iProbe - An Internal Shielding Approach for Protecting Against Frontside and Backside Probing Attacks

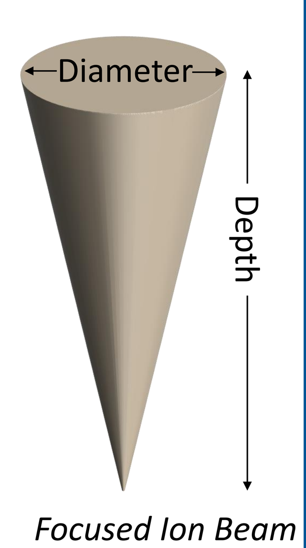
Huanyu Wang, Ana Covic, Qihang Shi, Mark M. Tehranipoor, and Domenic Forte
Department of Electrical and Computer Engineering, University of Florida

Motivation

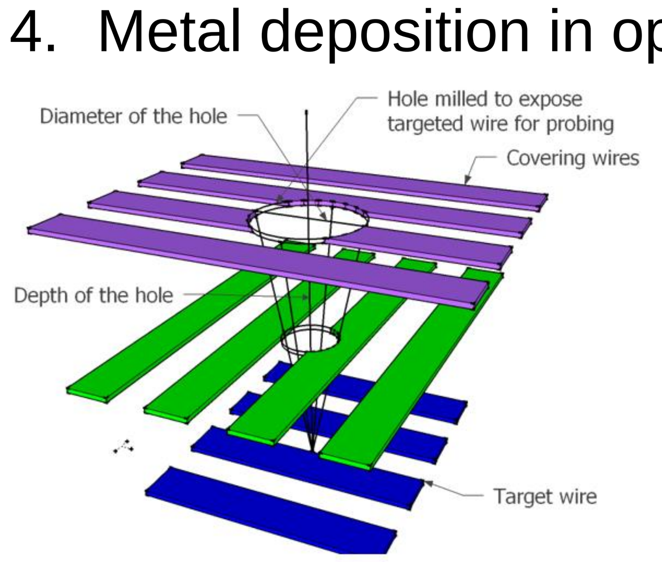
- Sensitive information or assets, e.g. encryption keys, within SoCs need to be properly protected
- Physical attacks, e.g. FIB-based probing attacks, are very powerful at extracting these security critical info
- Existing <u>frontside</u> solution, e.g. active shield, analog shield, or *t*-private, have been proven inefficient and expensive
- Specific backside countermeasures <u>do not exist</u>
- We propose a FIB-aware anti-probing physical design flow to mitigate frontside probing attacks vulnerability
- We propose backside attack model on latest technologies and possible countermeasure

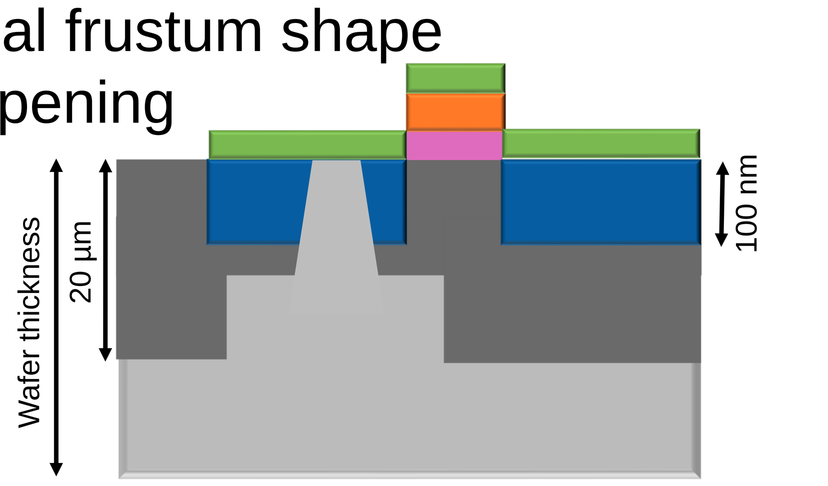
Background

- **Asset Examples:**
  encryption keys, device configuration, manufacturer firmware, RNG, communication credential, secret data
- **Focused Ion Beam (FIB)**
  - Powerful tool used in development, manufacturing, and editing of ICs, can do milling and depositing on ICs
  - Aspect ratio → $R_{FIB} = \frac{Depth}{Diameter}$



- **Probing Attack**
  Probing at signal wires to extract assets
- **Frontside Active Shield Limitations**
  - Occupy at least one routing layer
  - Need pattern generator
  - Vulnerable to bypass and reroute attack
  - Disabled by editing its control circuit
- **Contact-to-Silicide Backside Attack**
  1. Bulk silicon removal to 20 μm thickness using mechanical polishing / plasma etching
  2. FIB silicon removal to 100 nm thickness
  3. FIB opening → conical frustum shape
  4. Metal deposition in opening





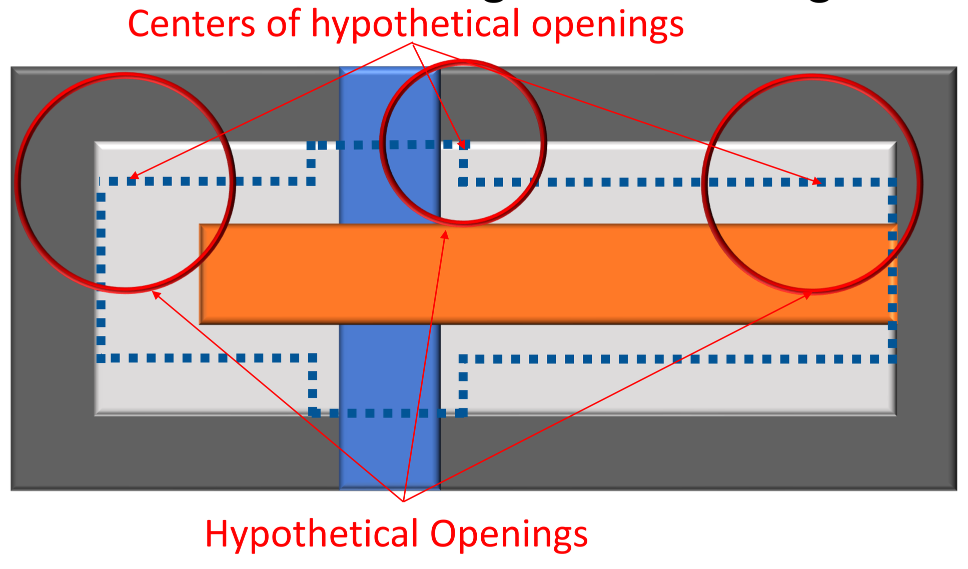
Frontside Protection Approach

Milling - Exclusion Area (MEA)

- The area in which milling center should not fall inside based on FIB parameters (FIB Aspect Ratio).

Exposed Area (EA)

- Complement of MEA on target wires
- Vulnerable designs have large EA to probing attack

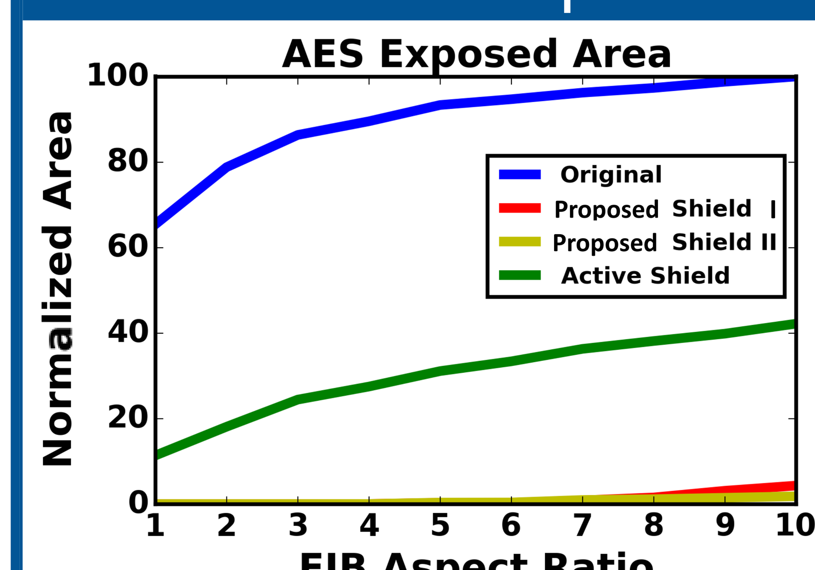


Evaluation of Proposed Automated Approach on AES

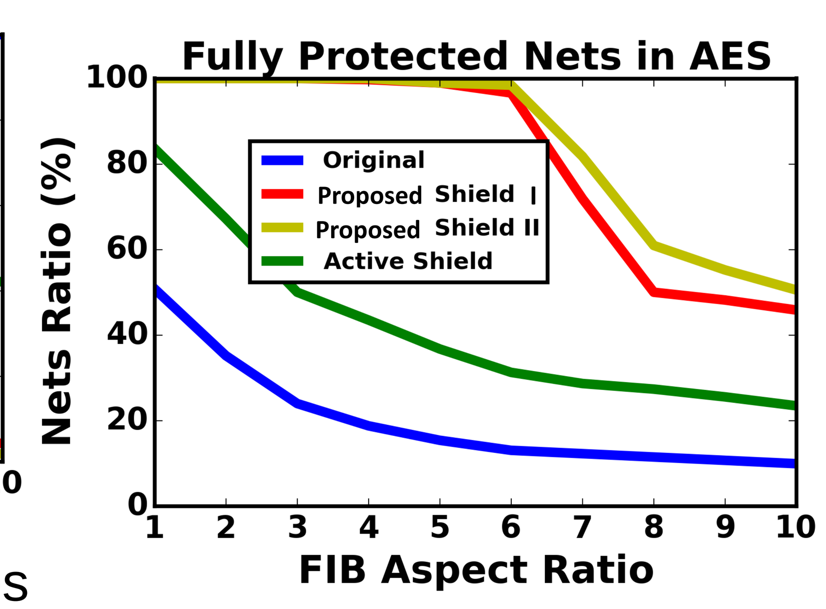
- Two level nets in the fanout of AES encryption keys are identified as target nets (384 nets in total)
- Single layer M6 and Two-layer M6 M8 → Shield I and II
- <u>**Overhead:**</u> Tremendous improvement compared to conventional shield

Design	Timing [%]	Power[%]	Area[%]	Routing[%]
Proposed Shield I	0.32	2.79	0.74	11.60
Proposed Shield II	0.34	4.90	1.44	17.77
Active Shield	10.53	439.82	402.31	407.40

Exposed Area Results



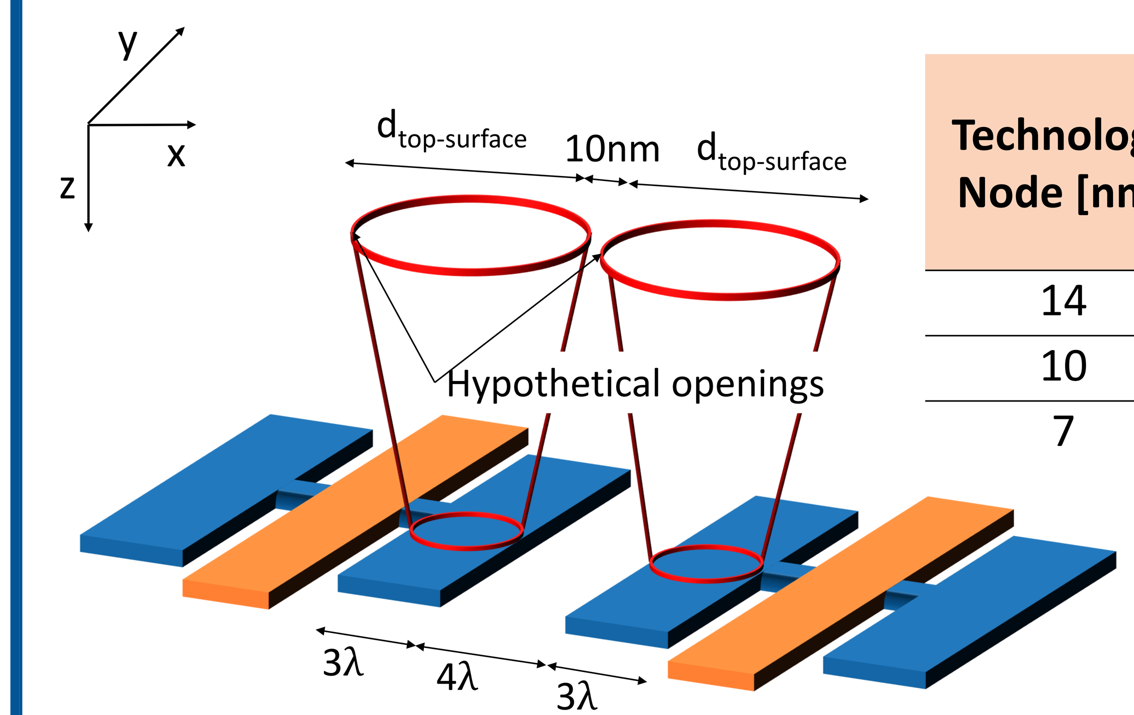
- For $R_{FIB} = 10$, EA decreases by 93% for Proposed Shield I and 95% for Proposed Shield II, with respect to Active shield



- All target nets → Fully protected for $R_{FIB} \leq 5$

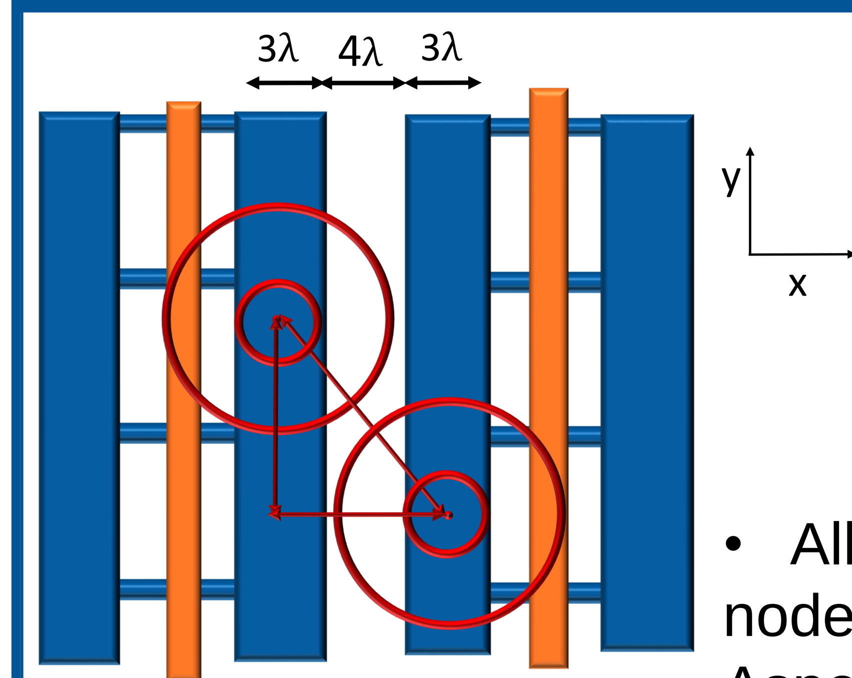
Backside Protection Approach

Attack Model on Single-fin FinFET



Technology Node [nm]	Aspect Ratio			
	3	5	8	10
	$d_{top\text{-}surface}$ [nm]			
14	57.3	44	36.5	34
10	51.3	38	30.5	28
7	45.3	32	23.5	22

Attack Model on Multi-fin FinFET



Technology Node [nm]	Aspect Ratio			
	3	5	8	10
	Number of Fins			
14	2	1	1	1
10	3	2	1	1
7	4	3	2	2

- All multi-fin FinFET technology nodes are vulnerable for all Aspect Ratios

Countermeasure: Metal Shield

- Backside metal shield connected to frontside shield with Through Silicon Vias (TSV)
- Impedance and Logic matching
- <u>**Area overhead**</u>: 16%
- Time to perform attack on protected die increases by:

$$\Delta t = t_{\text{Metal-trace-removal}} + t_{\text{TSV removal}} + t_{\text{FIB-opening}} + t_{\text{Re-routing}} + t_{\text{Lithography}}$$

Conclusion and Future Work

- An IC layout susceptibility to FIB based probing attacks can be quantified
- The overhead and effectiveness of active shields against frontside probing can be improved by automated CAD approaches
- More investigation is needed to prevent backside probing by Contact-to-Silicide and Contact-to-Metal