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

Challenge:

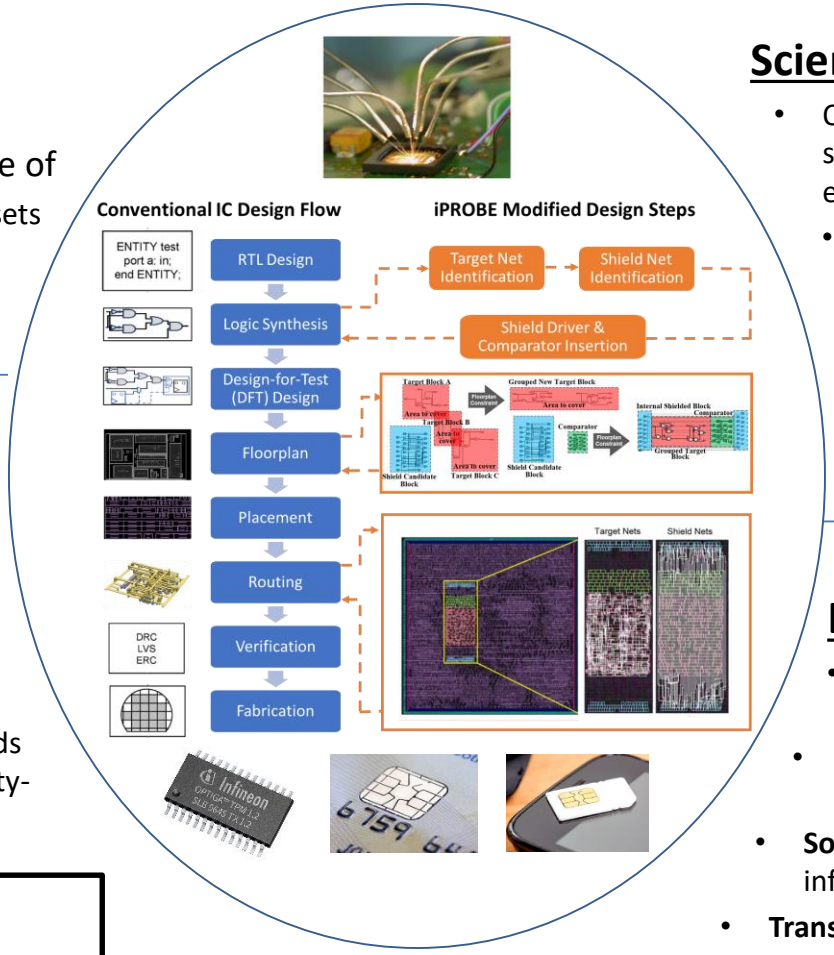
Focused Ion Beam (FIB) is a powerful circuit edit tool capable of

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

Solution:

iPROBE, the *1st* ever computer-aided design (CAD) approach against FIB-based probing

- Automatically identifies nets carrying sensitive information
- Optimally places and routes shields that surround and monitor security-sensitive nets



Scientific Impact:

- Quantification of chip layout's susceptibility to FIB-based attacks, & efficacy of shield-based protections
  - Low-overhead and quantifiable protection of secret keys, firmware, configuration features, etc. used for SW/HW security in cryptography, obfuscation, TPM, and many more applications

Broader Impact:

- **Gov't and Defense:** Protection of access control cards and IP
- **Commercial:** Protection of ATM cards, SIM cards, and DRM
- **Society:** Protection of personal information in smart and IoT devices.
- **Transition:** 2 patents pending
- **Education and Outreach:** Support of female PhD student and post doc

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