Toward Optical Probing Resistant Circuits: A Comparison of Logic Styles and Circuit Design Techniques

Sajjad Parvin, Thilo Krachenfels, Shahin Tajik, Jean-Pierre Seifert, Frank Sill Torres, and Rolf Drechsler

Sajjad Parvin,
Doctoral Researcher
AGRA Group, University of Bremen

University of Bremen
Fraunhofer SIT
DLR
berlin
WPI
Deutsche Forschungsgemeinschaft DFG

Agenda

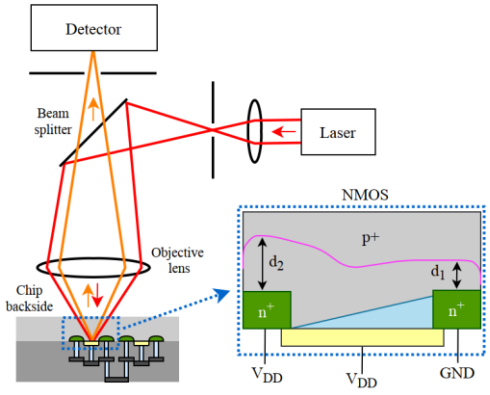
- What is the problem?
- What has been proposed to solve the problem so far?
- How are we trying to address the problem?
- Conclusion

What is the problem? I

- Meet the market demand
  - ↑ SOC complex ↓ yield → FA tools developed
- An adversary equipped with FA?
- Hijacking information using laser
- On what basis?

What is the problem? II

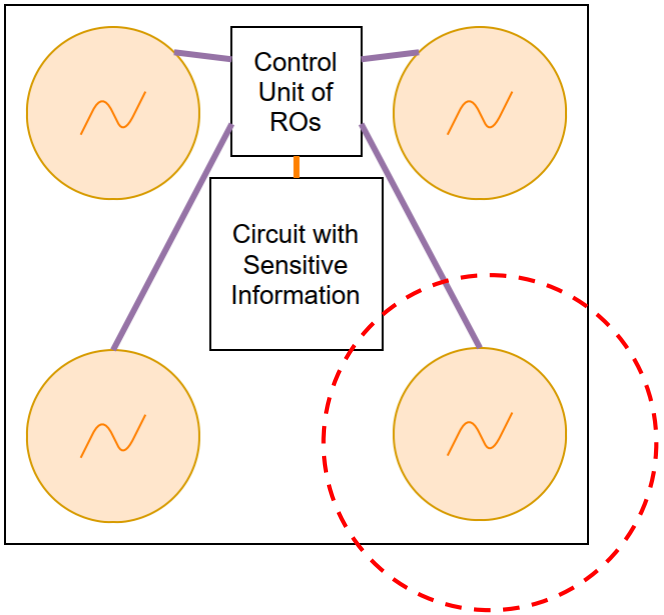
- Silicon → Transparent to NIR
- Go through backside
- As the light passes through the backside
  - Modulation of light
- Mainly doping concentration, but



Minor	Mobility Bulk Voltage
Major	Size Doping Voltage Structure

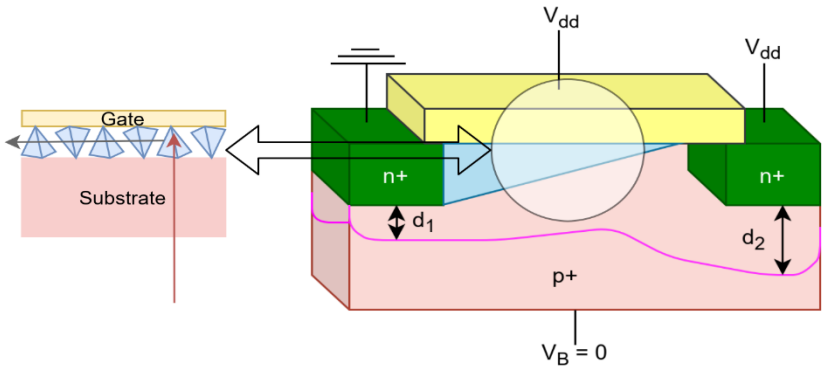
How to prevent optical probing (Literature) I

- Categorized into 3 types:
  - Sensor-based
  - Change fabrication process of the transistors
  - Circuit level
- Sensor-based*
  - Active monitoring
  - Large area
  - Can be shut down



Tajik, S., Lohrke, H., Seifert, J. P., & Boit, C. (2017). On the power of optical contactless Probing: Attacking bitstream encryption of FPGAs. Proceedings of the ACM Conference on Computer and Communications Security.

How to prevent optical probing (Literature) II

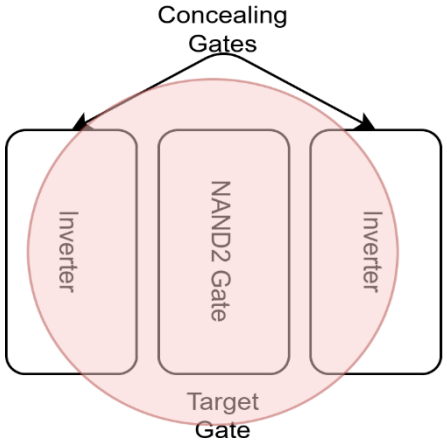


- Fabrication based:
  - Opaque layer
    - requires built-in sensors
  - Scramble the light
    - New materials in FET*
- Circuit level countermeasures
  - Concealing gates
  - Clever circuit designs

Shen, H., Asadizanjani, N., Tehranipoor, M., & Forte, D. (2018). Nanopyramid: An Optical Scrambler Against Backside Probing Attacks. ISTFA 2018: Conference Proceedings from the 44th International Symposium for Testing and Failure Analysis, 81009, 280–289.

Circuit level countermeasures I

- Concealing gates*
  - Gate obfuscate data
  - Concentration never goes to zero
    - How?
      - Counterpart transistor must switch
- Problem?
  - Multi-input gates
- Solution:
  - Change gate's circuit design
  - Propose gates with concealing property



Rahman, M. T., Florida, U., Asadizanjani, N., & Florida, U. (2020). CONCEALING-Gate : Optical Contactless Probing Resilient Design. 1(1), 1–25.

Circuit level countermeasures II

- Let's start on our contribution
  - Formulate the Reflection
  - Proposed several design techniques
  - Experiment on circuits
    - Simulation

Circuit level countermeasures III

- Magnitude of reflection is:

$$RCV = V \times K \times \beta \times P_L \int_0^{2\pi} \int_0^{r_{spot}} p(r) \times A(r,\theta)\, dr d\theta$$

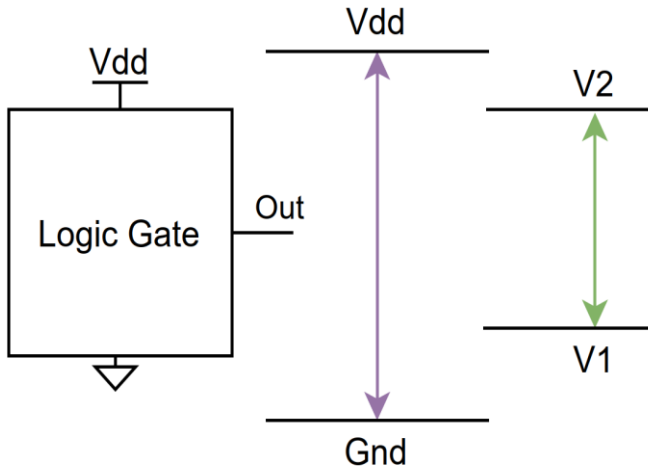
- Magnitude of reflection of a FET:

$$RCV_{FET} = RCV_D + RCV_S + RCV_G + e^{-N} \times RCV_{Bulk}$$

- Magnitude of reflection of a Logic Gate:

$$RCV_{Log.Gate} = \sum_{\forall t \in Log.Gate} \sum_{i \in \{D,S,G,Bulk\}} RCV_{ti}$$

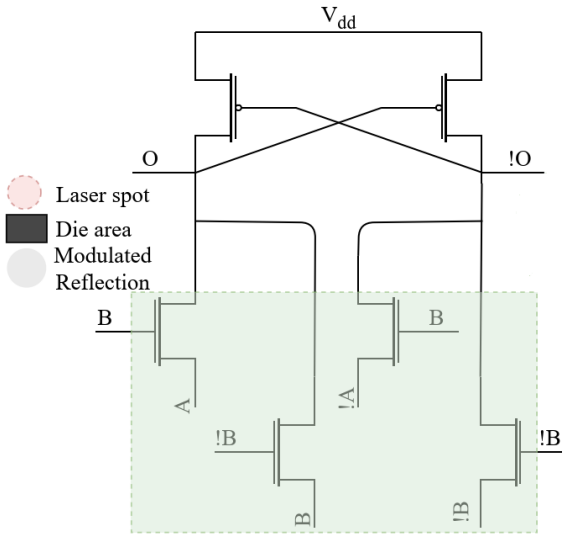
Circuit level countermeasures IV

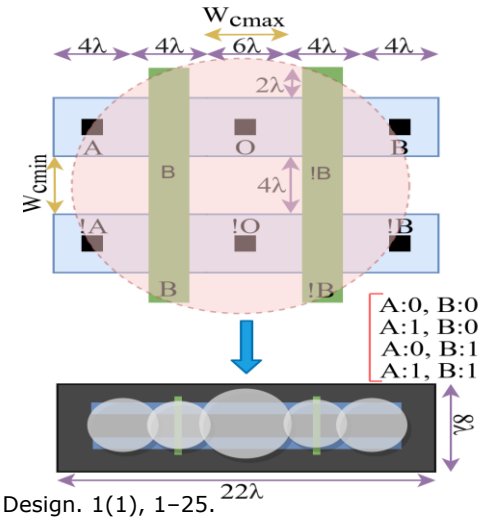


- Smaller Area → better
  - Merging diffusion areas
  - 50-75% reduction in area
- Reducing supply power
  - Subthreshold/Near Threshold design
  - Requires on-chip regulator
- Limited output swing
  - No need for voltage regulator
  - Sacrifices the noise margin

Circuit level countermeasures V

- Inherently obfuscating gates
  - Dual Rail Logic (DRL)
  - How?
- DRL → Both signals
- How well it obfuscate?
  - CARD

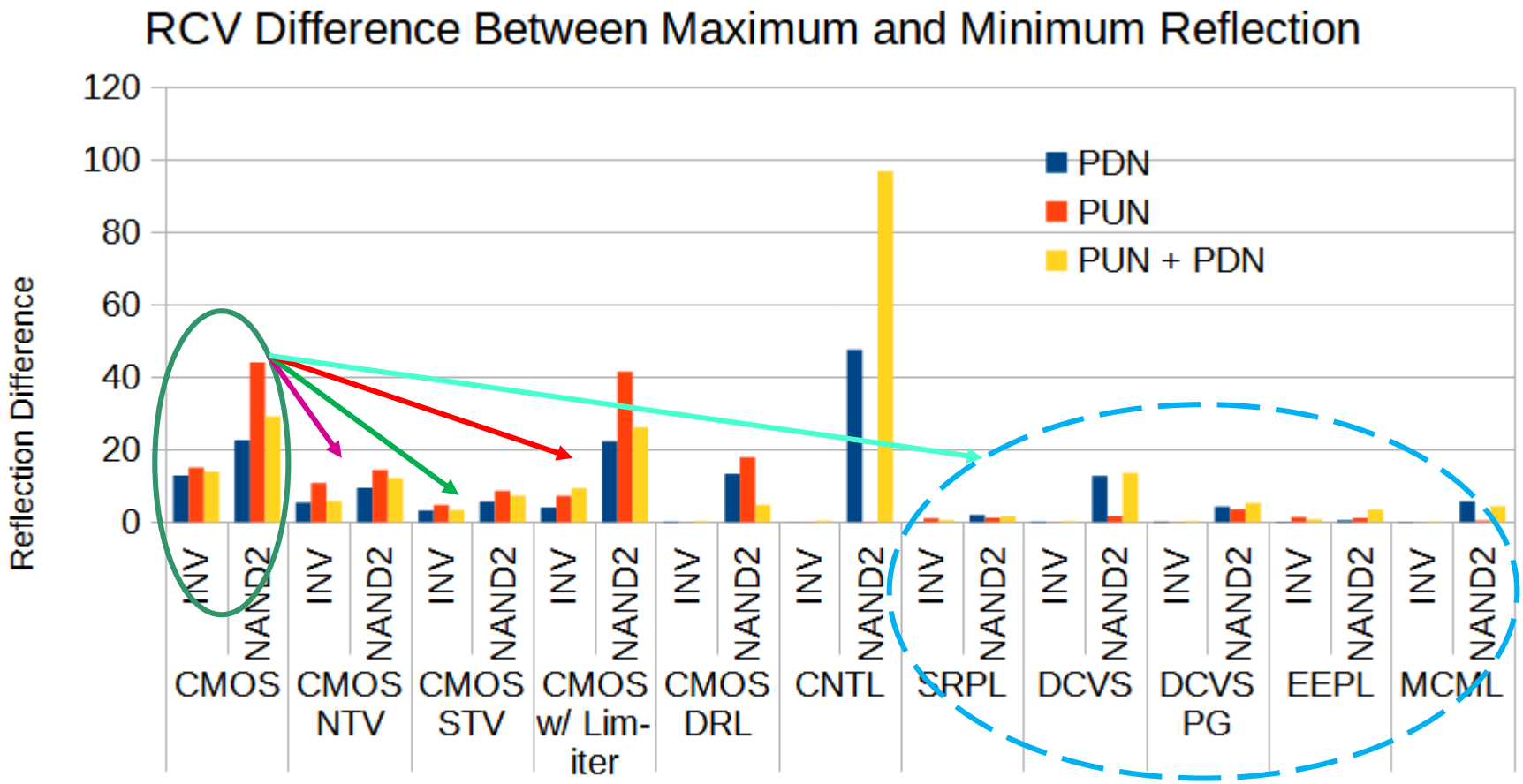




Technology Node (nm)	C_{min} [∗]	C_{min} ours	C_{max} [∗]	C_{max} ours
90	0.780	0.208	1.561	0.312
45	0.390	0.104	0.780	0.156
32	0.277	0.074	0.555	0.111
22	0.191	0.051	0.382	0.076

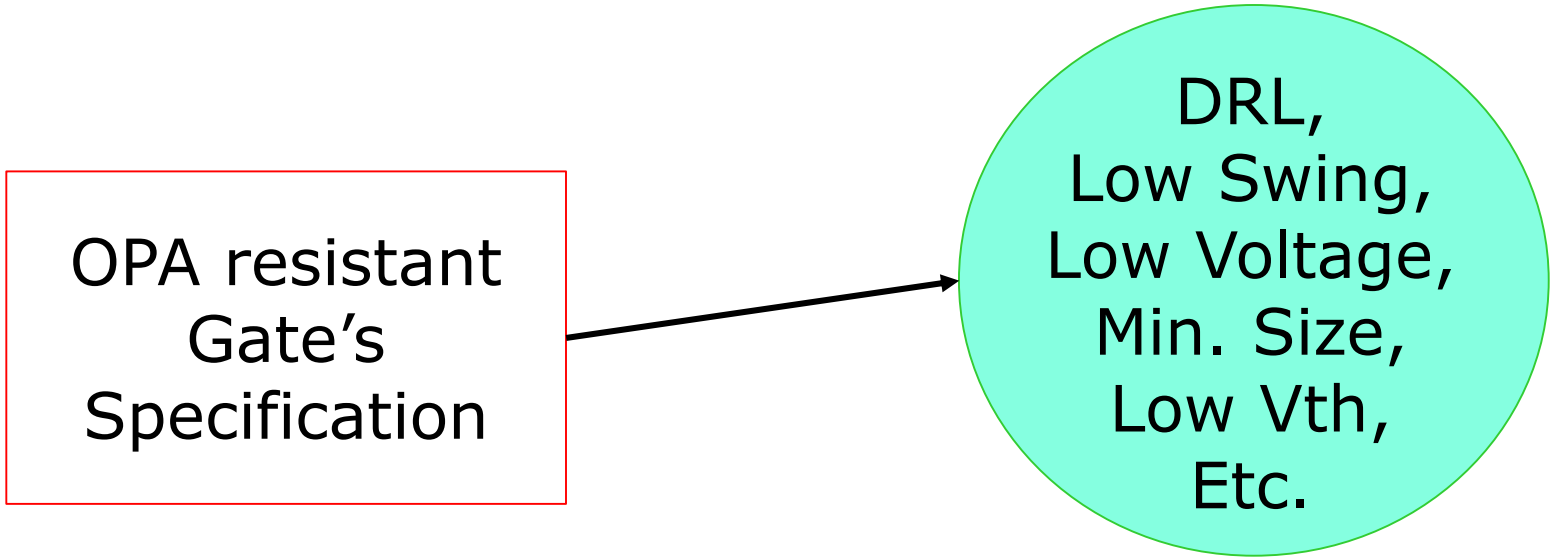
*Rahman, M. T., Florida, U., Asadizanjani, N., & Florida, U. (2020). CONCEALING-Gate : Optical Contactless Probing Resilient Design. 1(1), 1–25.

Circuit level countermeasures IV : Results



Conclusion

- Physics of optical probing
- Logic gates and circuit techniques
- Combination of all techniques



Thank you for you attention! ☺

- Questions?