut of shield wires



- Other approaches all have major weakness
 - analog shield, t-private circuit, Probe Attempt Detector (PAD)

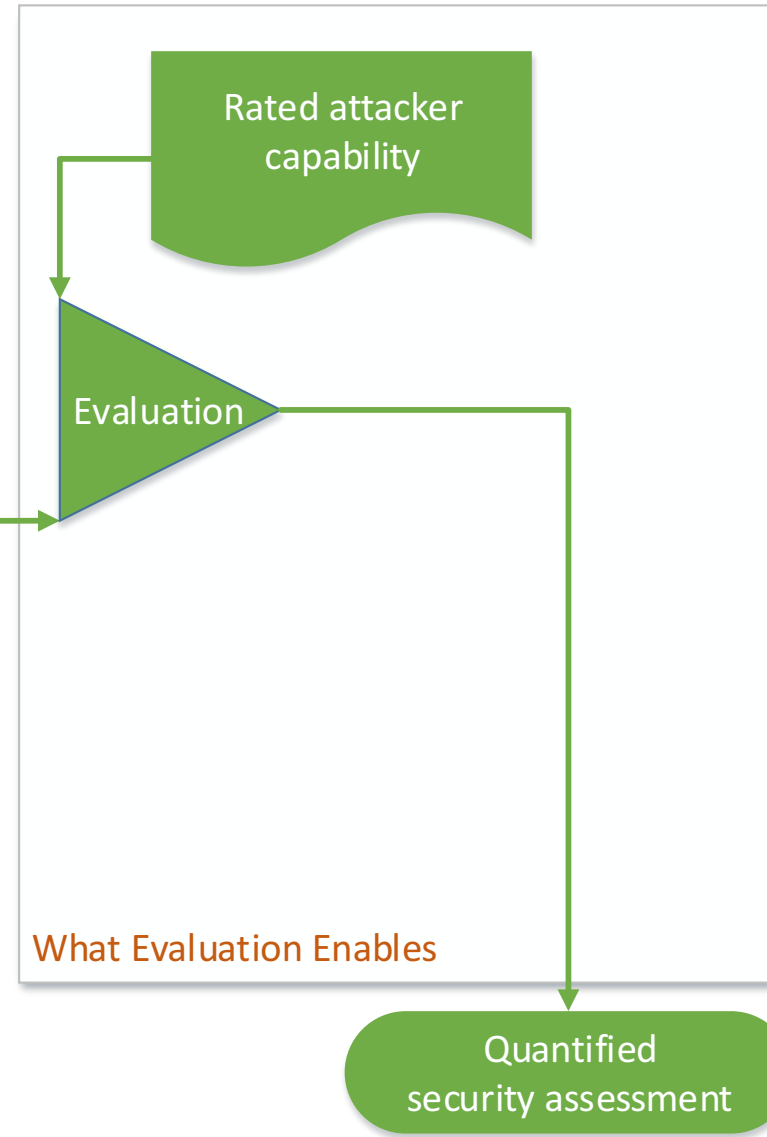
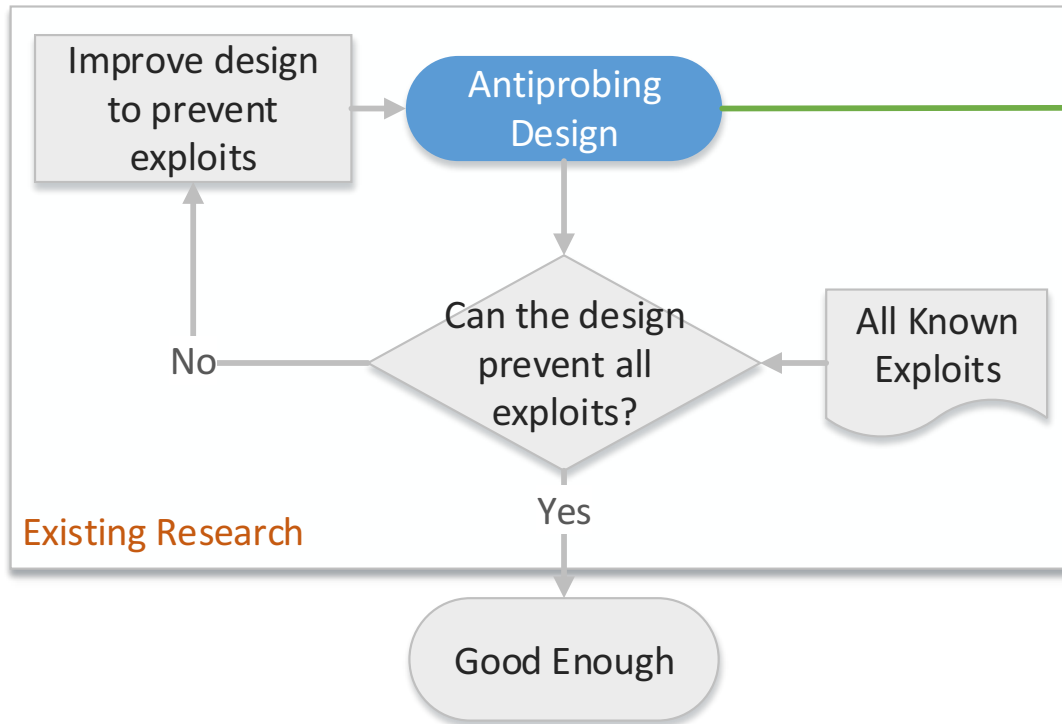
Bypass Attack



- **Security intensive hardware require realistic protection standards**
 - Smartcards, security tokens: mass-produced, might not afford shield
- **High-end protection need complete awareness of threat**
 - Even high-end products are vulnerable to control circuitry editing
 - Security is never absolute: better expressed as cost for attacker
- **Technology advance demands re-evaluation on old design**
 - Legacy generation of protection design needs security evaluation in updated threat environment
 - Especially for mass-produced devices

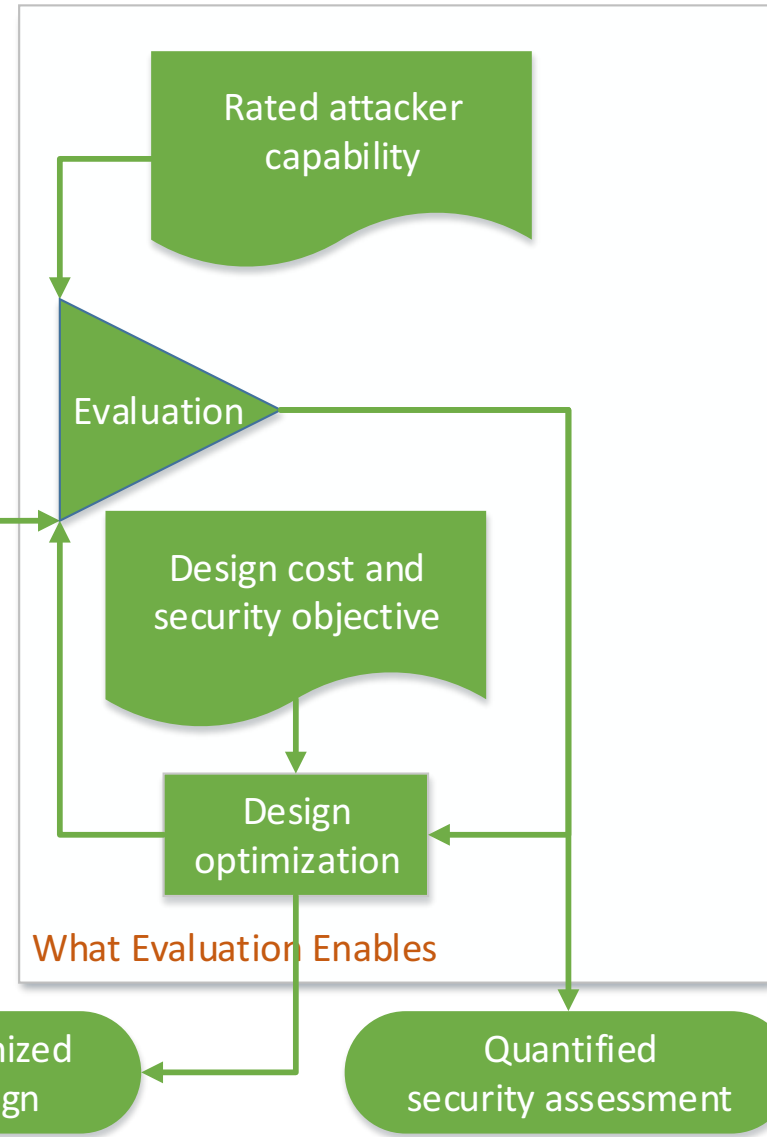
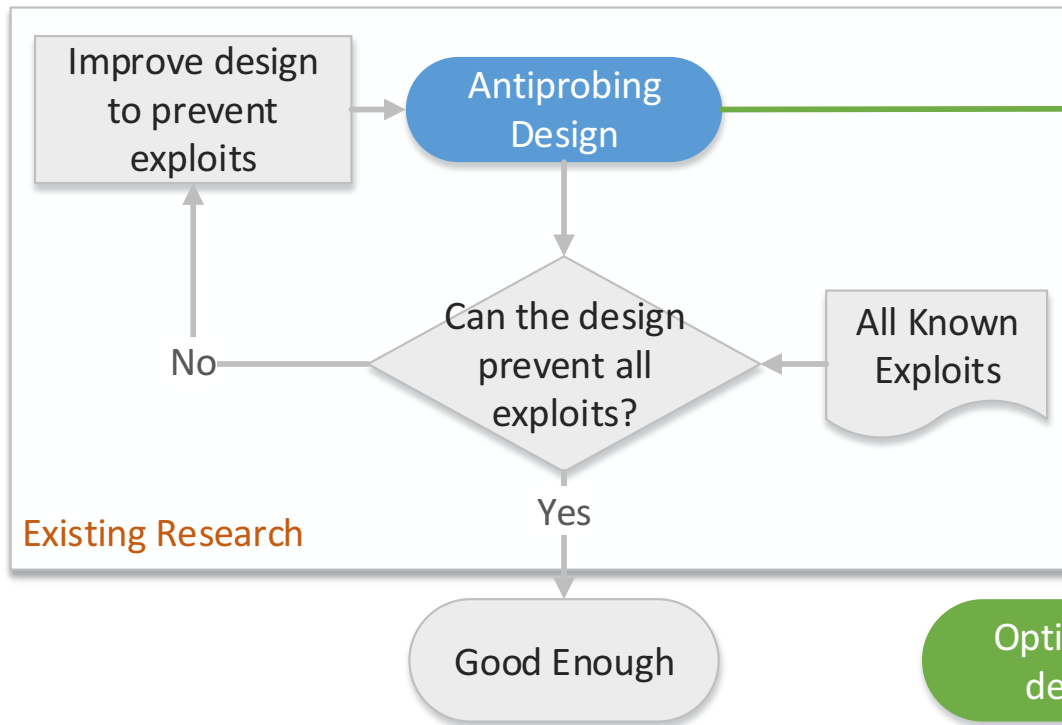
What Evaluation Enables

Evaluation of antiprobing designs provides a realistic and quantifiable security assessment based on well-defined attacker capability;



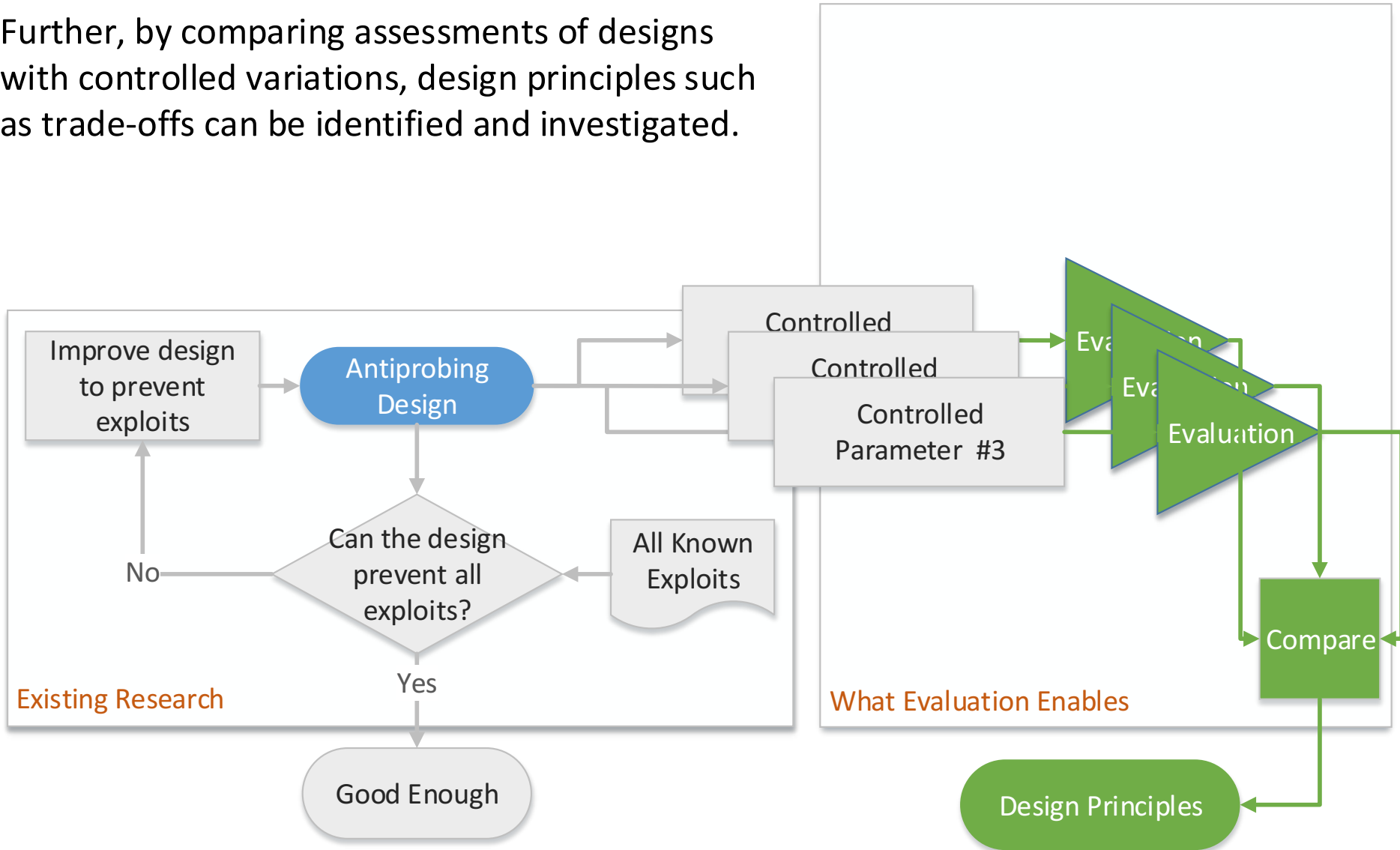
What Evaluation Enables

Evaluation of antiprobing designs provides a realistic and quantifiable security assessment based on well-defined attacker capability; With the help of this, designs could be optimized for best trade-off between design cost and security objective.



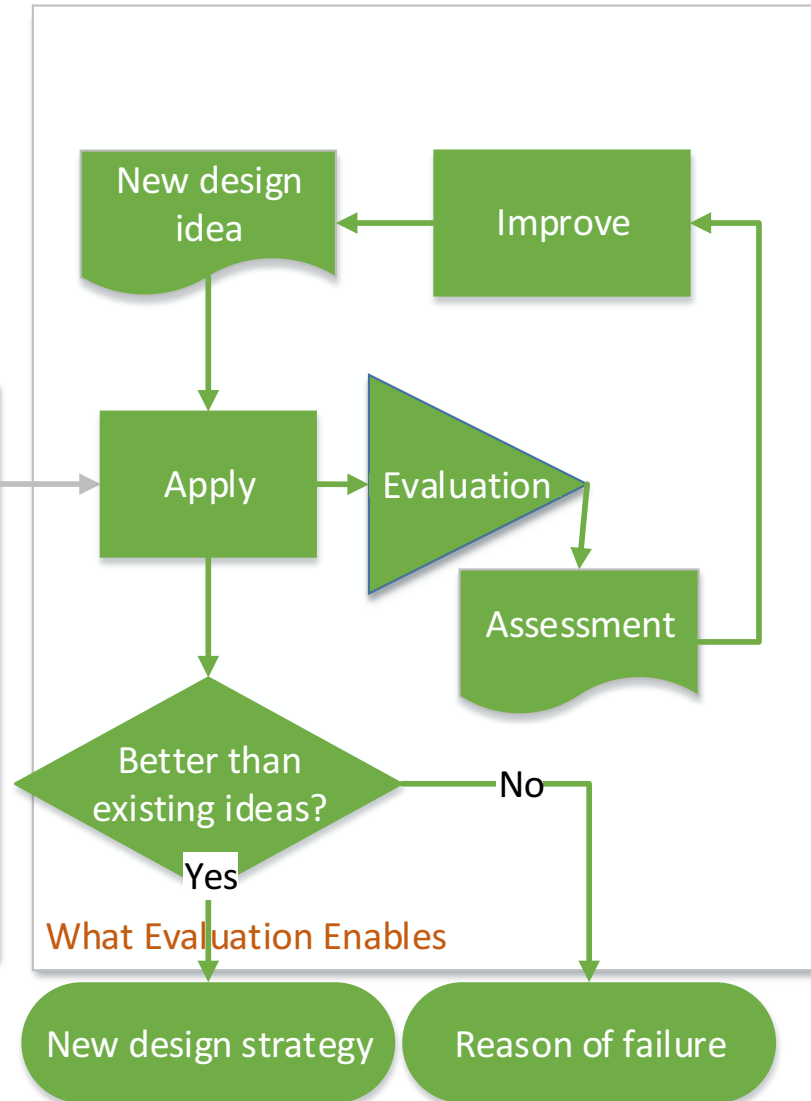
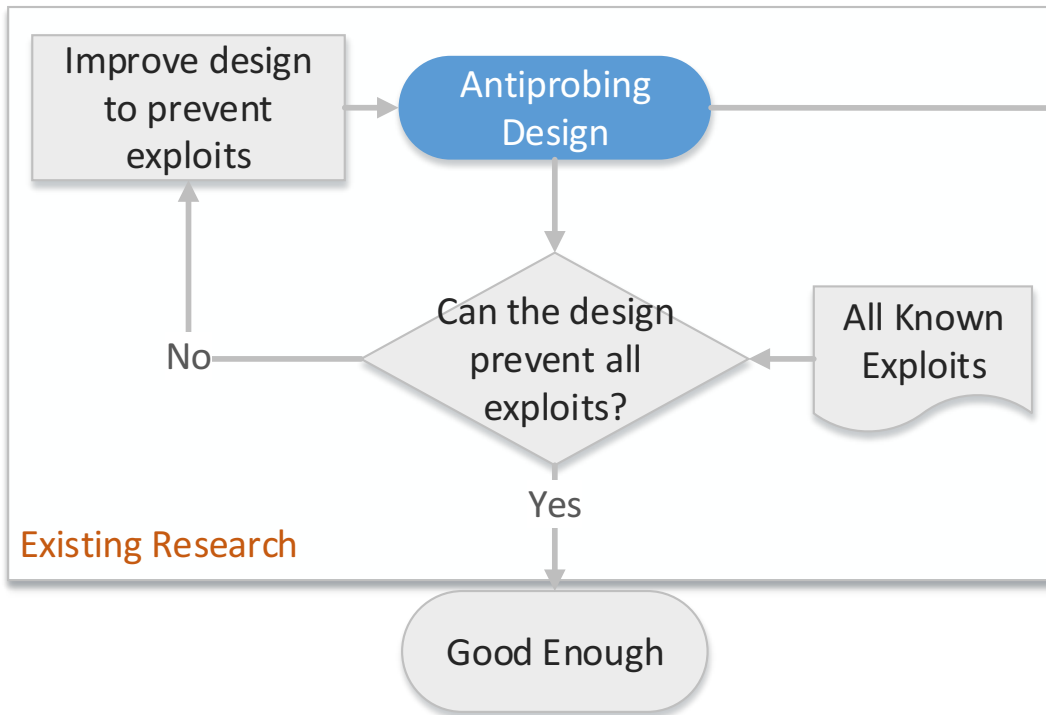
What Evaluation Enables

Further, by comparing assessments of designs with controlled variations, design principles such as trade-offs can be identified and investigated.



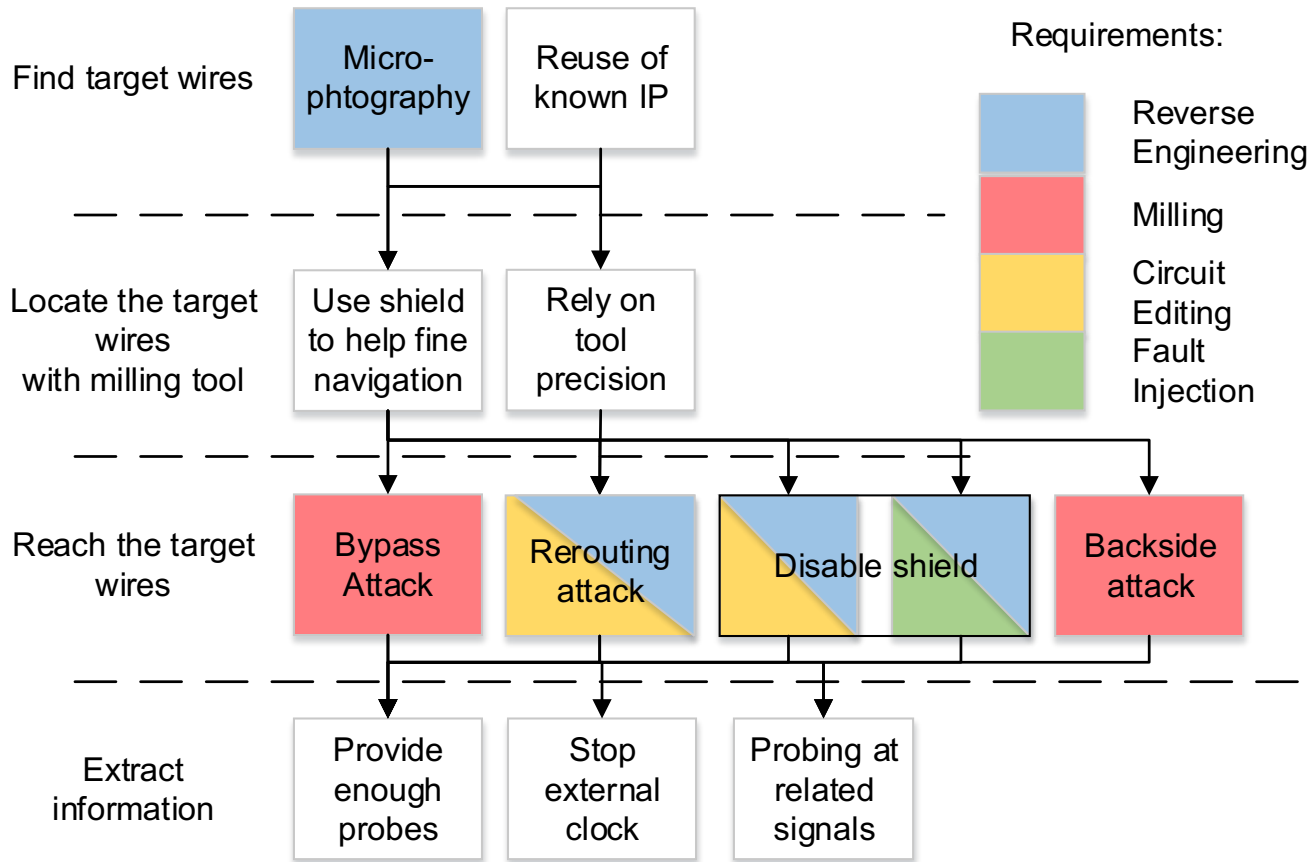
What Evaluation Enables

Additionally, evaluation could be performed on **new design ideas**, for example new mesh designs that does not have to cover a whole layer or restricted to top metal layer.



- **A layout-driven framework to assess designs against microprobing attacks**
 - Performance metric derived based on known attacks *modus operandi*.
 - We discover bypassing attack deserves particular attention
 - An algorithm based on a mainstream layout editor to evaluate exposed area of targeted wires.
 - Exposed area as a quantitative evaluation method
 - Case studies on protection design principles with proposed algorithm on OpenSPARC T1 core.
 - Findings: traditional top layer shield deteriorates fast as R_{FIB} increases; functional wires provide coverage but is not sufficient on its own
 - Thorough mathematical analysis on bypassing attack.
 - Protecting against bypassing attack requires layout knowledge as well

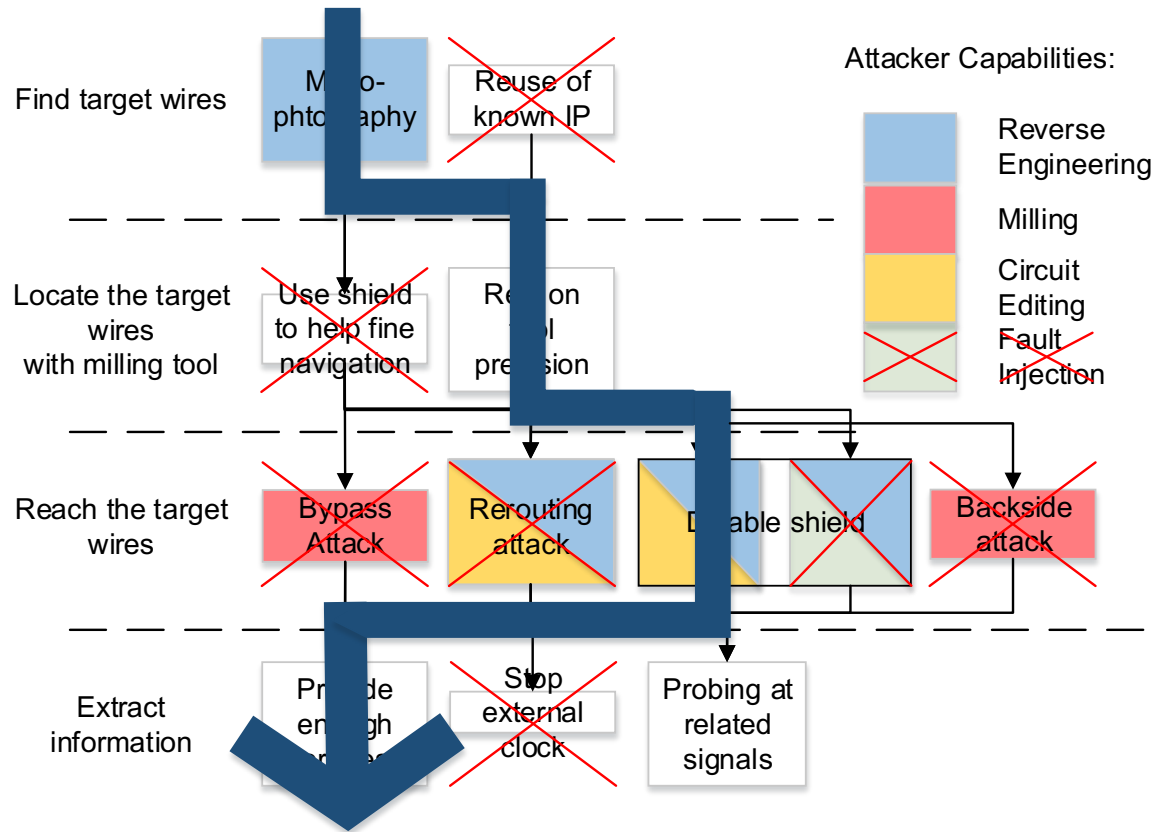
Proposed Framework for Assessment



- Assessment based on essential steps of microprobing attack
- Each step consists of alternatives of varying requirements and time cost

Assessment Principle

- Example assessment on state-of-art shield (figure)
- Alternatives resized to represent typical time cost
- Consider all attack alternatives in terms of the capability and time cost they require

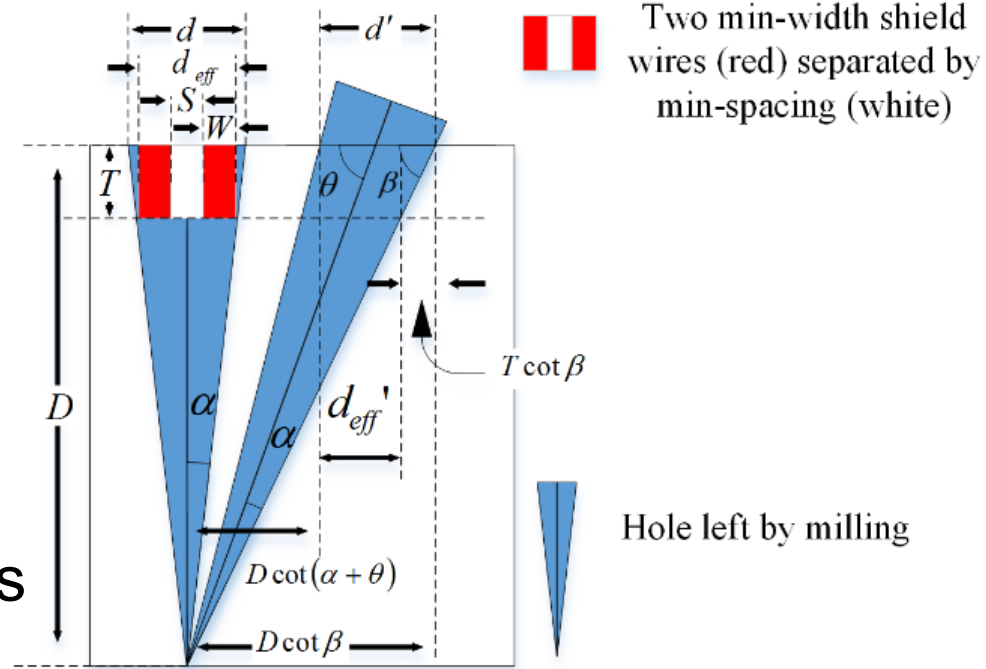


Rule: Security is defined as **sum of lowest time cost** of alternatives available to that level, against **attackers** with **rated level of capability**

Bypass Attack: How safe are we?

- What if the attacker choose to mill at angle θ ?
- As shown in figure, d_{eff}' replaces d_{eff} in perpendicular milling

- Solving for $\frac{\partial \left(\frac{d_{eff}'}{d_{eff}} \right)}{\partial \theta} = 0$ yields

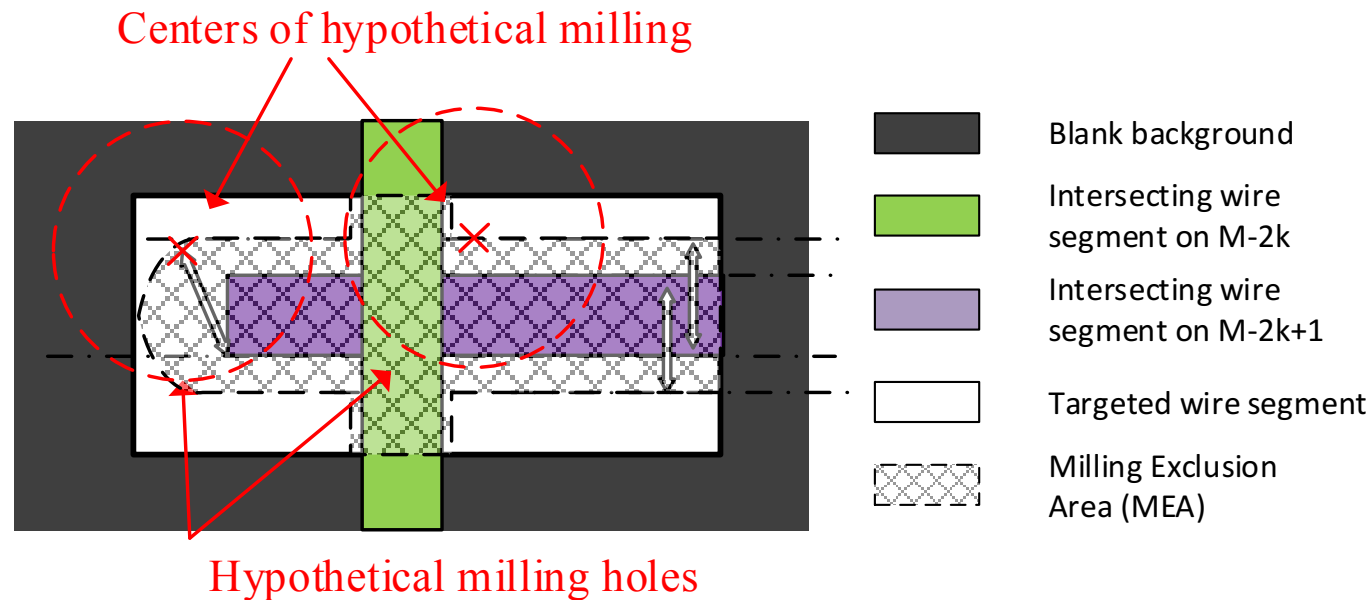


R_{FIB}	5	6	7	8	9	10
Reduction (%)	7.88	9.42	10.53	11.37	12.02	12.55
Optimal angle(°)	68.93	68.69	68.52	68.38	68.28	68.19

Takeaway: bypass attack can become more penetrating depending on layout – **layout information is important**

Find Exposed Area in a Wire Segment

- Consider one rectangular wire segment (“targeted wire”) below rectangular wire segments (“Intersecting wire”)

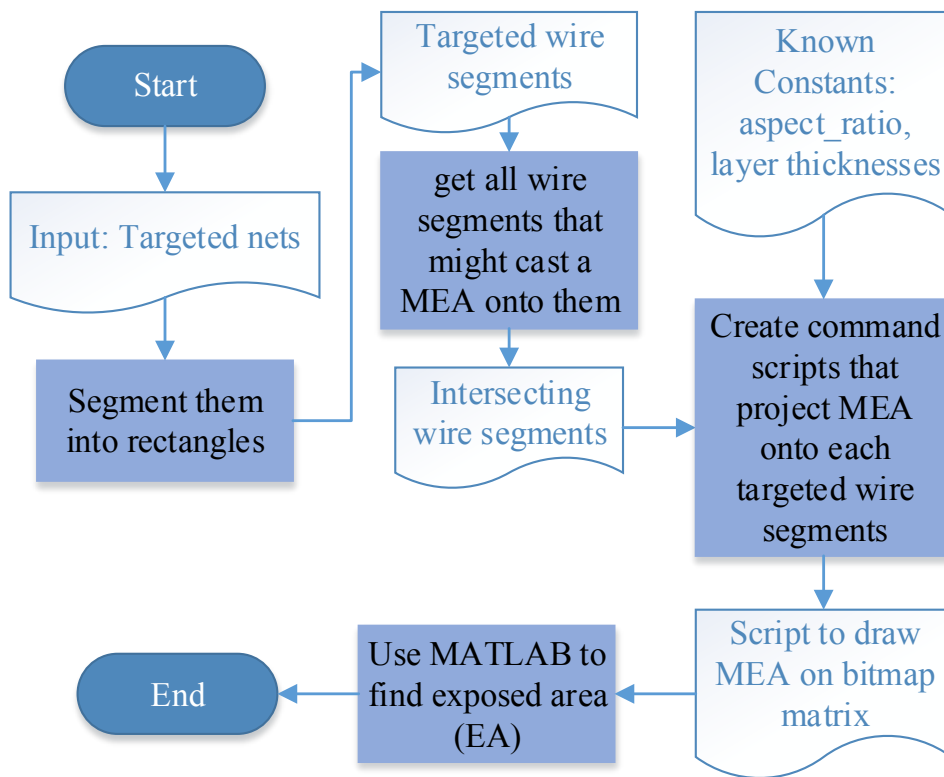


* Figure shows top-down view of an layout

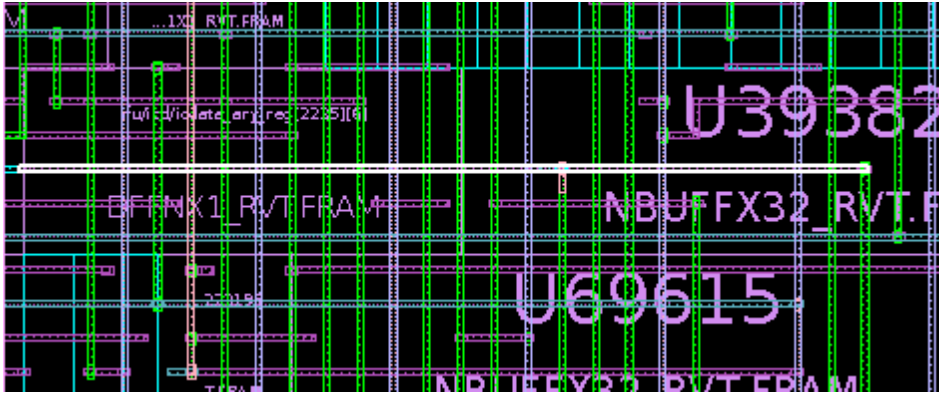
- Milling-Exclusion Area (MEA)**
 - Complement of MEA is the desired **Exposed Area (EA)**
 - If center of milling falls in MEA, an intersecting wire will be completely cut
 - Overall MEA found by adding MEA from each intersecting wire together




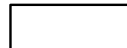
Algorithm to Find Exposed Area

- Rectangular wire segments supplied in all mainstream layout editors (IC compiler/Encounter/..)
- Iterate through each rectangular wire segments for all targeted wires
- MEA found by plotting into bitmap matrices
- EA can be easily found by finding spaces

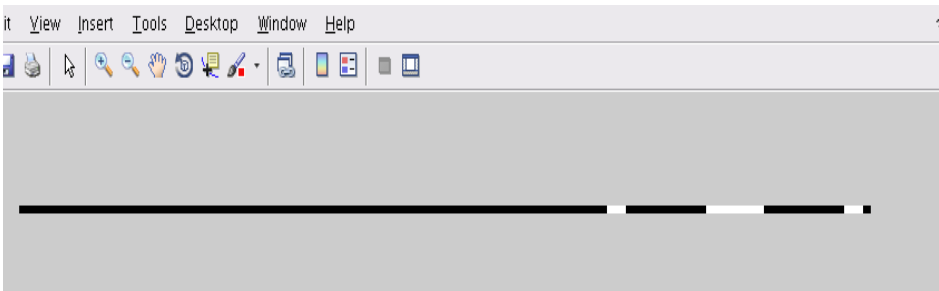



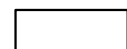
Sample Results of the Algorithm



-  Blank background
-  Intersecting wire segment on $M-2k$
-  Intersecting wire segment on $M-2k+1$
-  Targeted wire segment

Layout view of targeted wire (highlighted)



-  Milling Exclusion Area (MEA)
-  Exposed Area (EA)

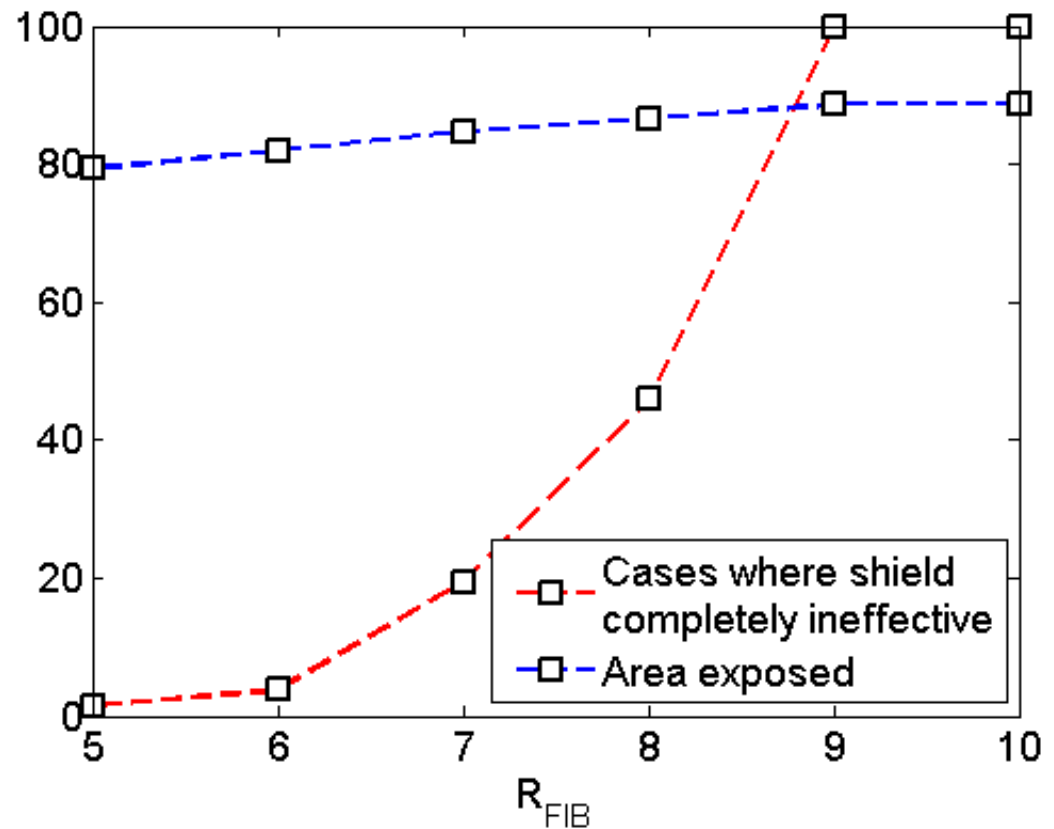
Found Exposed Area (white space)

Easily found from bitmap: 11.2
4% of total area are exposed.

Case Study: Shield Efficacy wrt. R_{FIB}

- OpenSPARC T1 core
- Synopsys SAED 32nm library
- Assumptions
 - active shield in place on top layer
 - Attacker target long nets ($> 500 \mu\text{m}$, top 1%)

Performance degradation of shield at top layer as R_{FIB} increases

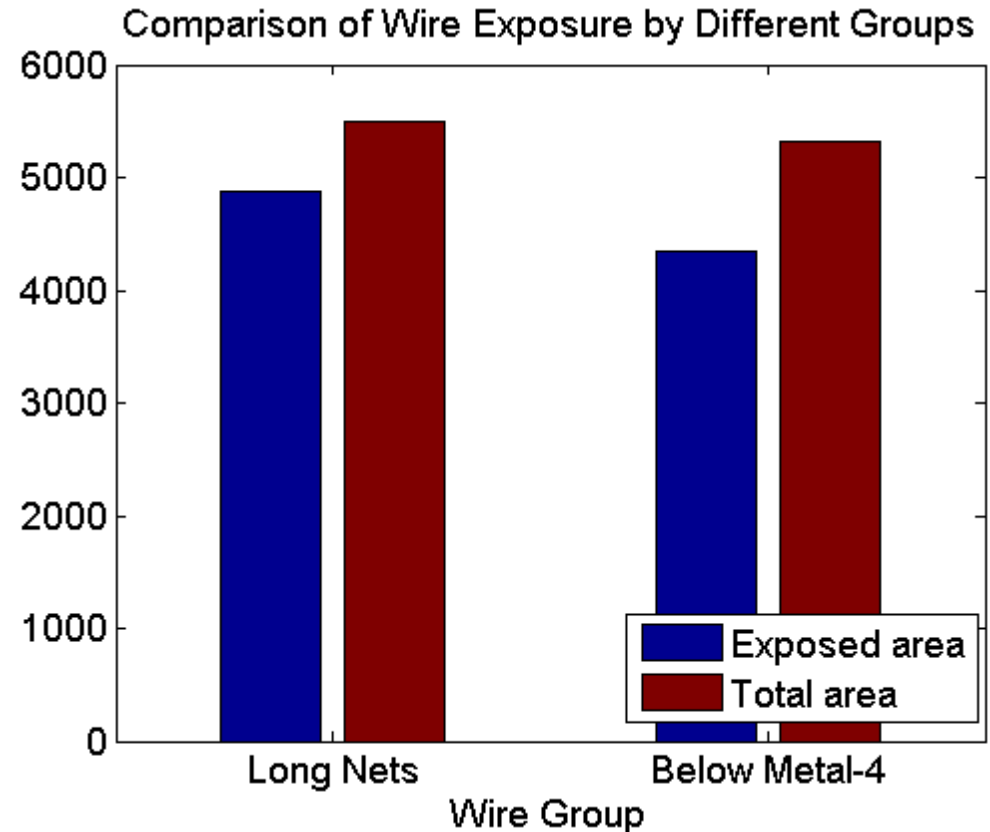


Takeaways:

1. Top layer shield **soon ineffective** against high R_{FIB}
2. **Functional routing helps** where shield fails

Case Study: Layers of Targeted Wires

- Compare two groups of candidate wires
 - Long nets ($> 500 \mu\text{m}$, top 1%)
 - Random sub-M4 layer nets



Takeaways:

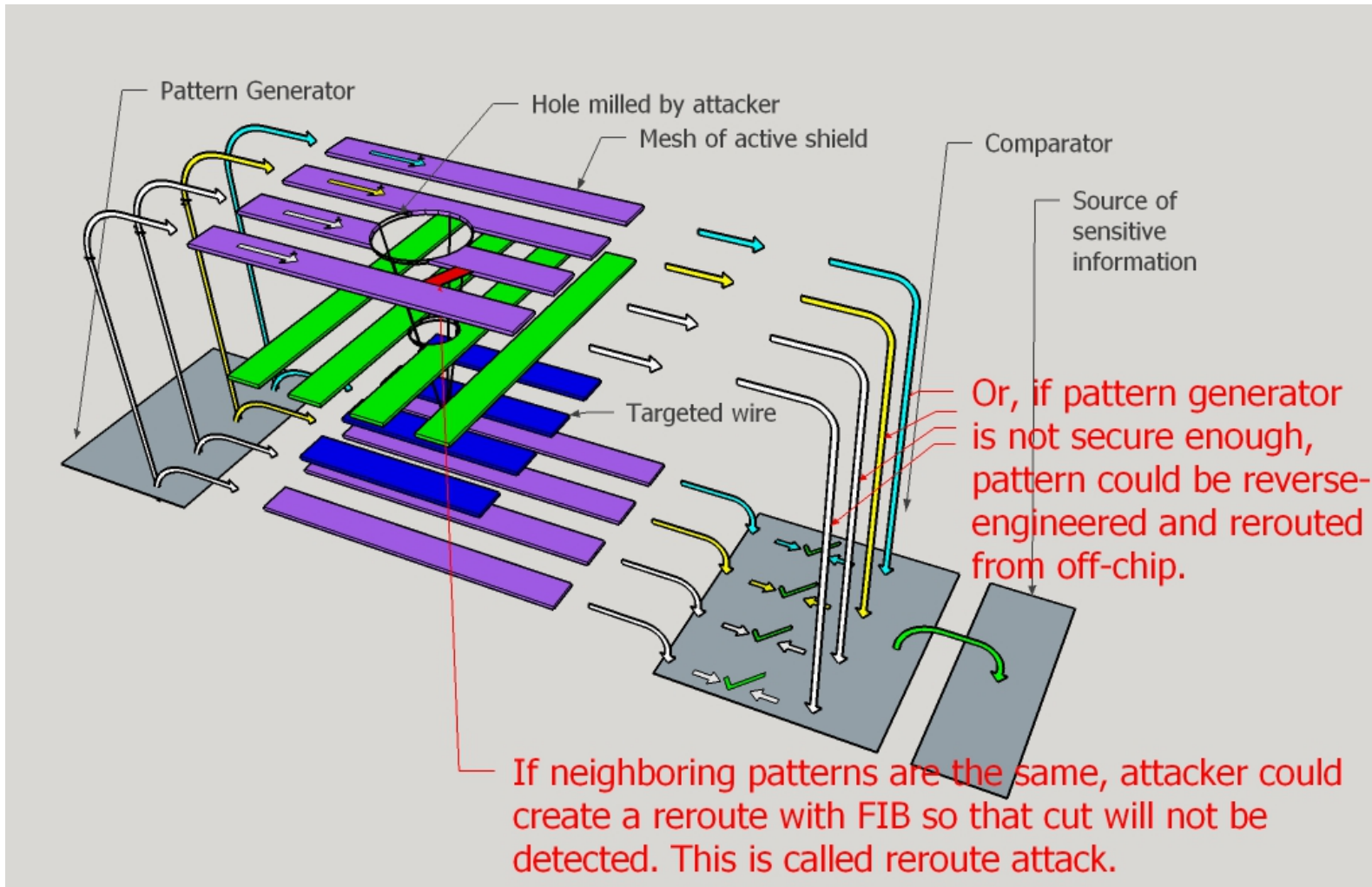
1. **Lowering targeted wire layer helps**
2. **Functional wires** alone may **not** give **sufficient coverage**
3. Future work: **Combining** functional wires with shield mesh

- Existing anti-probing designs reviewed
- **Layout-based assessment framework** and **tool** developed
- Questions on design principles investigated
 - Layout information essential in security against bypass attack
 - Top metal shield found to deteriorate fast as R_{FIB} increases
 - Lower layer wires are better covered by functional wires; however functional wire alone is not sufficient
- **Future works**
 - Alternative shield not restricted to top metal layer
 - Shield and functional wires that complements each other

Thank You!



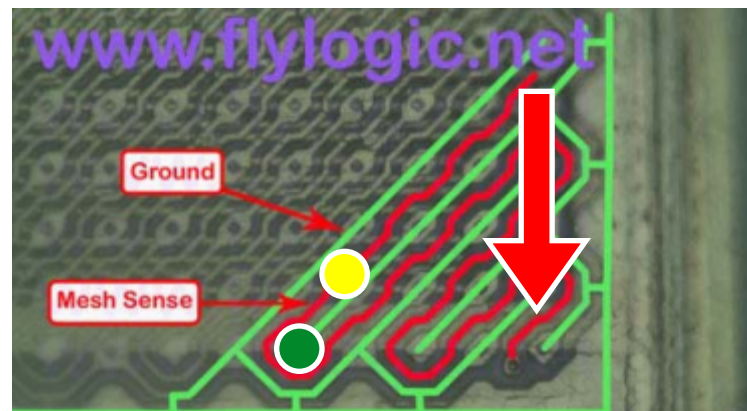
Reroute Attack



Microprobing Technique Examples

- Rerouting attack

- Create wire as shown by the arrow
- Then attacker can remove most “mesh sense”
- This leads to active shield design principles:
 - Never “serpentine”
 - Use independent signals on neighboring wires
 - Cover entire layer; don’t leave room to reroute



Active shield using single serpentine route [17]

- Bypassing attack

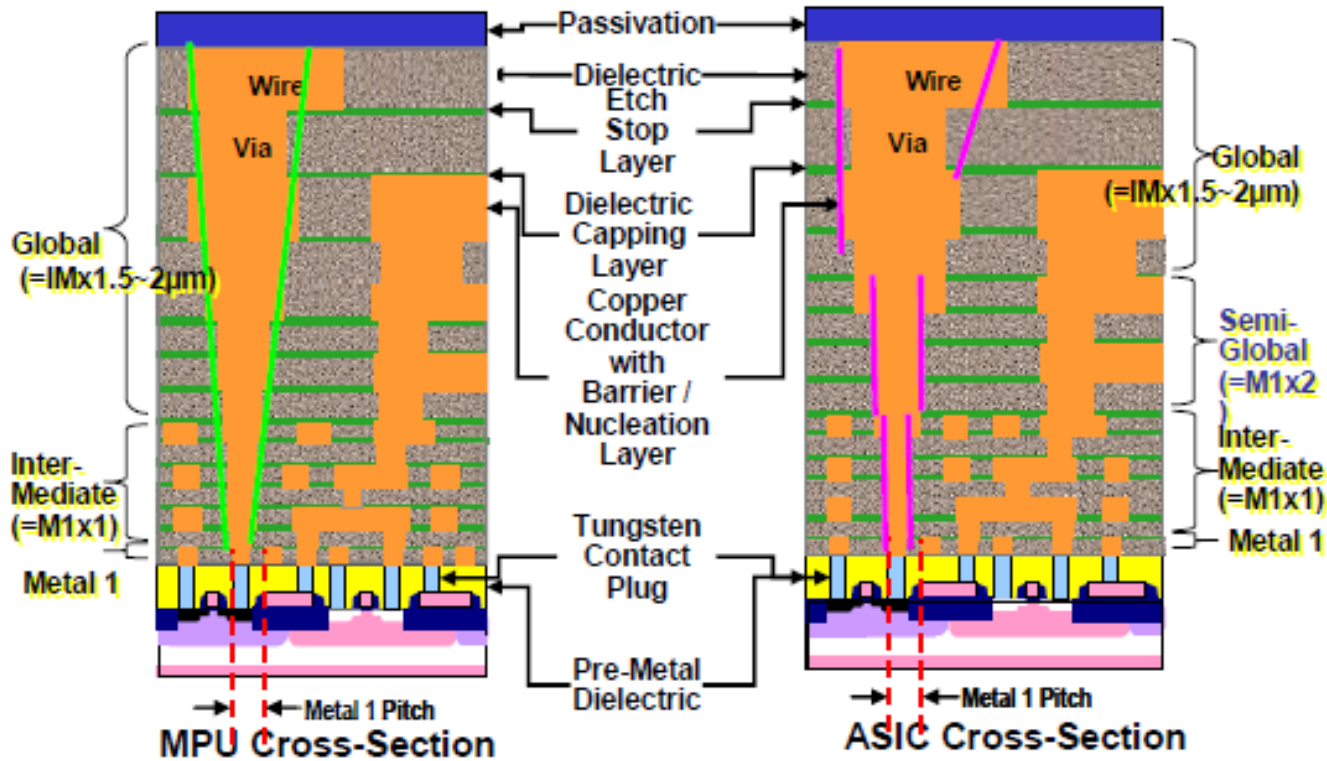
- FIB milling leaves holes on top layer
- Milling can be positioned so that shield wires are not cut (green circle), if R_{FIB} is high enough

- Prediction attack

- If shield signals predictable, attacker could cut wires and play them at shield detection circuit
- Shield signals should not be predictable: cryptographically secure signals [10]

- t -private circuits: modify netlist so that attack requires at least $t + 1$ probes^[14]
 - However, circuit designers are not known for their love of 3rd party modifications on their designs
- PAD: Detect capacitance change on sensitive wires^[12]
 - Problem: most sensitive information can be probed from more than a few nets PAD can protect ^[15]
- Therefore, active shield designs still are in majority
- Attackers and antiprobing designers focus on exploits to defeat shields

Background: Min-Width by Layers

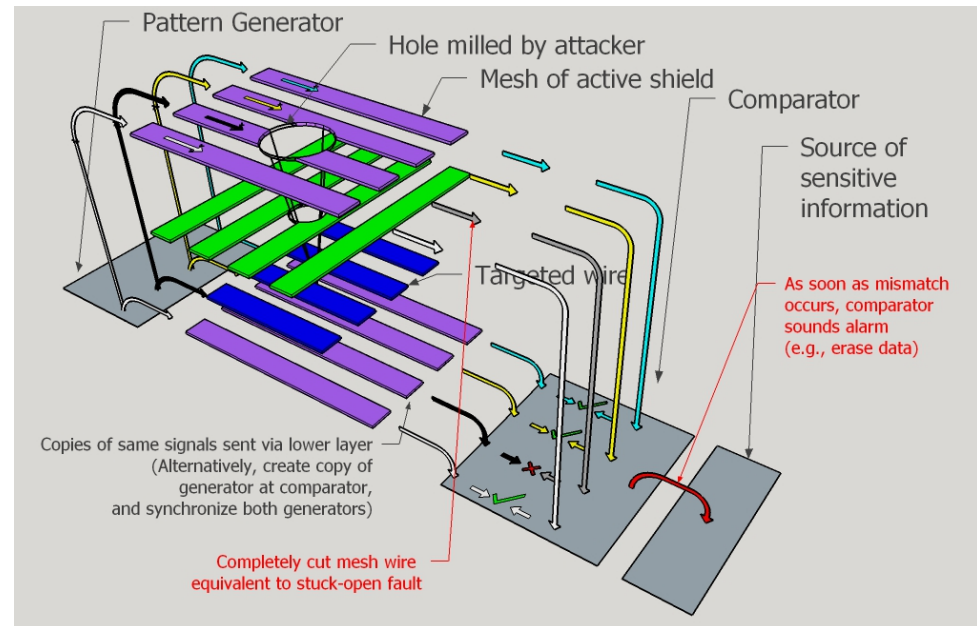


Typical cross-sections of microprocessors (MPU) and Application-Specific Integrated Circuits (ASIC) [19]

- Top layers too wide; less suitable than lower layers
- Since shields have to cover entire layer, have to use top layers or giving up all layers above shield

Problem Formulation: Assumptions

- Designer use top layer for active shield
- Attacker's best case: able to place hole in the middle between shield wires
- Design protected against known exploits
- Use straight wires, feed independent and cryptographically secure patterns, etc.
- Design relies on complete cuts for detection
 - All existing digital shields rely on complete cuts
 - Detection based on partial cut might be possible; however, parametric measurements are inherently uncertain, yielding possible detections at best



Problem Formulation: Milling at Angle

- If instead of perpendicular milling, the attacker choose to mill at angle θ ?
- As shown in figure, d_{eff}' replaces d_{eff} in previous equation
- Solving for $\frac{\partial(d_{\text{eff}}')}{\partial\theta} = 0$ yields

- $\theta_0 = \frac{1}{2} \arccos\left(\frac{bc - \sqrt{b^2c^2 - (a^2 + b^2)(a^2 - b^2)}}{a^2 + b^2}\right)$, where

- $a = (2(A/R)\tan\alpha + 6)\sin 2\alpha$
- $b = 2(A/R)\tan\alpha \cos 2\alpha$
- $c = 2(A/R)\tan\alpha$

- If instead of perpendicular milling, the attacker choose to mill at angle θ ?
- As shown in figure, d_{eff}' replaces d_{eff} in previous equation

Proposed Framework for Assessment

- Assessment rules
 - Consider all attack alternatives and the capability and time cost they require
 - Protection against attackers with given level of capability is given by **sum of lowest time cost of alternatives available** to that level of capability of each step
- Example

Designs	Performance against				
	Bypass Attack	Reroute Attack	Disable Shield	Backside Attack	Related Signals
Analog Shield	Weaker [15]	Unprotected	Unprotected	Unprotected	Protected
Random Active Shield[11]	Protected	Increased reverse engineering	Unprotected	Unprotected	Protected
Cryptographically Secure Shield [10]	Protected	Protected	Unprotected	Unprotected	Protected
PAD[12]	N/A	N/A	Unprotected	Unprotected	Unprotected

- Bypass attack is likely fastest, deserves particular interest
- Still worth avoiding cutting more wires after getting past the shield – each cut wire introduces more reverse engineering
- Therefore, exposed area of targeted wires are of interest too
- We have studied these two aspects in detail and will show you what we found

- Active shield might not need to completely cover the design to achieve good all-around protection
 - Shield wires can be **relocated to lower layers** for better protection against high R_{FIB} attackers
 - Now **cost-sensitive designs and technologies with few layers** can be protected too
- Finding Exposed Area opens up possibility to protect security sensitive wires **with multiple layers of routes**
 - Functional routes can be utilized by encrypting them
 - Multiple layers of routes could prove to be more resilient than top layer shields, since simultaneously rerouting wires on multiple layers can be difficult

Implementation Results

- Layout: OpenSPARC T1 core(Synopsys SAED 32nm library)
- Candidates:
 - Random sub M4 layer nets
 - Long nets ($> 500 \mu\text{m}$, top 1%)
- Evaluation of Performance (right)
- Evaluation of hypothetical active shield on MRDL layer (bottom)
 - takeaway: top layer shield soon ineffective against high R_{FIB} attackers

TABLE III: Evaluation results on long nets and nets on low layers

Performance	Nets on Metal-4 or Lower Layers	Long Nets
Total Number of Nets	5000	128
Total Processing Time (s)	27145	11708
Processing Time per Unit Area ($s/\mu\text{m}^2$)	5.1242	2.1297
Total Area (μm^2)	5320.58	5497.66
Exposed Area (μm^2)	4339.84	4869.21

TABLE IV: Evaluation of active shield performance

R_{FIB}	5	6	7	8	9	10
Performance						
% shield ineffective (%)	1.52	3.82	19.50	45.90	100	100
Exposed Area (μm^2)	4364.63	4507.47	4656.88	4760.98	4869.21	4869.21

References

1. Skorobogatov, S., "Physical attacks on tamper resistance: progress and lessons," Proc. of 2nd ARO Special Workshop on Hardware Assurance, Washington, DC., 2011
2. Anderson, R., "Security engineering: A guide to building dependable distributed systems," Wiley, 2001.
3. Fu, Y.; Ngoi, K. A. B., "Investigation of aspect ratio of hole drilling from micro to nanoscale via focused ion beam fine milling," 2005
4. Wu, H.; Ferranti, D.; Stern, L., "Precise nanofabrication with multiple ion beams for advanced circuit edit," in Microelectronics Reliability, vol. 54, iss. 910, pp. 1779-1784, September-October 2014
5. Boit, C.; Helfmeier, C.; Kerst, U., "Security Risks Posed by Modern IC Debug and Diagnosis Tools," in Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on, IEEE, pp. 3-11, August 2013
6. Quadir, S. E.; Chen, J.; Forte, D.; Asadizanjani, N.; Shahbazmohamadi, S.; Wang, L.; Chandy, J.; Tehranipoor, M., "A Survey on Chip to System Reverse Engineering," to appear ACM Journal on Emerging Technologies in Computing Systems (JETC).
7. Laackmann, P.; Taddiken, H., "Apparatus for protecting an integrated circuit formed in a substrate and method for protecting the circuit against reverse engineering," U.S. Patent No. 6,798,234. 28 September 2004
8. Ling, M.; Wu, L.; Li, X.; Zhang, X.; Hou, J.; Wang, Y., "Design of Monitor and Protect Circuits against FIB Attack on Chip Security," in Computational Intelligence and Security (CIS), 2012 Eighth International Conference on , pp.530-533, 17-18 November 2012
9. Beit-Grogger, A.; Riegebauer, J., "Integrated circuit having an active shield," U.S. Patent No. 6,962,294. 8 November 2005
10. Cioranescu, J.-M.; Danger, J.-L.; Graba, T.; Guilley, S.; Mathieu, Y.; Naccache, D.; Xuan Thuy Ngo, "Cryptographically secure shields," in Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on , vol., no., pp.25-31, 6-7 May 2014
11. Briais, S.; Cioranescu, J.-M.; Danger, J.-L.; Guilley, S.; Naccache, D.; Porteboeuf, T., "Random Active Shield," in Fault Diagnosis and Tolerance in Cryptography (FDTC), 2012 Workshop on , pp.103-113, 9-9 September 2012
12. Manich, S.; Wamser, M.S.; Sigl, G., "Detection of probing attempts in secure ICs," in Hardware-Oriented Security and Trust (HOST), 2012 IEEE International Symposium on, pp.134-139, 3-4 June 2012

References

13. Wei, L.; Zhang, J.; Yuan, F.; Liu, Y.; Fan, J.; Xu Q., "Vulnerability analysis for crypto devices against probing attack," in Design Automation Conference (ASP-DAC), 2015 20th Asia and South Pacific , vol., no., pp.827-832, 19-22 January 2015
14. Ishai, Y.; Sahai, A.; Wagner, D., "Private circuits: Securing hardware against probing attacks," Advances in Cryptology-CRYPTO 2003. Springer Berlin Heidelberg, 2003. 463-481.
15. Ray V., "FREUD Applications of FIB: Invasive FIB Attacks and Countermeasures in Hardware Security Devices", East-Coast Focused Ion Beam User Group Meeting, February 2009
16. Tarnovsky C., "Tarnovsky Deconstruct Processor," Youtube, <https://www.youtube.com/watch?v=w7PT0nrK2BE>, 2013
17. Tarnovsky C., "Security Failures In Secure Devices", Black Hat Briefings, February 2008
18. FreePDK45: Metal Layers. <http://www.eda.ncsu.edu/wiki/FreePDK45: Metal Layers>
19. International Technology Roadmap for Semiconductors 2013 Edition. <http://www.itrs.net/ITRS%201999-2014%20Mtgs,%20Presentations%20&%20Links/2013ITRS/Home2013.htm>
20. Wu, H.; L. Stern; D. Xia; D. Ferranti; B. Thompson; K. Klein; C. Gonzalez;P. Rack, "Focused Helium Ion Beam Deposited Low Resistivity Cobalt Metal Lines with 10 nm Resolution: Implications for Advanced Circuit Editing," Journal of Materials Science: Materials in Electronics 25 (2): 587-595, 2014
21. Sidorkin, V.; vanVeldhoven, E.; vanderDrift, E.; Alkemade, P.; Salemink, H.; Maas, D., "Sub-10-nmnanolithographywithascanningheliumbeam," Journal of Vacuum Science & Technology B, 27, L18-L20, 2009