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

Challenges:

Focused Ion Beam (FIB) is a powerful integrated circuit (IC) edit tool capable of

- Accessing & probing on-chip assets
- Bypassing hardware protection mechanisms

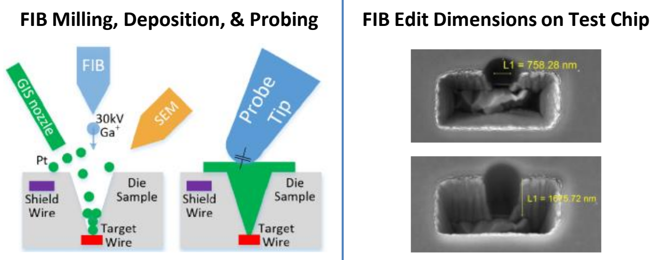
Existing computer-aided design & electronic design automation (CAD/EDA) tools do not consider security of IC layout

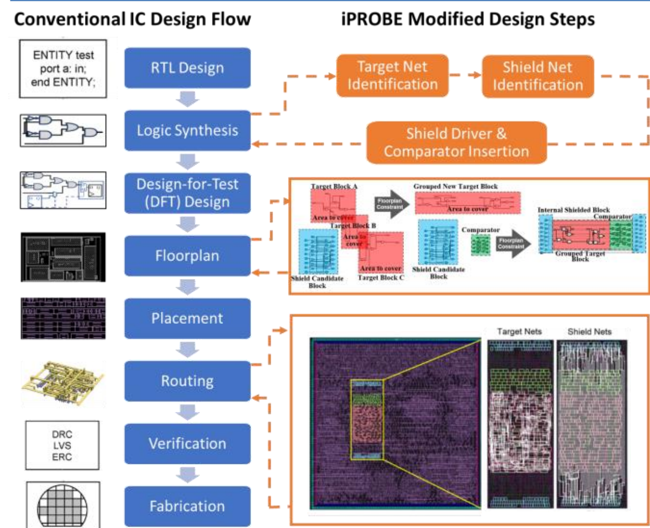
Solutions:

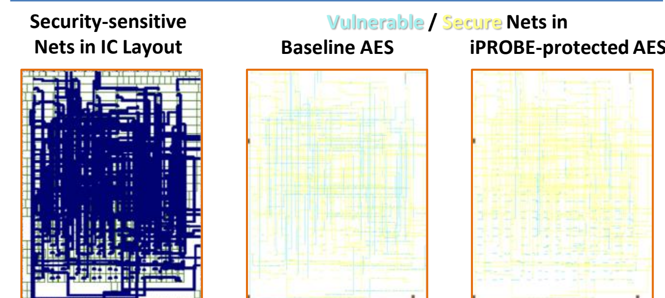
iPROBE consists of a suite of approaches compatible with commercial CAD/EDA tools to support security-aware physical design

1) Quantifies & visualizes IC layout susceptibility to front- & back-side probing
2) Automatically identifies shield candidate nets & security-sensitive (target) nets
3) Automatically inserts probing detection logic into IC netlist
4) Automatically places-and-routes shields around security-sensitive nets to protect them from front- & back-side probing

Project No.: #1717392
Institution: University of Florida
PI: Domenic Forte, dforte@ufl.edu
Co-PI: Mark Tehranipoor, tehranipoor@ufl.edu







Scientific Impacts:

- Metrics & rules for assessing IC layout vulnerability to bypass attacks, reroute attacks, & angled probing
- Metrics for evaluating & optimizing single & multi-layer shield-based protections
- First look at complimenting physical countermeasures (shields) with theoretical probing (masking) models
- Measurement/demo in 65nm silicon

Broader Impacts:

Low-overhead & quantifiable protection of secret keys, firmware, configuration features, etc. for

- **Gov't/Defense:** Access control cards & classified IP
- **Commercial:** ATM/SIM cards & DRM
- **Society:** Personal information stored in smart/IoT devices

Successful education & outreach

- Supported multiple female PhD students & a post doc
- 8+ publications & 2 patents
- CAD/EDA tool training & tapeout