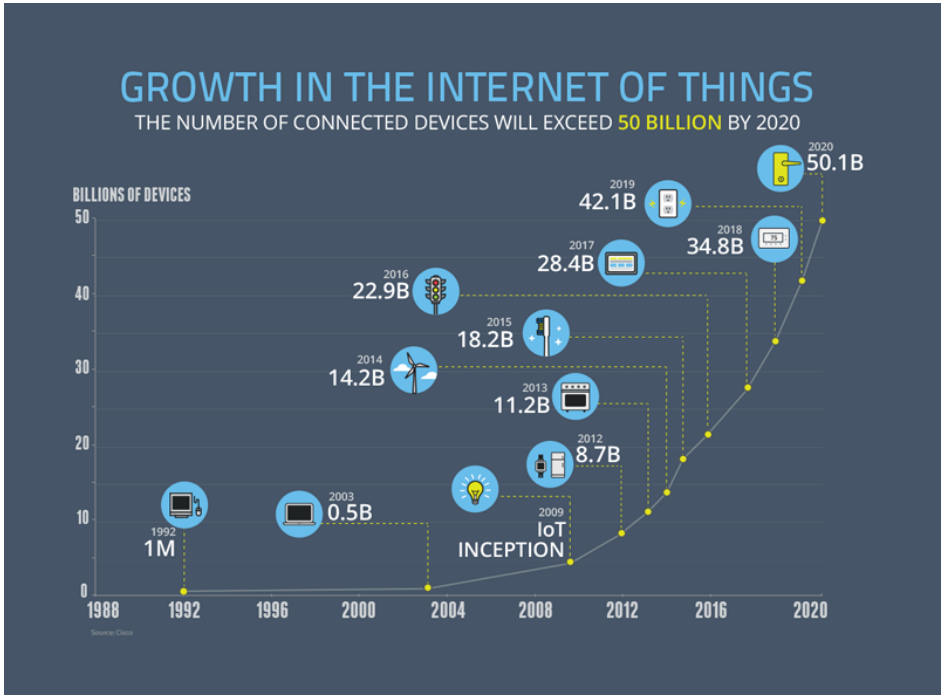
Backside Imaging for Hardware Trojan Detection

Boyou Zhou
Advisor: Ajay Joshi

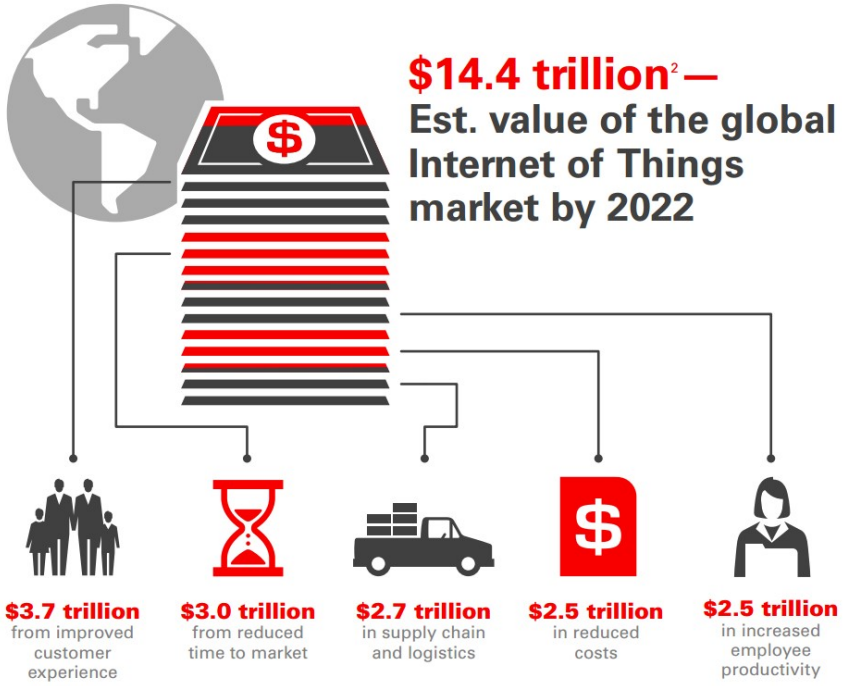
Department of Electrical and Computer Engineering

BOSTON UNIVERSITY

The Era of Internet of Things (IoT)

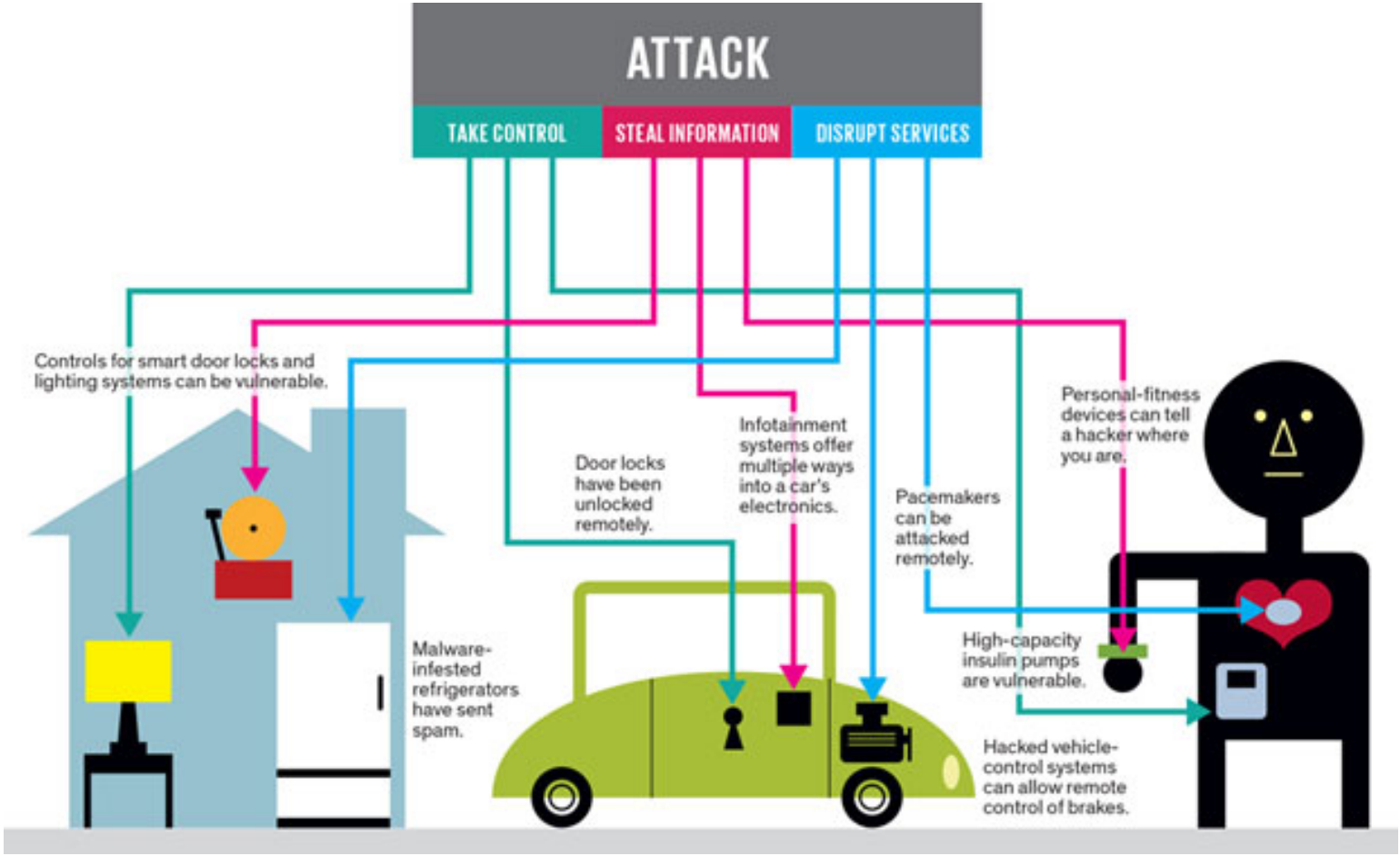


[InfosecPartner, 2015]



[Forbes, 2015]

But the IoTs are under attack!



[IEEEspectrum, 2016]

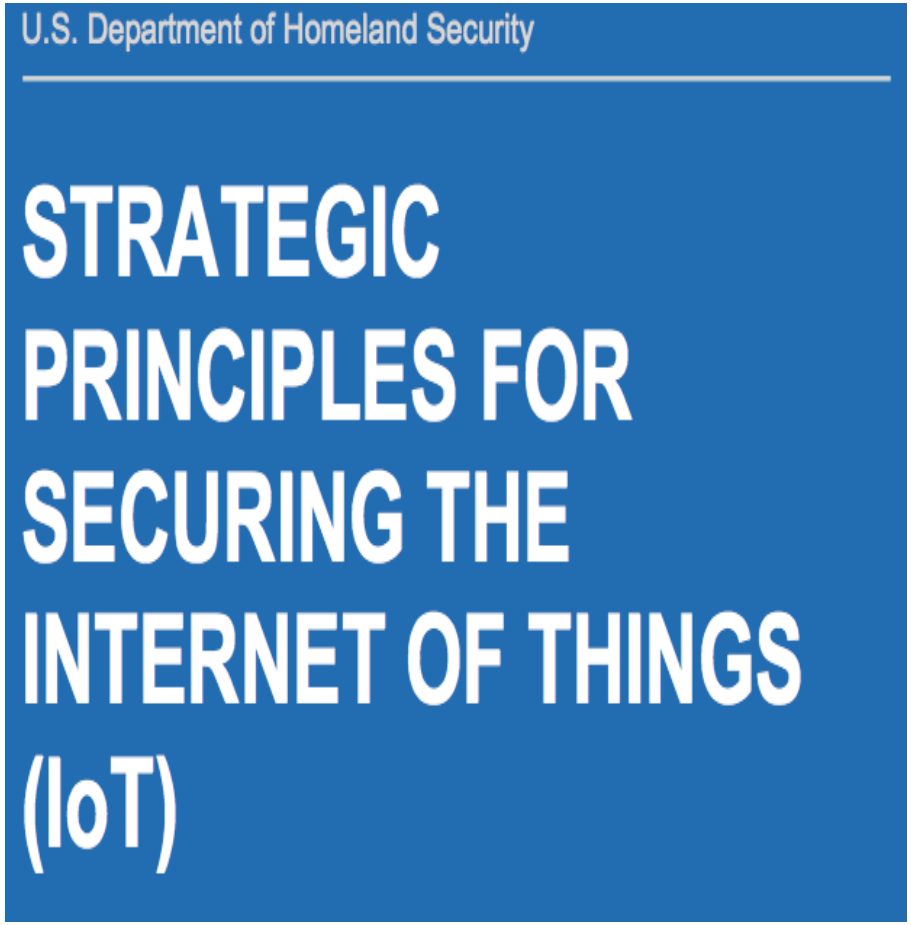
Millions Lines of Code

[Delphi, 2016]

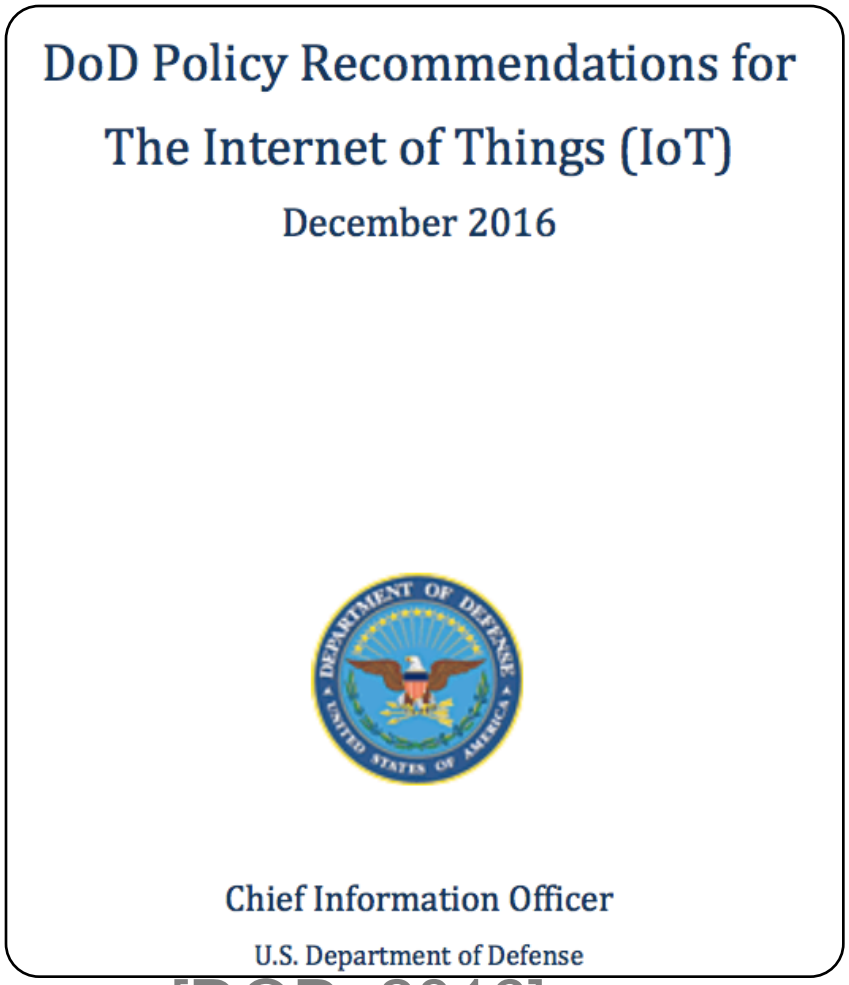
Cyber Attacks Around the World

Attacked map
http://map.norsecorp.com/ [Norse, 2014]

Security of IoT is critical



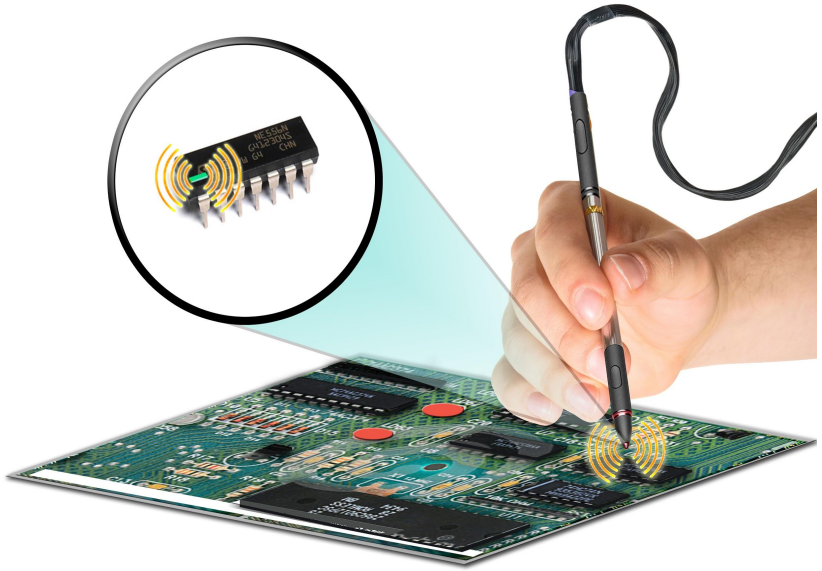
[DHS, 2016]



[DOD, 2016]

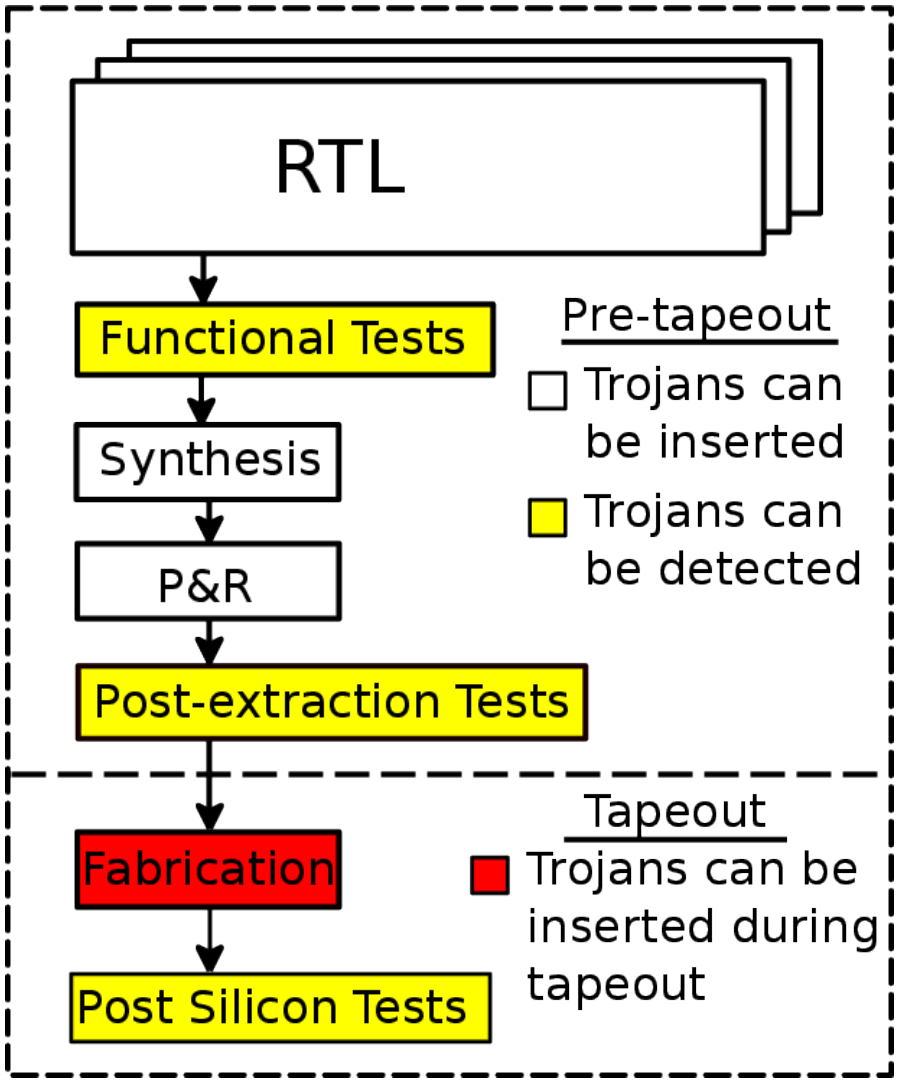
Attacks on ICs of IoTs

- ICs are becoming vulnerable to malicious modifications due to globalization of IC production
- Variety of attacks are possible including
  - Hardware Trojans (HTs)
  - IP privacy and IC overbuilding
  - Reverse engineering
  - Side-channel analysis
  - IC counterfeiting

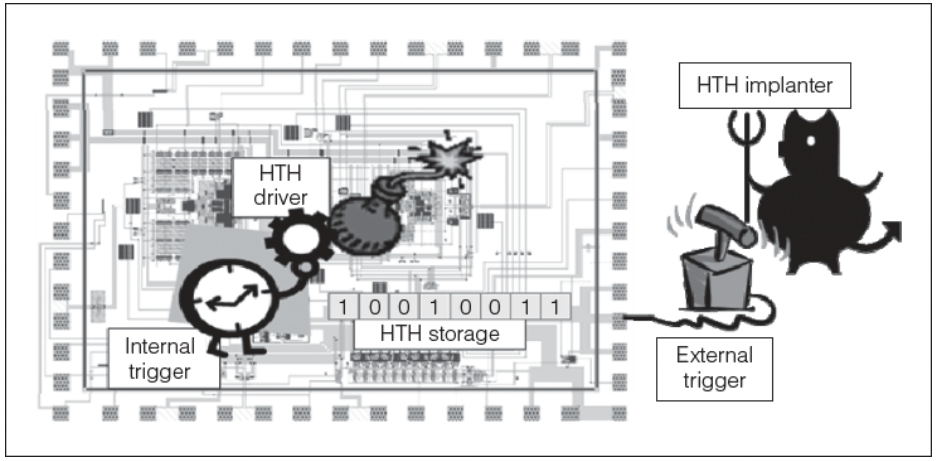


[DARPA, 2014]

Hardware Trojan Insertion



- Hardware Trojans are malicious HW blocks that are inserted in IC chips
- Hardware Trojans can be inserted during design as well as after tapeout

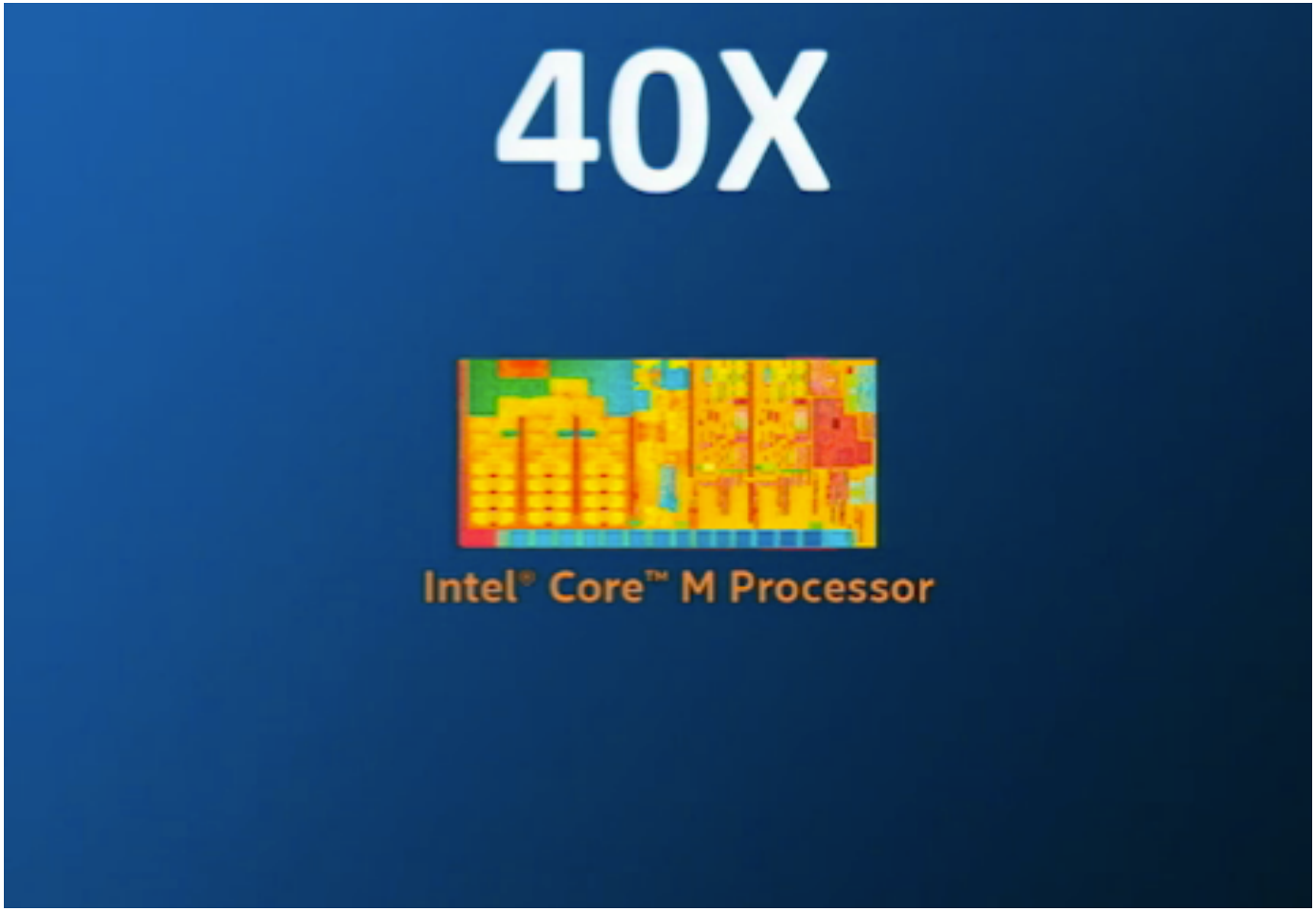


[Tehranipoor, 2013]

Size of Laptop

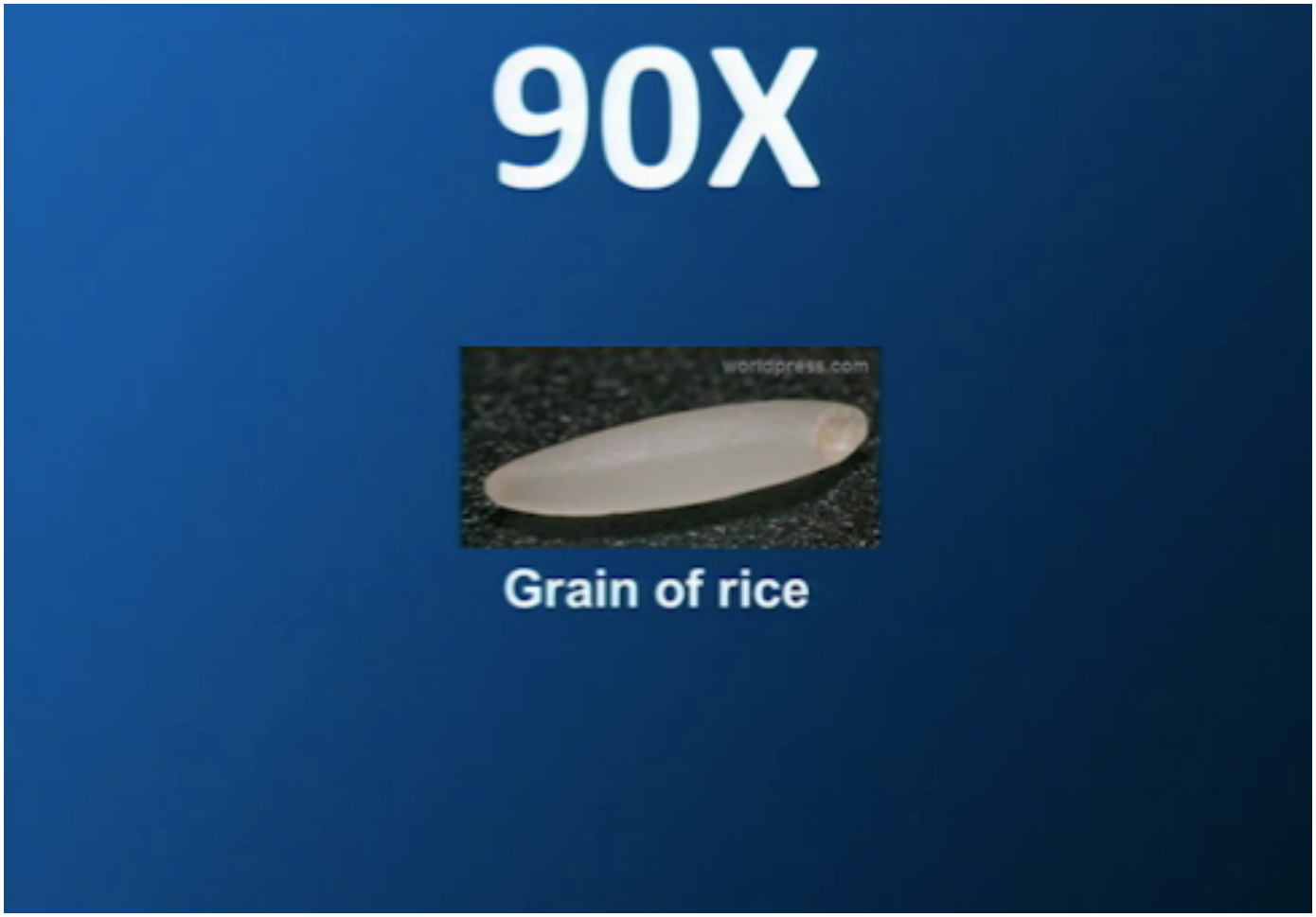
[Singh, 2014]

Size of Microprocessor



[Singh, 2014]

Size of Rice



[Singh, 2014]

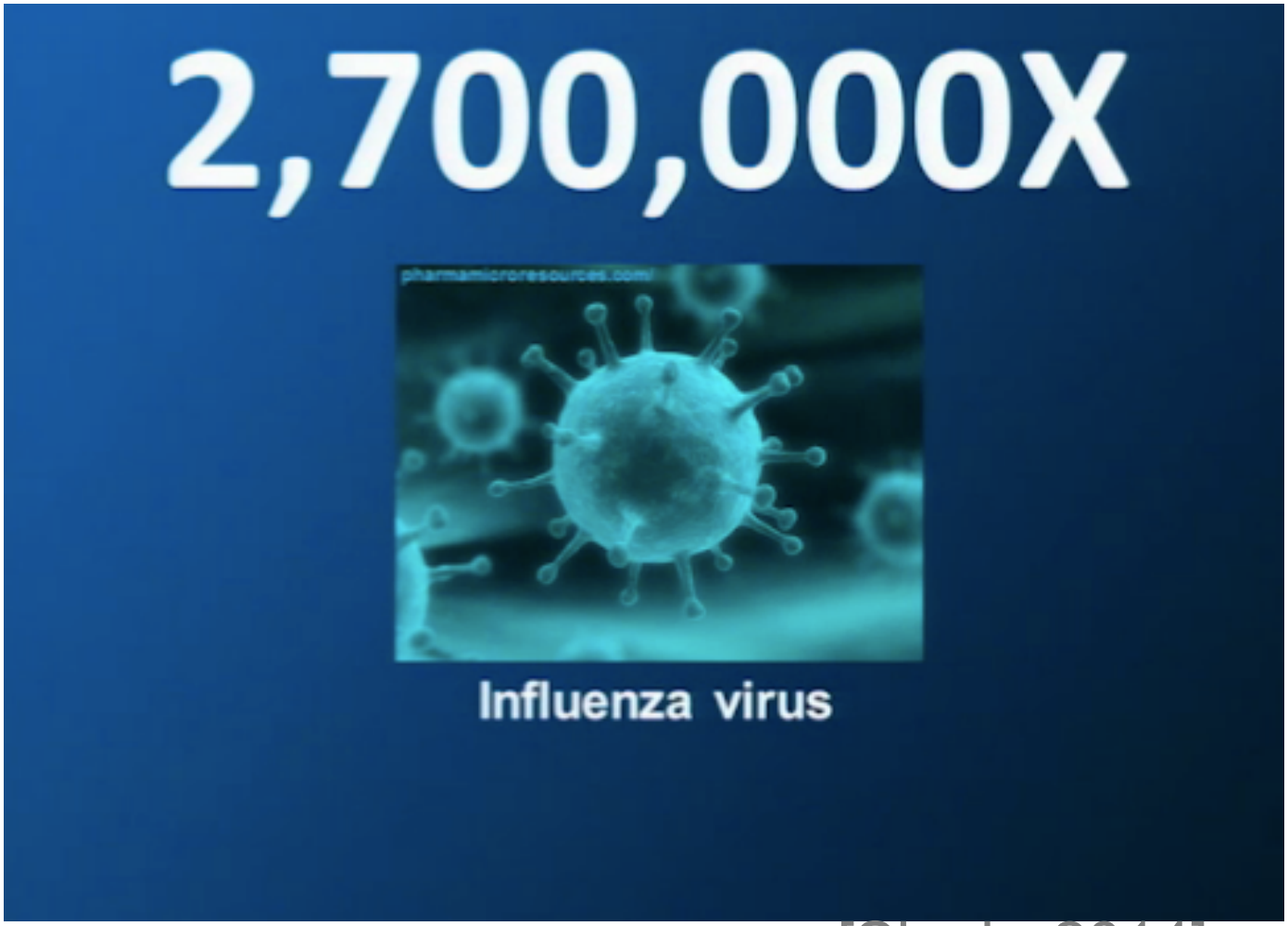
Size of Hair

[Singh, 2014]

Size of Blood Cell

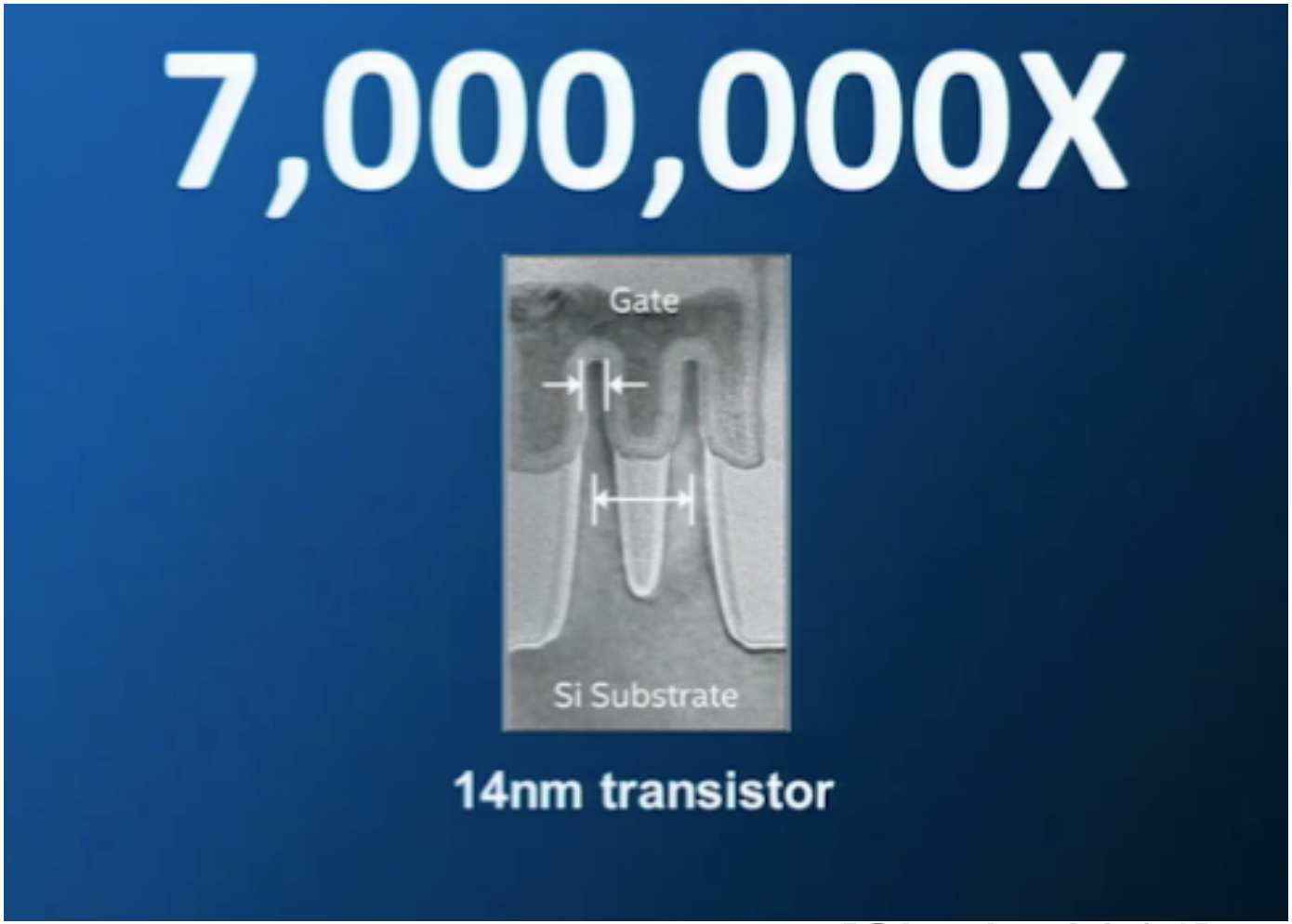
[Singh, 2014]

Size of Virus



[Singh, 2014]

Size of Transistor

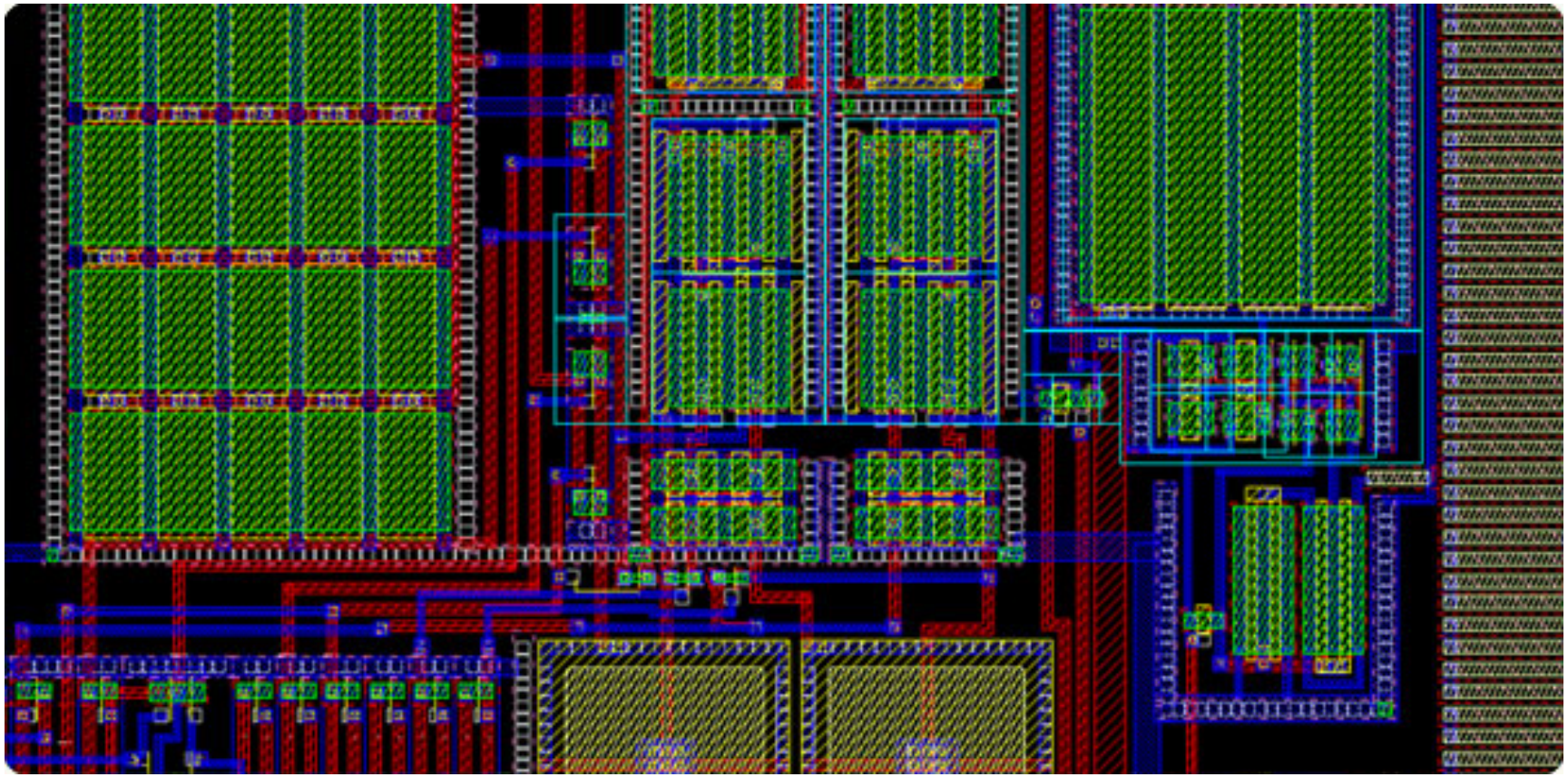


[Singh, 2014]

Scan Electron Microscope

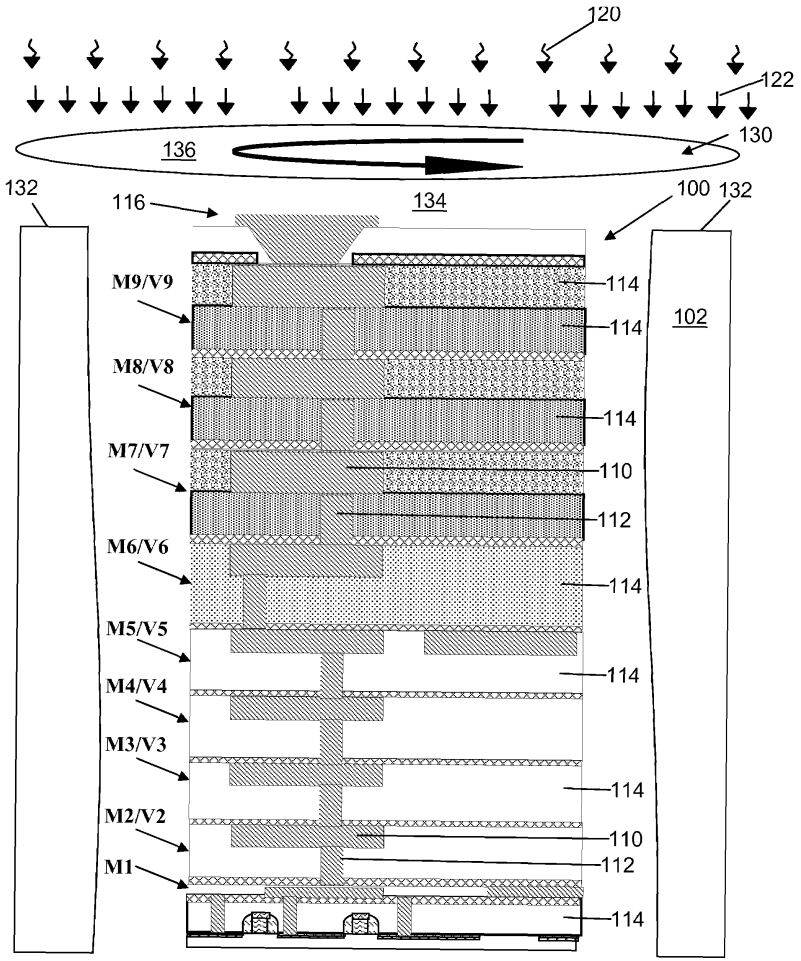
[LTScientific, 2017]

IC Layout



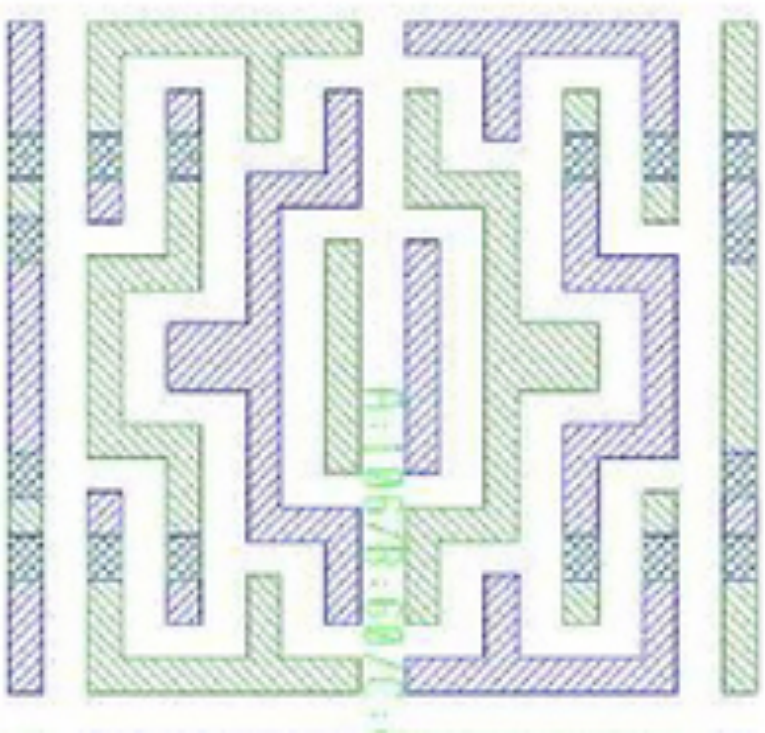
[Zeni EDA, 2009]

Delayering Metal Layers

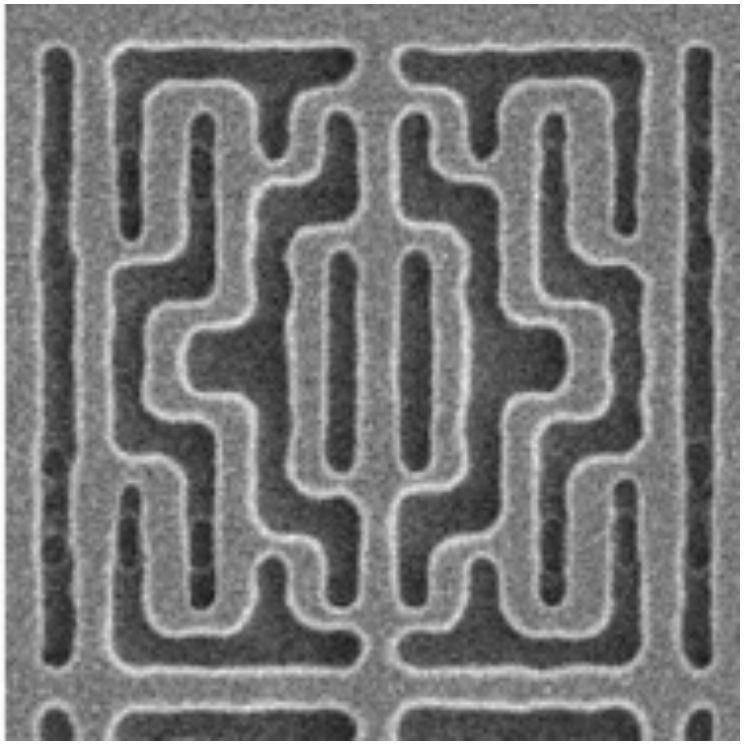


[US 7504337, 2009]

Process Variations



Design Layout



Fabricated Chip

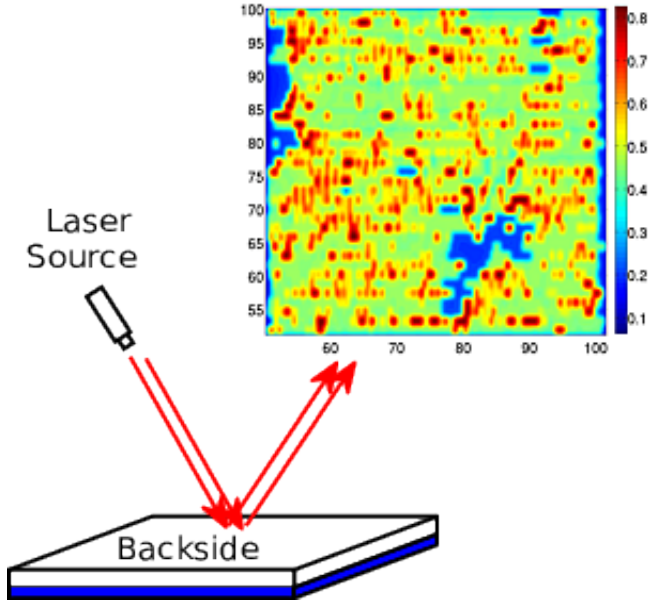
[SPIE, 2013]

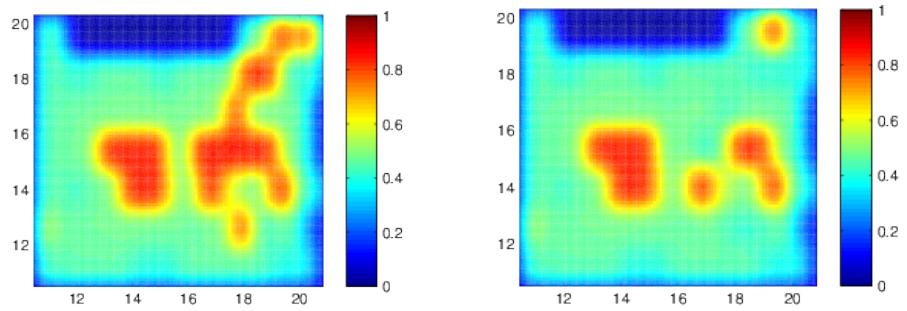
HT Detection Methods

- Both electrical methods and non-electrical methods can be used to detect Hardware Trojans
- Electrical Methods:
  - Delay-based Analysis Ref: Li 2008, Jin 2008
  - Power Analysis Ref: Wei 2013
- Non-electrical Methods:
  - Thermal Analysis Ref: Kangqiao 2013, Norwroz 2014, Forte 2013
  - Sound Analysis Ref: Tehranipoor 2010
  - Electromagnetic Analysis Ref: Song 2011, Stellari 2014

HT Detection using Engineered Fill Cells

- Engineer fill cells to have higher optical response
- Use correlation method to compare ”golden reference” and imaged results
- Evaluate proposed approach using a variety of IC blocks
- Demonstrate that our approach is robust against measurement noise and process variations



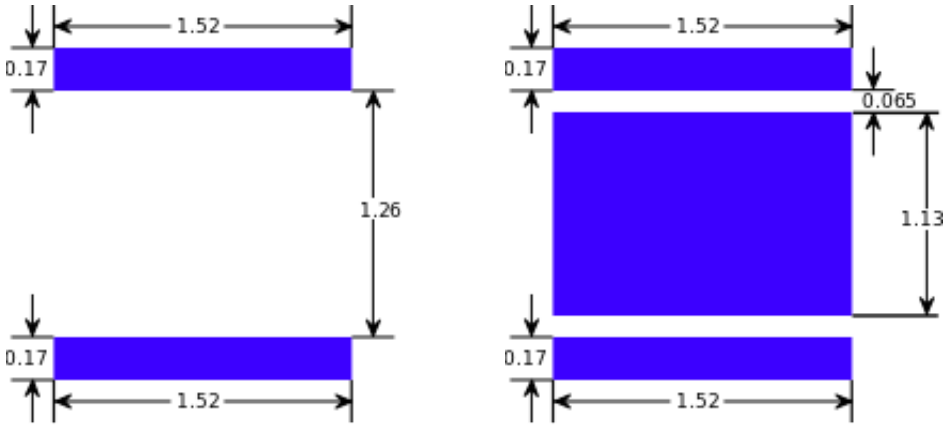


Observed Image without HTs

Observed Image with HTs

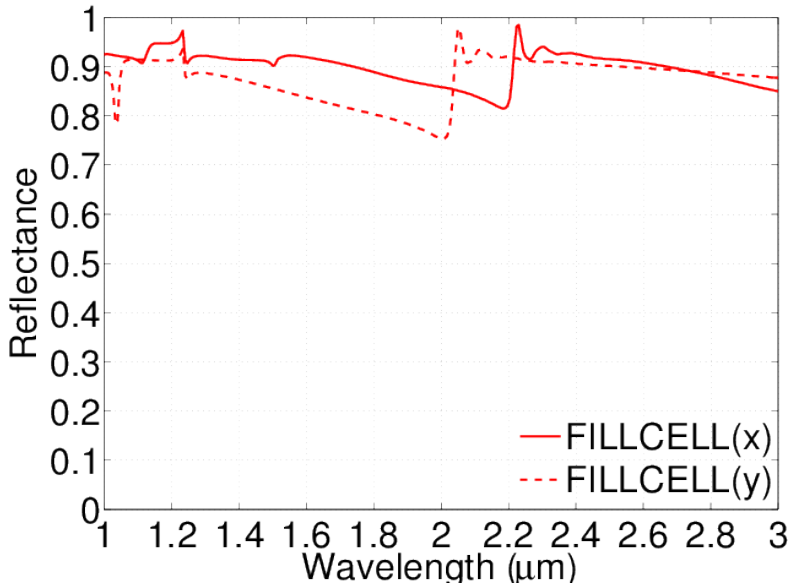
[Zhou, 2015]

Fill Cell Design



Fill Cell without Metal Filling

Fill Cell with Metal Filling

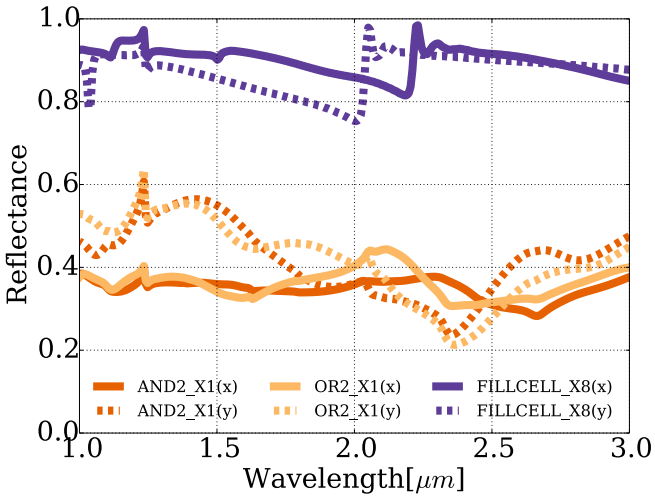


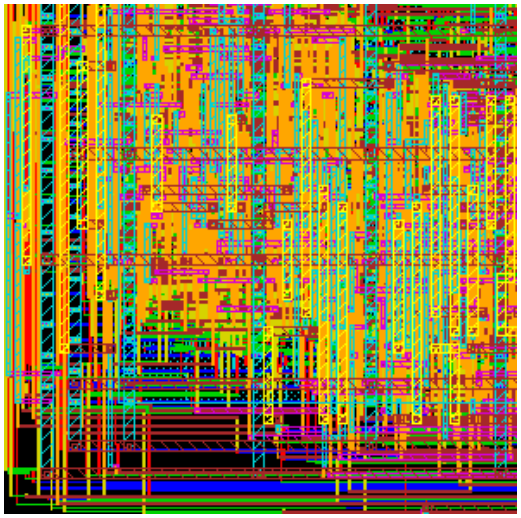
Fill Cell Response

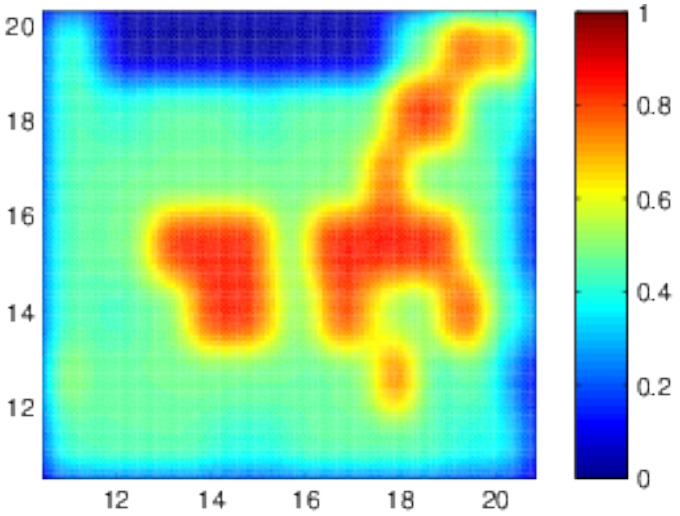
- We add metal filling in fill cell to achieve high optical response
- CAD tools control where the fill cells are placed

Optical Watermarks

Solid:x Dotted:y







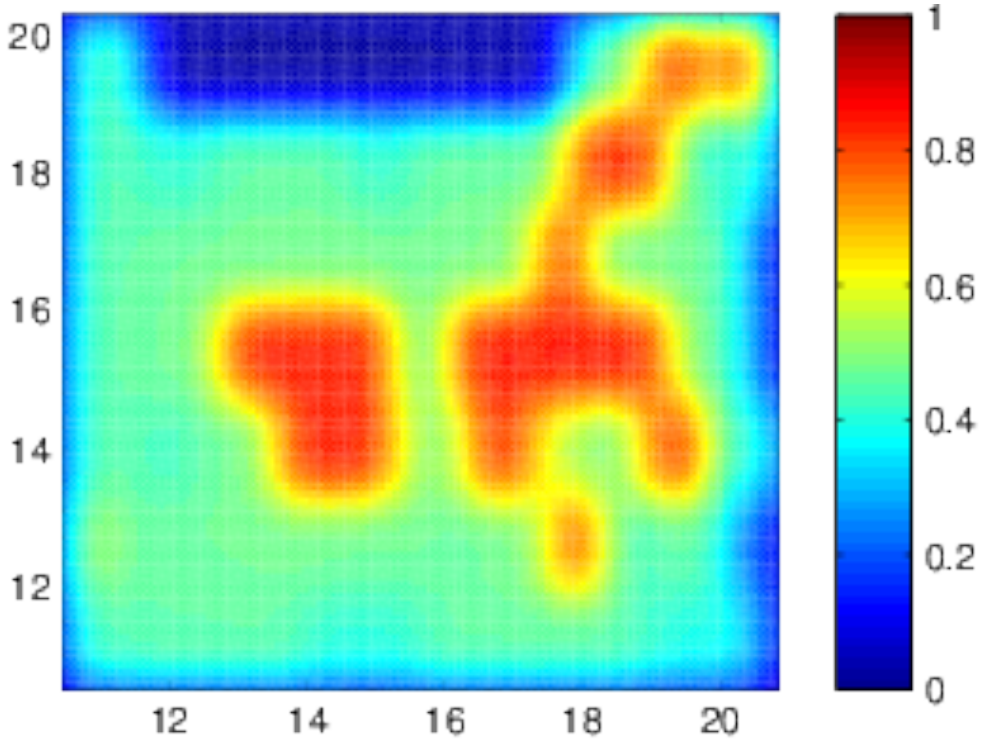
Optical Response

Layout from Cadence Encounter Tool

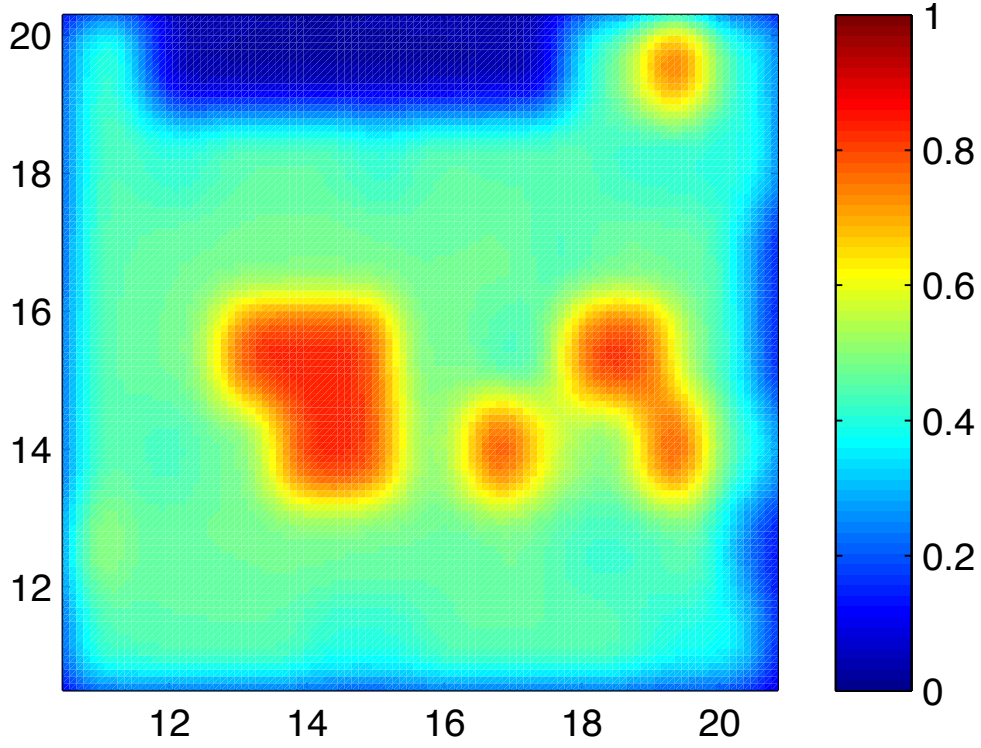
Optical Response

- Optical response of the engineered fill cells is higher than those of functional cells
- We use these engineered fill cells as watermarks

Hardware Trojan Detection - Case 1

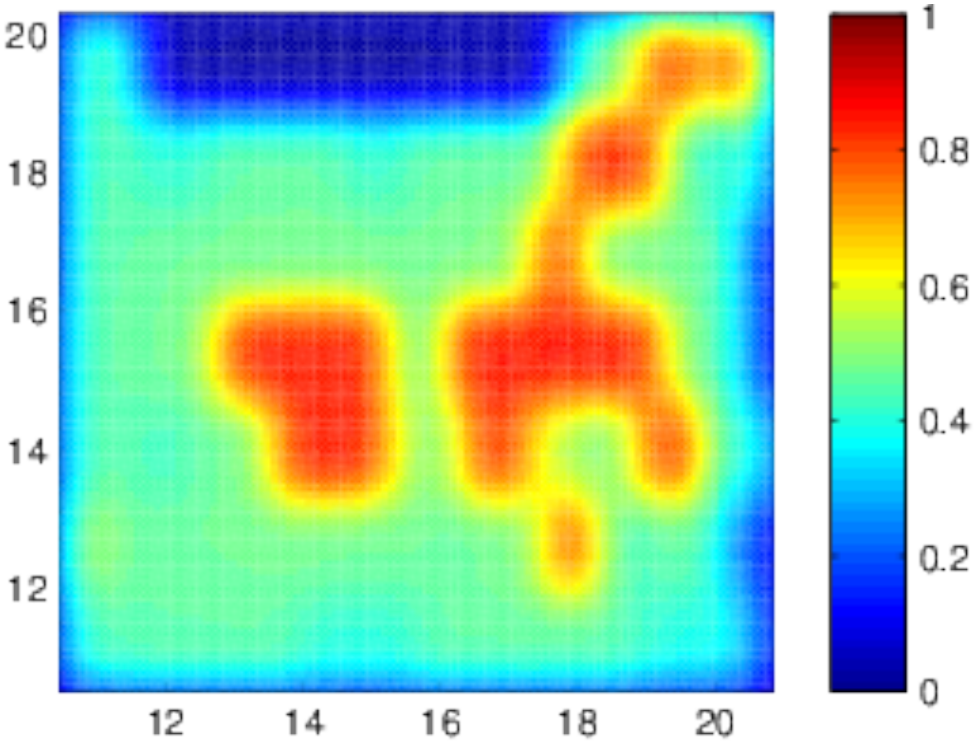


10 um by 10 um region of the original design

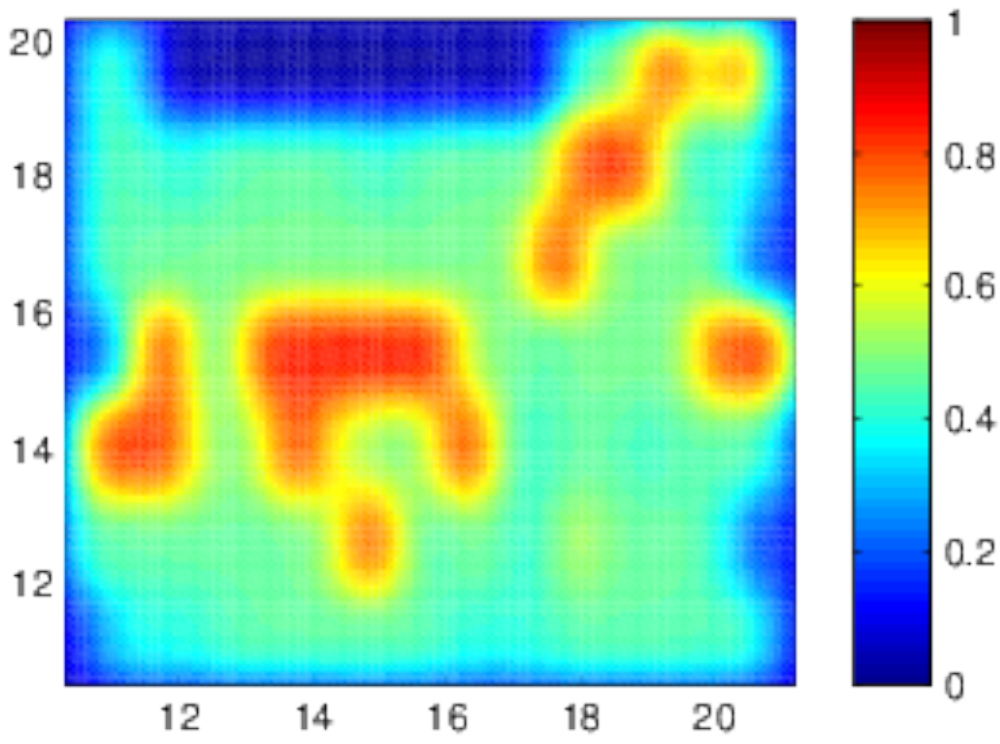


Fill cells are replaced with HT functional cells

Hardware Trojan Detection - Case 2

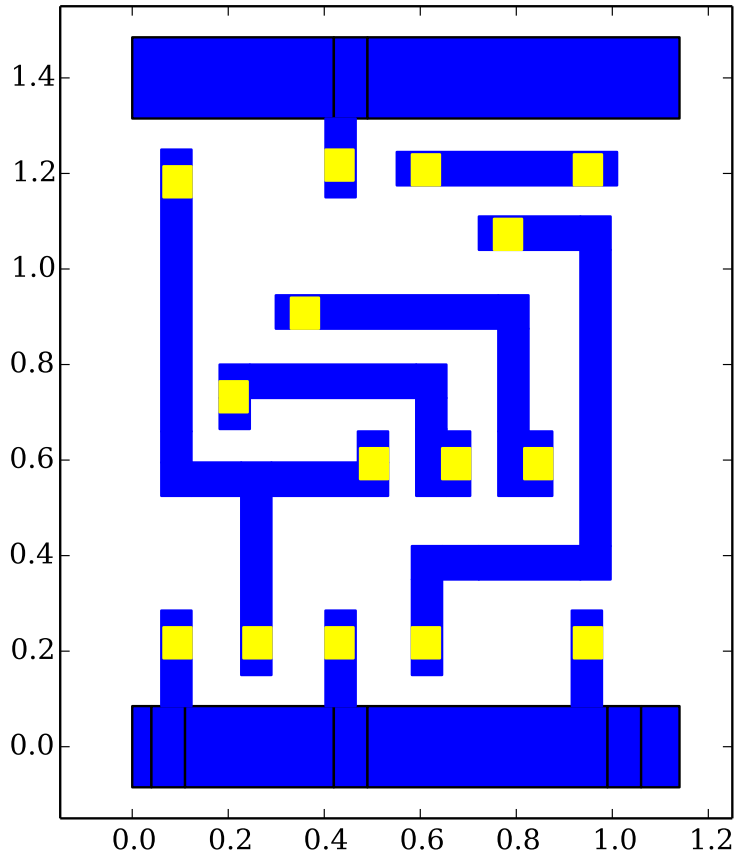


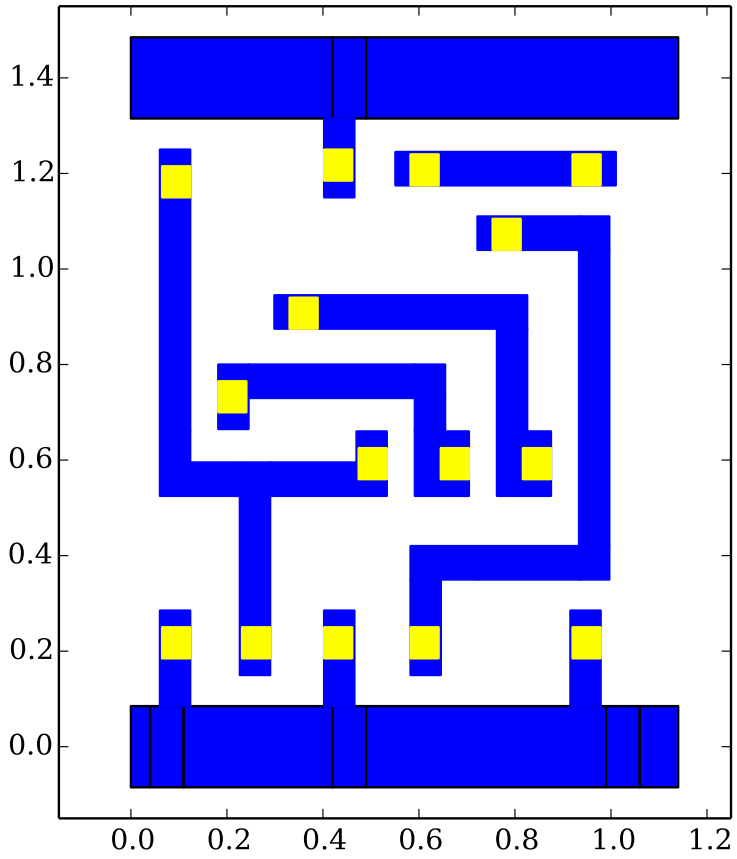
10 um by 10 um region of the original design



Cells in the bottom half are shifted by 5 um to the left to make room for HTs

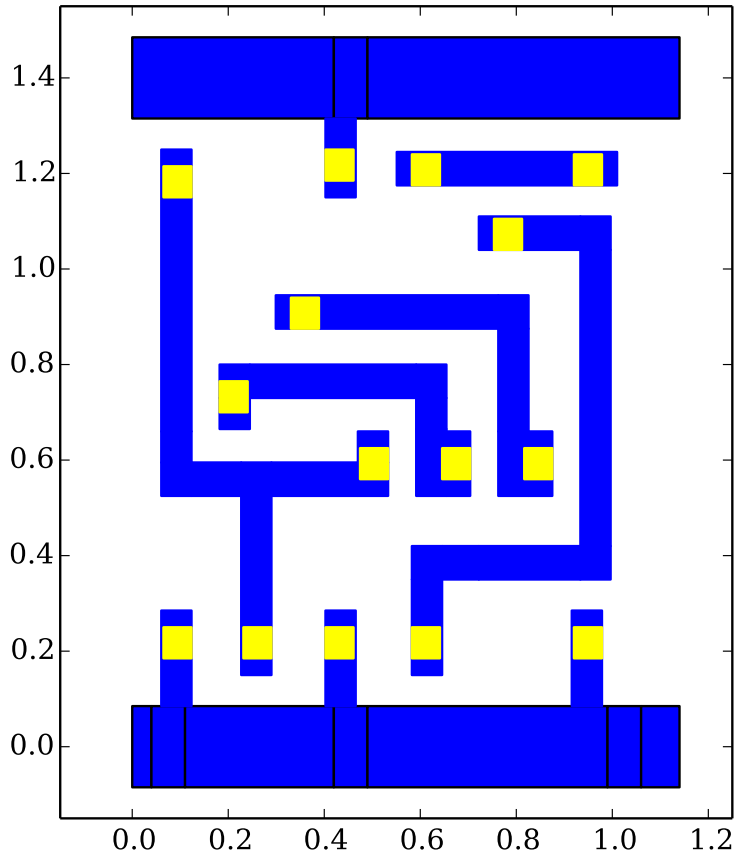
Effects of PVs



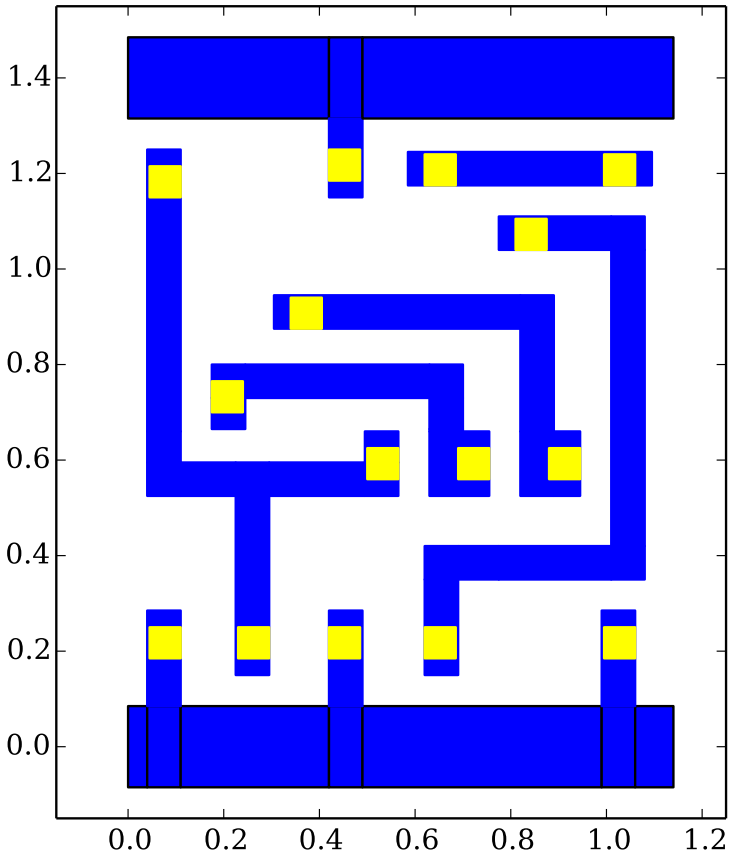


XOR2_X1 without PVs

Modeling in PVs

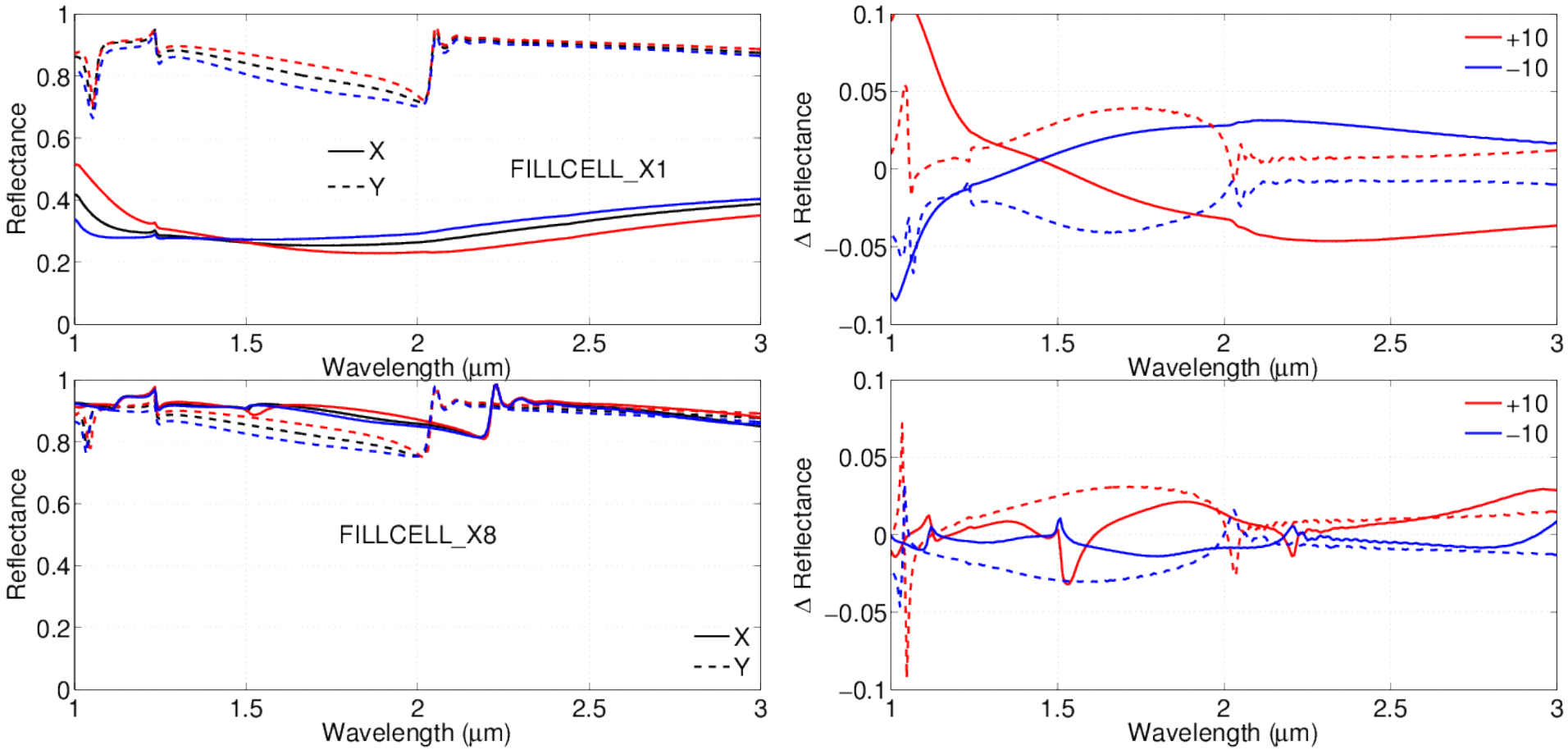


XOR2_X1 without PVs



XOR2_X1 with 10% increase in X direction

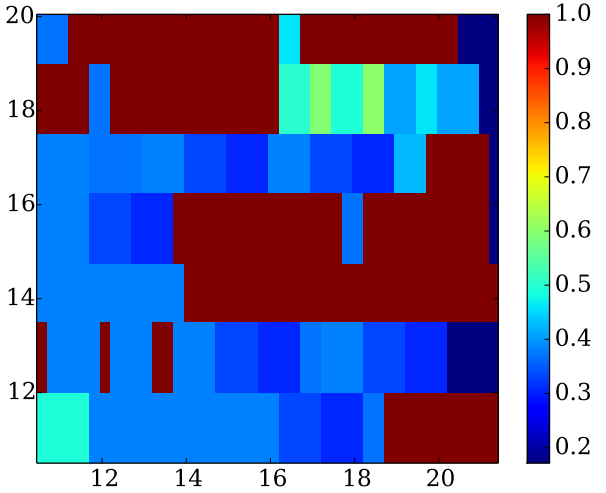
Effect of PVs on Optical Reflectance

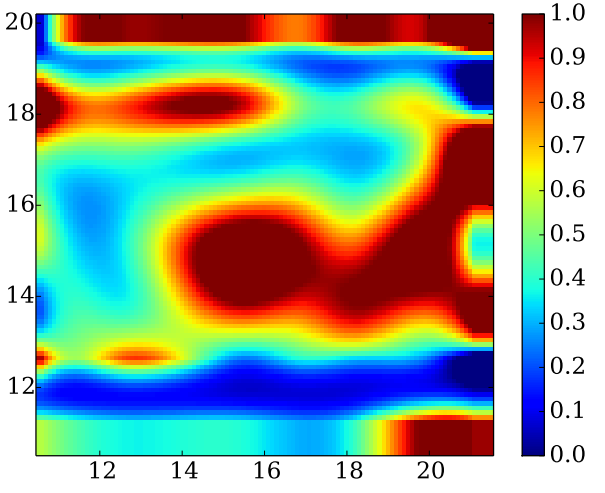


Reflectance in presence of ±10% process variations

Noise Based Detection

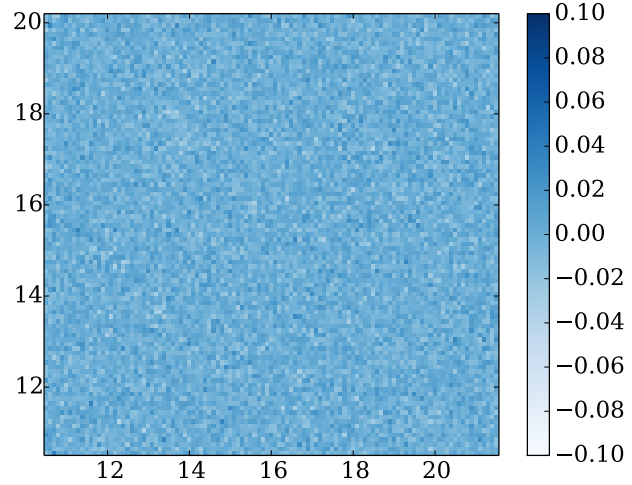
Mapped Response

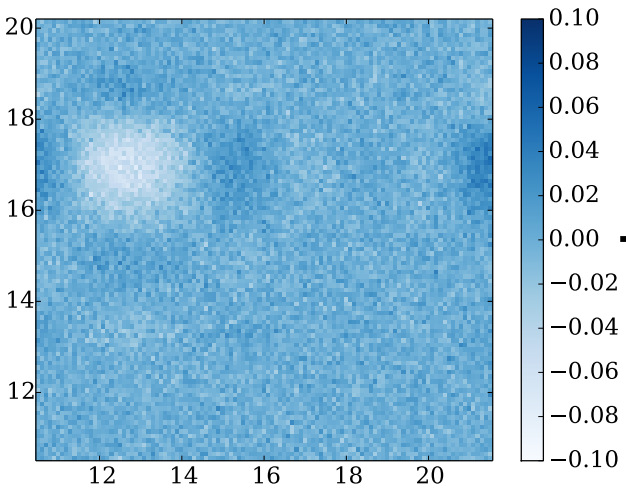




Interpolated Response

Gaussian Noise

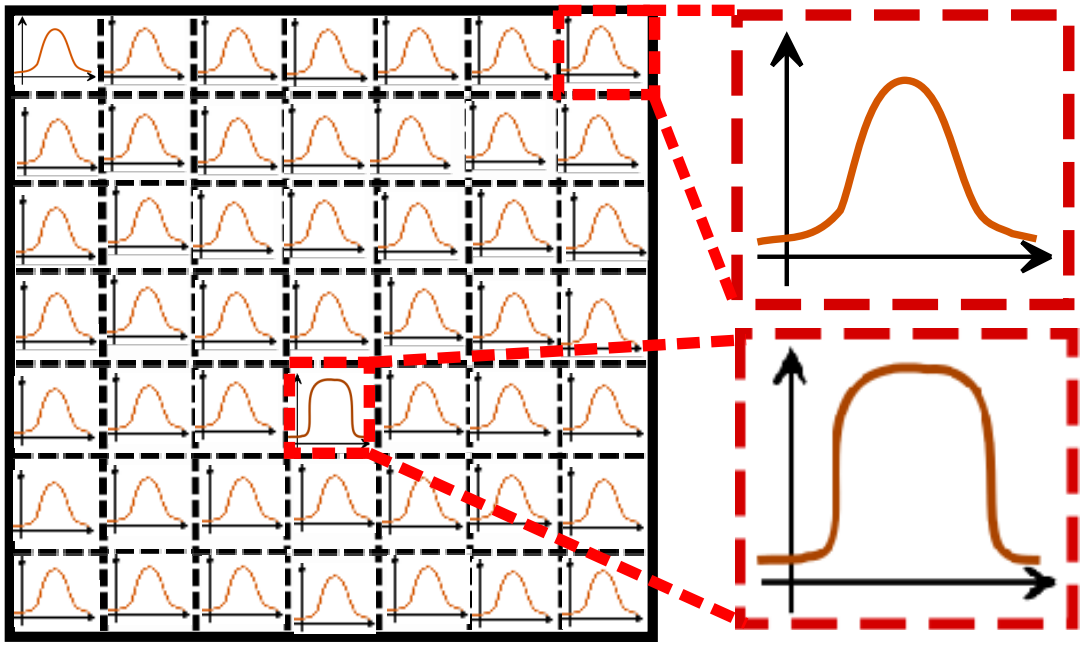




Noise From Tampered Chip

Batch Mode in Detection

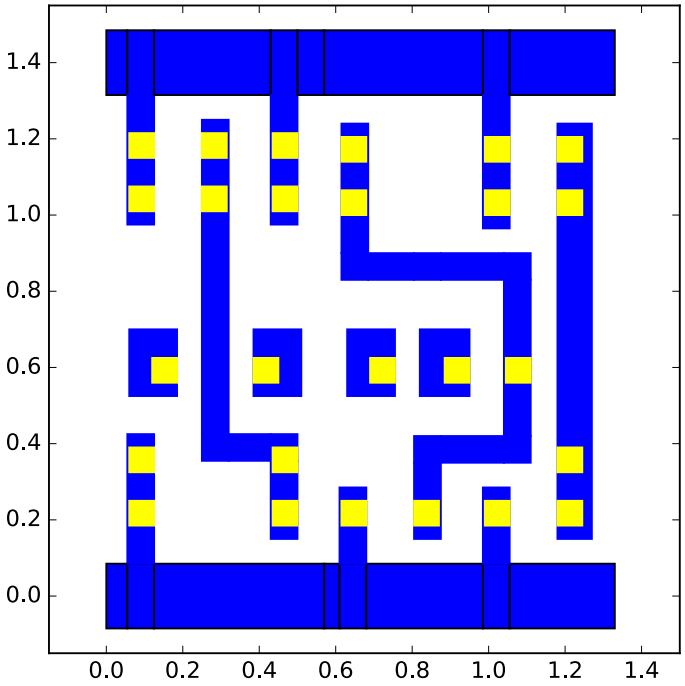
- We divide the entire chip into smaller areas (detection windows).
- If one of the window does not follow Gaussian Distribution (D'Agostino's K-square test), we consider the entire chip tampered.



Divide the whole image into smaller detection windows

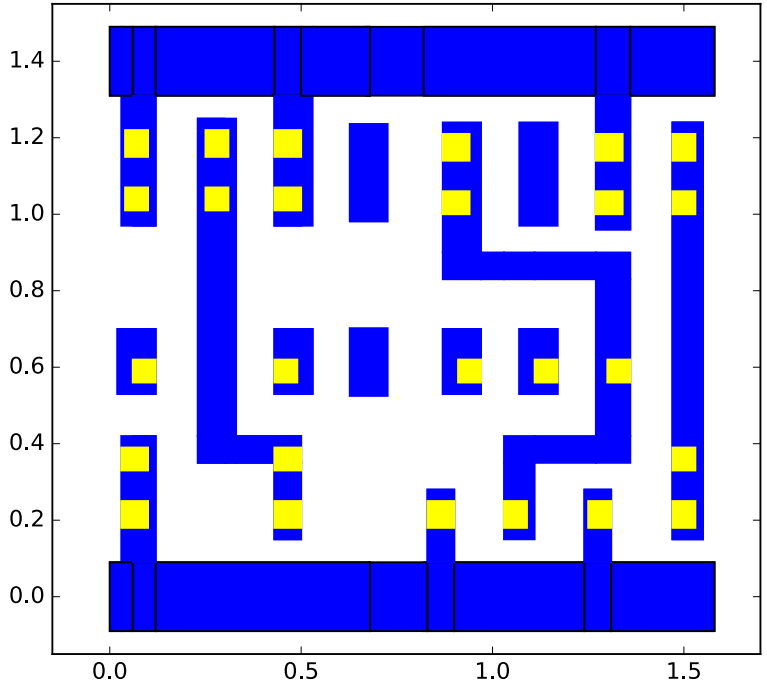
Gate Level Analysis

NAND-OR



Original Gate Design

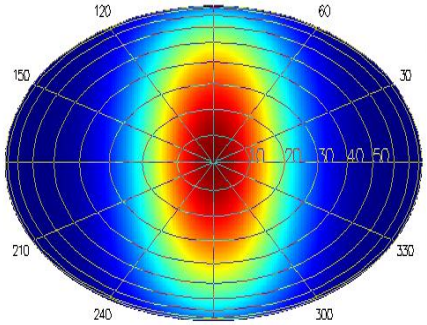
NAND-OR with Antenna

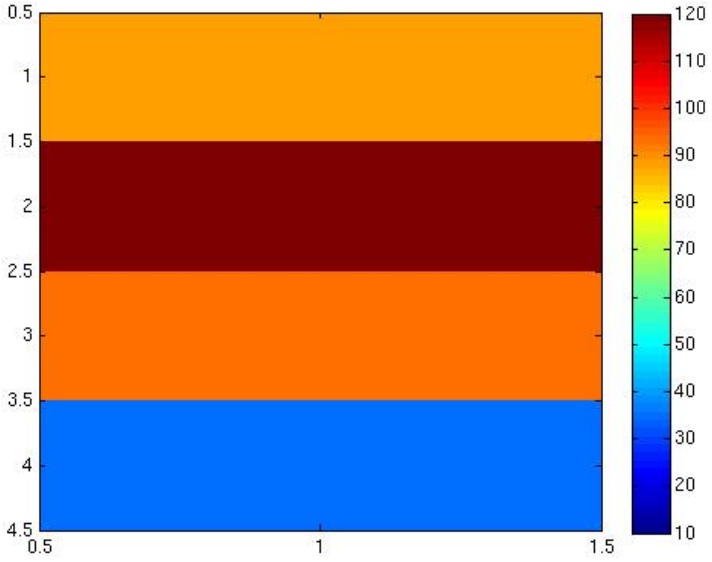


Gate Design with Plasmonic Bar Antenna

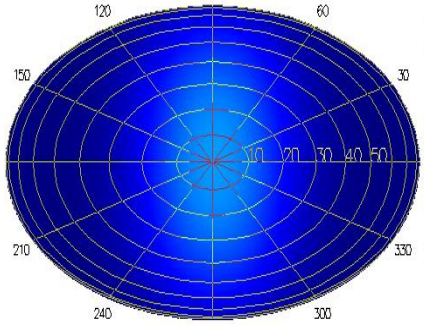
Reflectance From Nano-Antennas

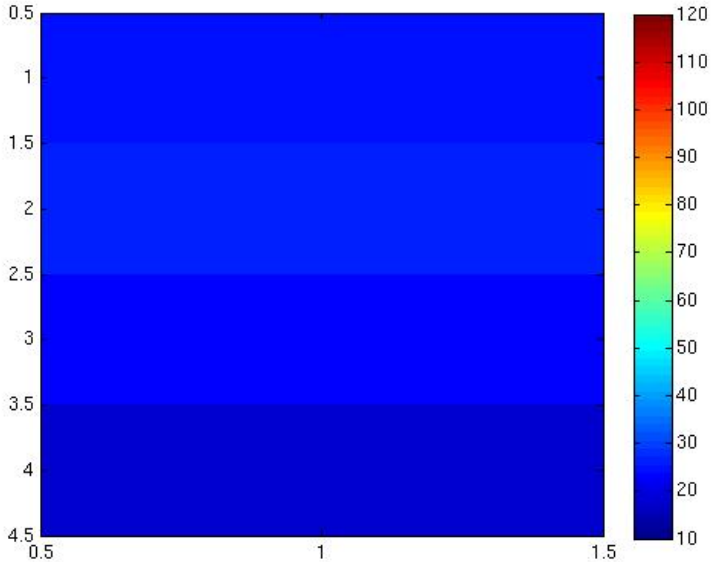
Y-Polarization





X-Polarization





[Negin, 2017]

Thank you!