Spear and Shield: Evolution of Integrated Circuit Camouflaging

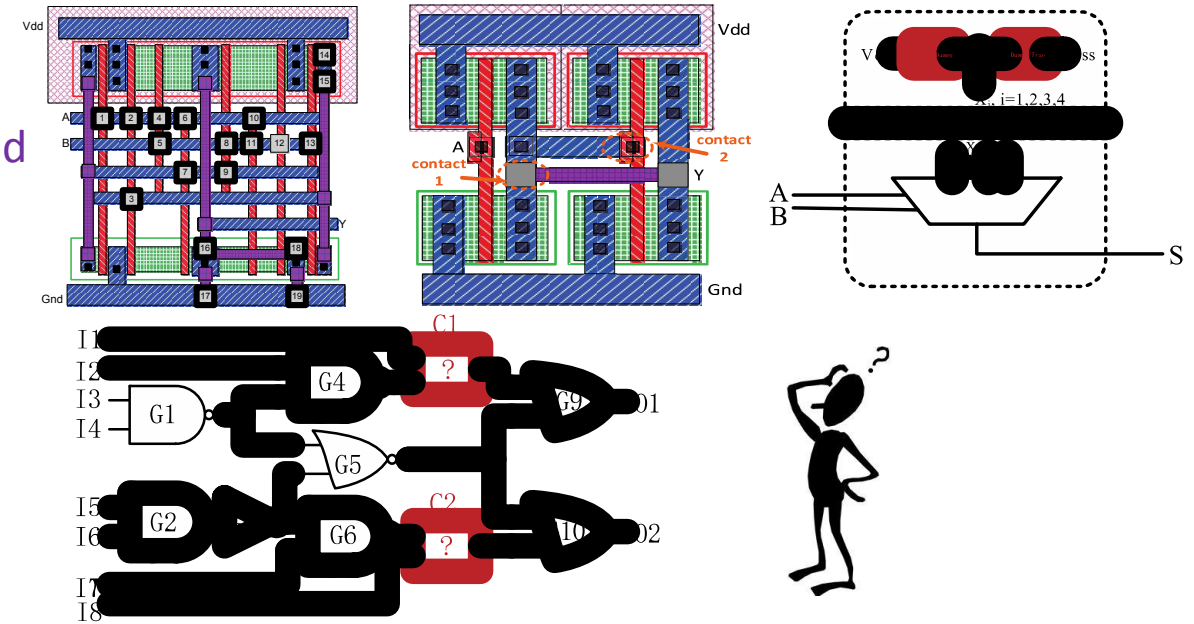
Xueyan Wang, Qiang Zhou, Yici Cai, Gang Qu

Wang XY, Zhou Q, Cai YC et al. Spear and shield: Evolution of integrated circuit camouflaging. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 33(1): 42–57 Jan. 2018. DOI 10.1007/s11390-018-1807-6

Why Gate Camouflaging?

- Design Complexity & Design Cost Increase.
- Intellectual Property (IP) Infringement Enabled by Reverse Engineering (RE) .
- Gate Camouflaging---Proactive Countermeasure against RE
  - Camouflaged cells can be configured to have one of the multiple functionalities with identical look.
  - Selective gates are replaced by camouflaged cells.

Various camouflaged cells



Existing De-Camouflaging Attacks

- Brute Force Attack (BFA)
  - Enumerate to try each possible functionality combination and compare with the functional IC.
- IC Testing-Based Attack (ITA)
  - Get the input-output behaviors of each camouflaged gate by justifications and sensitizations.
- SAT-Based Attack (SATA)
  - Prune incorrect functionality combinations with a discriminating set of input patterns by SAT solvers.
- Circuit Partition Attack (CPA)
  - Apply the divide and conquer methodology to partition camouflaged gates into multiple sub-circuits and de-camouflage each sub-circuit separately.

Defenses Against De-Cam. Attacks

- Clique-Based camouflaging
  - Ensure that each camouflaged gate's either inputs cannot be justified, or output cannot be sensitized.
- CamoPerturb
  - Perturb one minterm of the original design, and "re-correct" it with additional camouflaged module.
- And-Tree Camouflaging
  - Camouflage the inputs of And-tree structure, to prevent controlling the inputs of camouflaged gates.
- Equivalent Class-Based Camouflaging
  - Select gates for camouflaging from one certain equivalent class to avoid being partitioned into different sub-circuits to attack separately.

Challenges and Opportunities

- How to reduce the overhead incurred by circuit camouflaging would continue to be an urgent need.
- Design countermeasures against the newly proposed SAT-based de-camouflaging attacks.
- Explore intrinsic reconfigurable properties of emerging devices and how they can be utilized for circuit camouflaging.