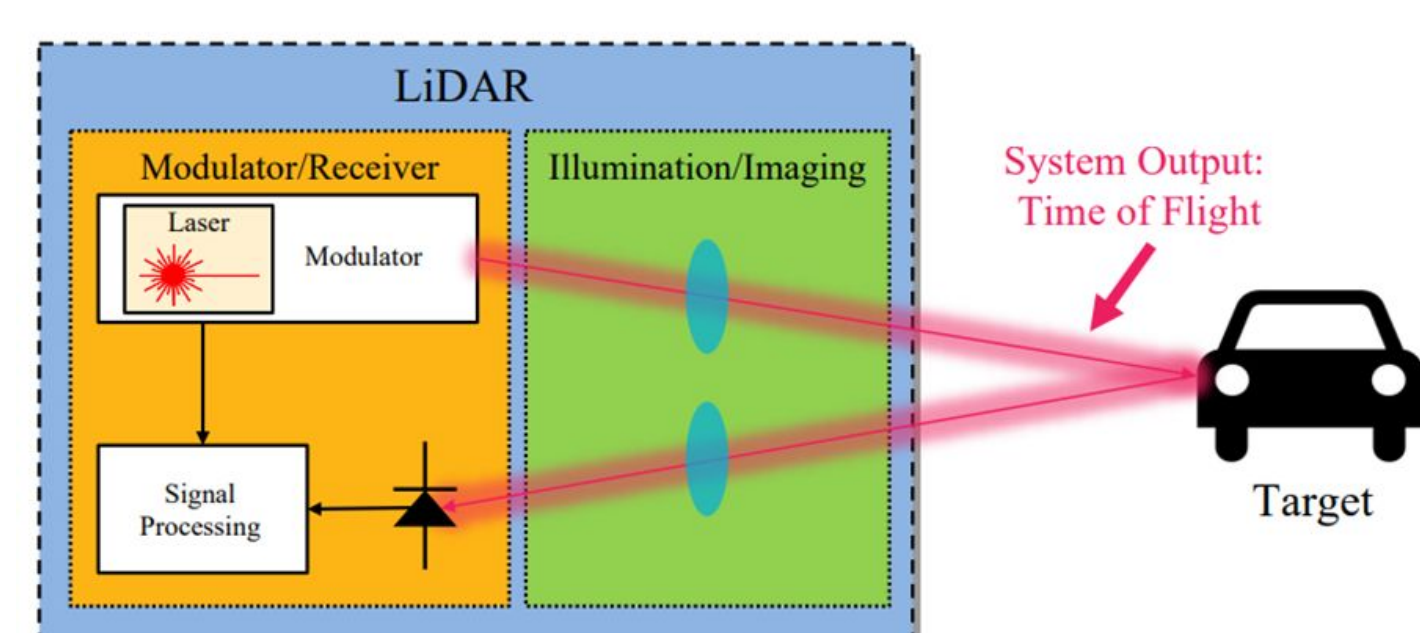


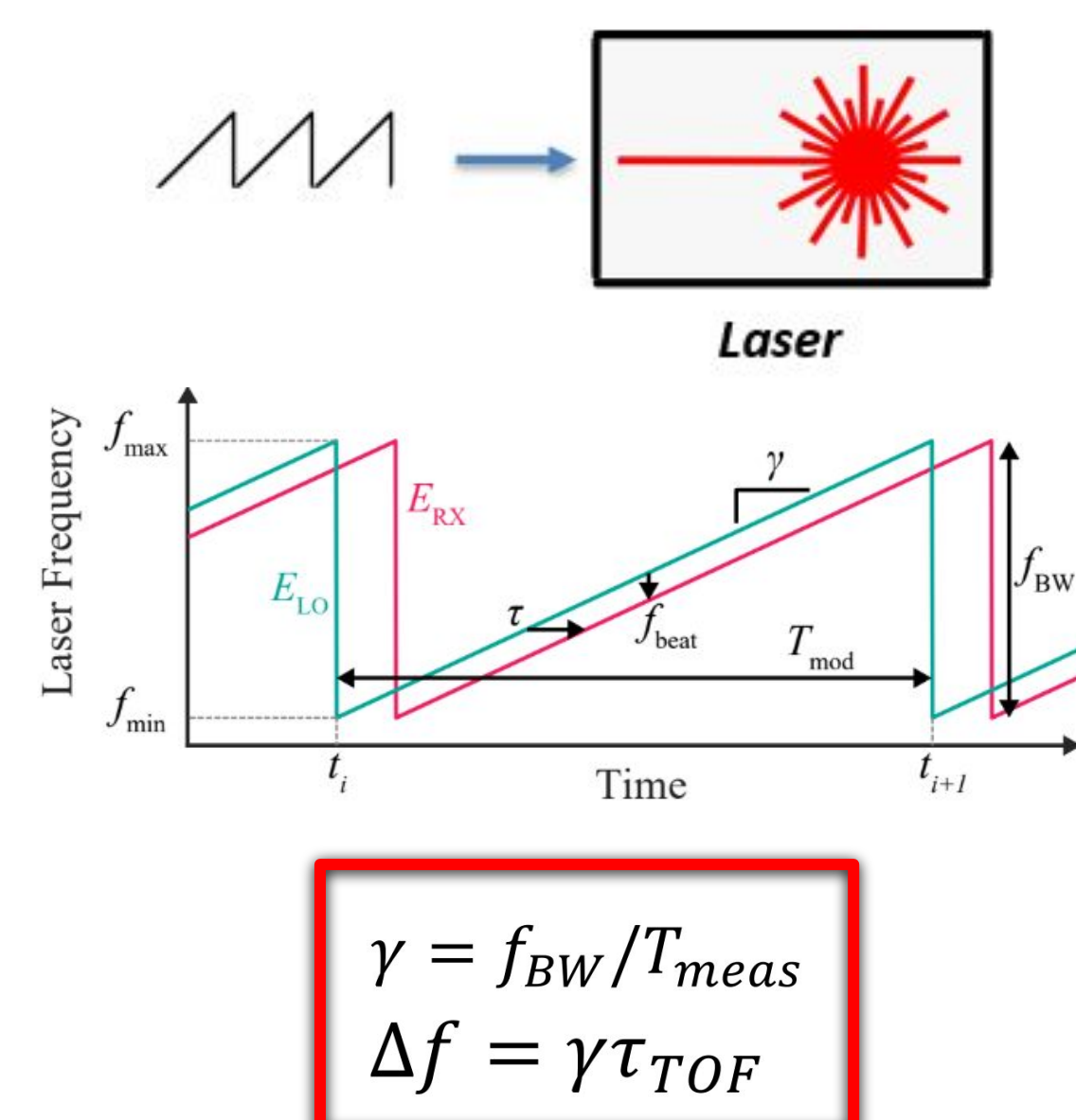
Background

- LiDAR is a major 3D imaging technology used for accurate range measurement
- Typical LiDAR systems can have security vulnerabilities that pose threats to human safety
- This work investigates:
 - Security vulnerabilities of LiDAR systems using MATLAB Simulink
 - Secure frequency encrypted beam-steering frequency modulated continuous wave (FMCW) LiDAR systems



FMCW Beam-Steering LiDAR

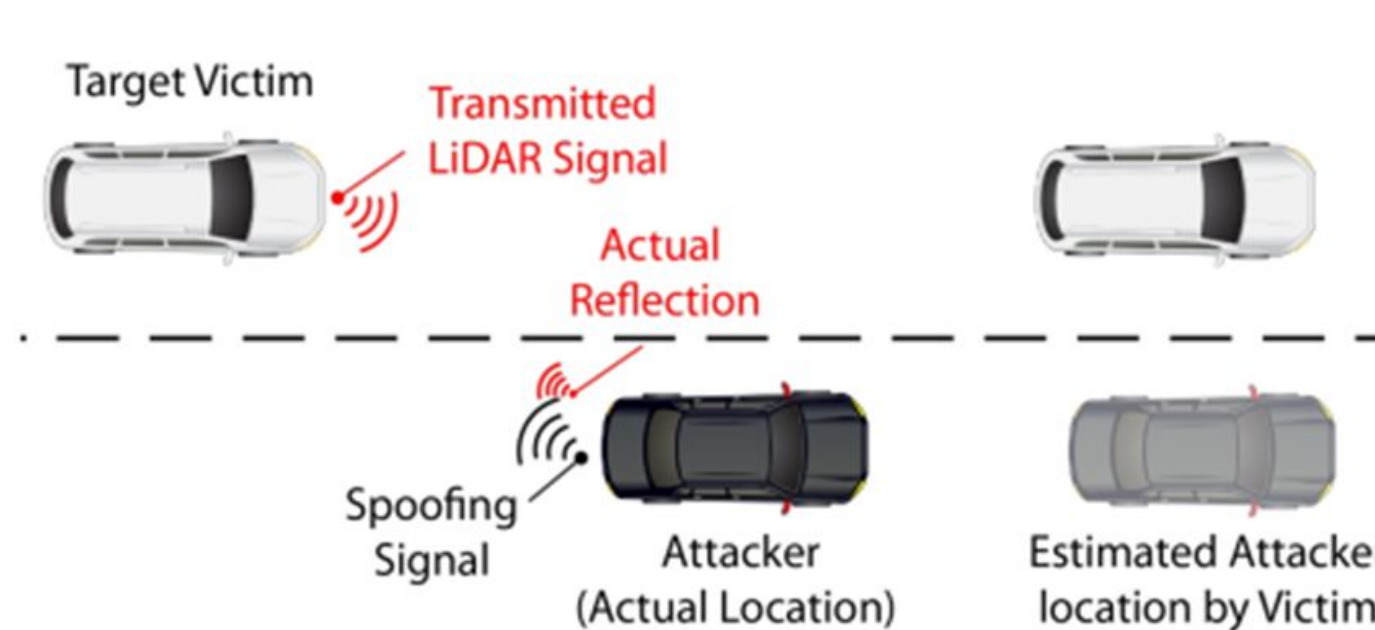
- Laser frequency is linearly modulated with a ramp signal
- There is a constant frequency difference between Tx and Rx signals known as *beat frequency*, which is linearly proportional to Time of Flight (TOF)
- At the receiver, RX and TX lights beat together the **distance to the object** is calculated from **Time of Flight**



Adversarial LiDAR System Attacks

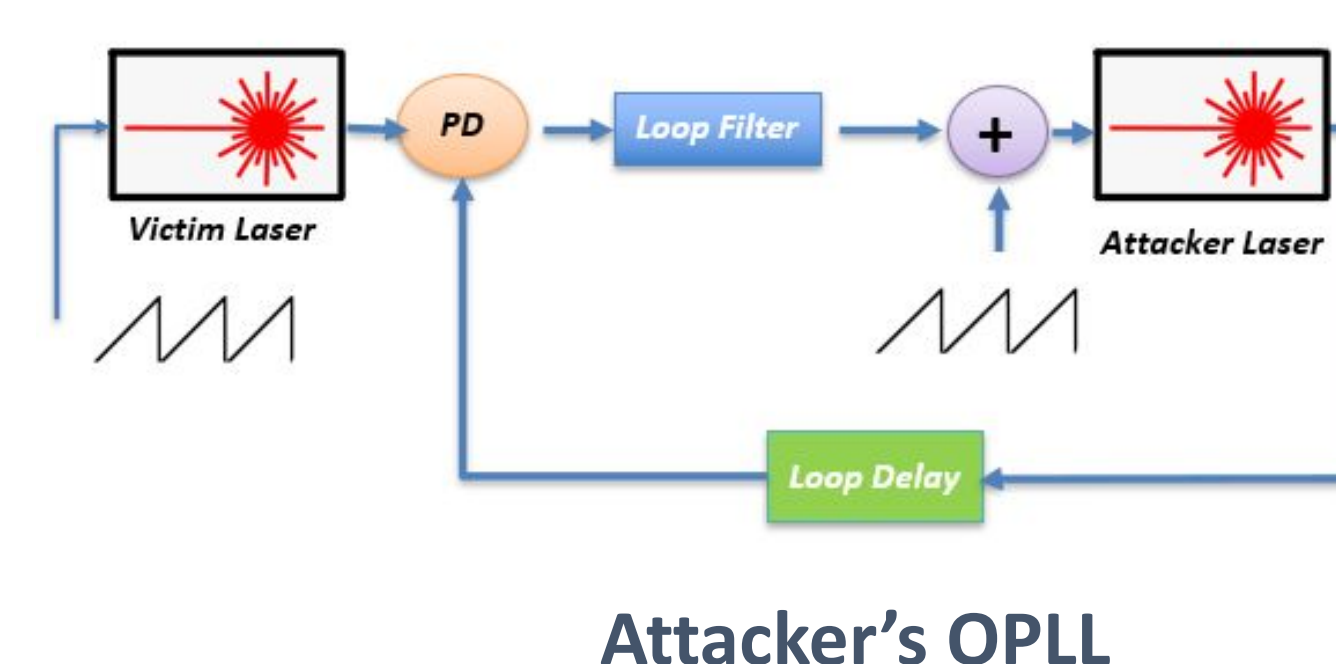
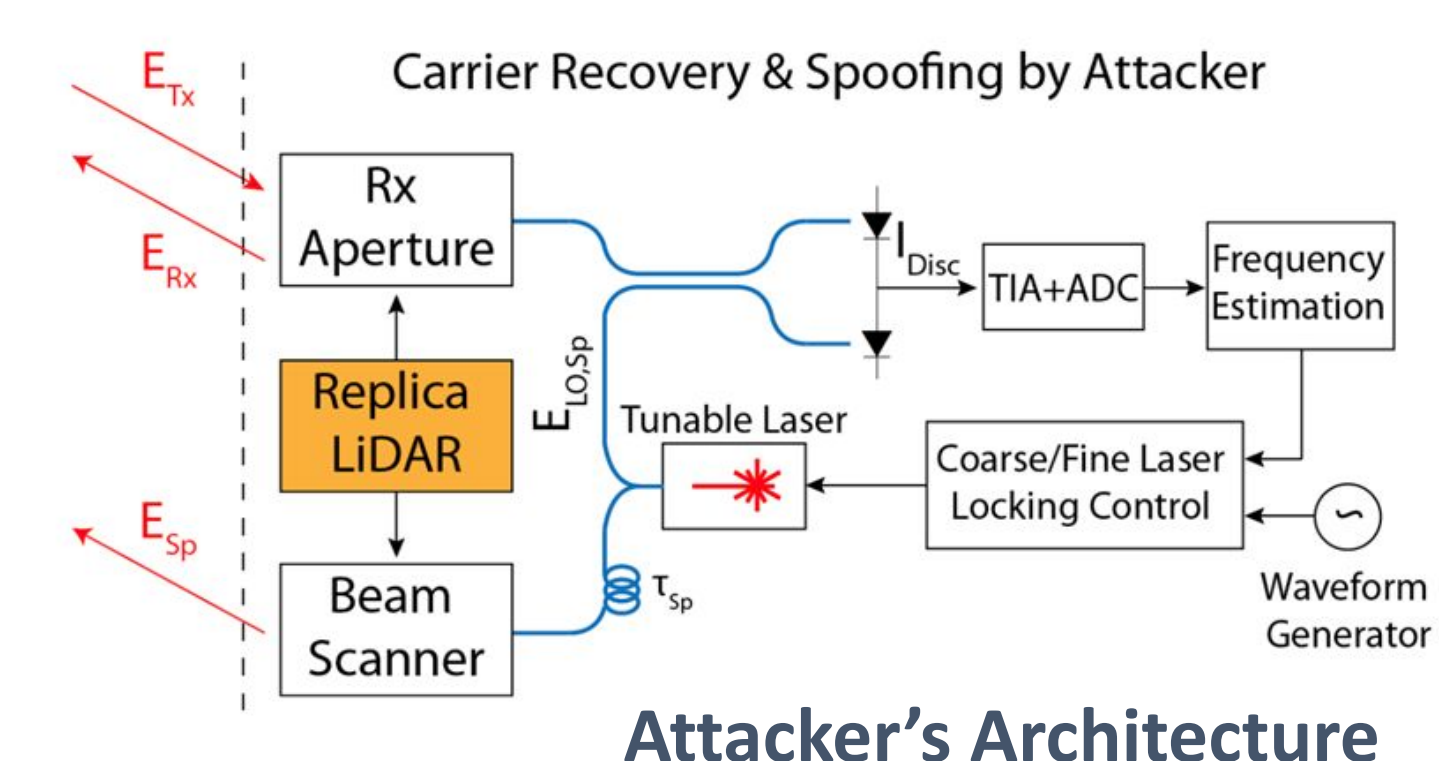
The most spiteful types of attacks are:

- Jamming:** Attacker transmits high power light to saturate victim's receiver
- Spoofing (Most Detrimental):** Attacker can lock its laser frequency to the victim's laser and overwrite the actual reflection



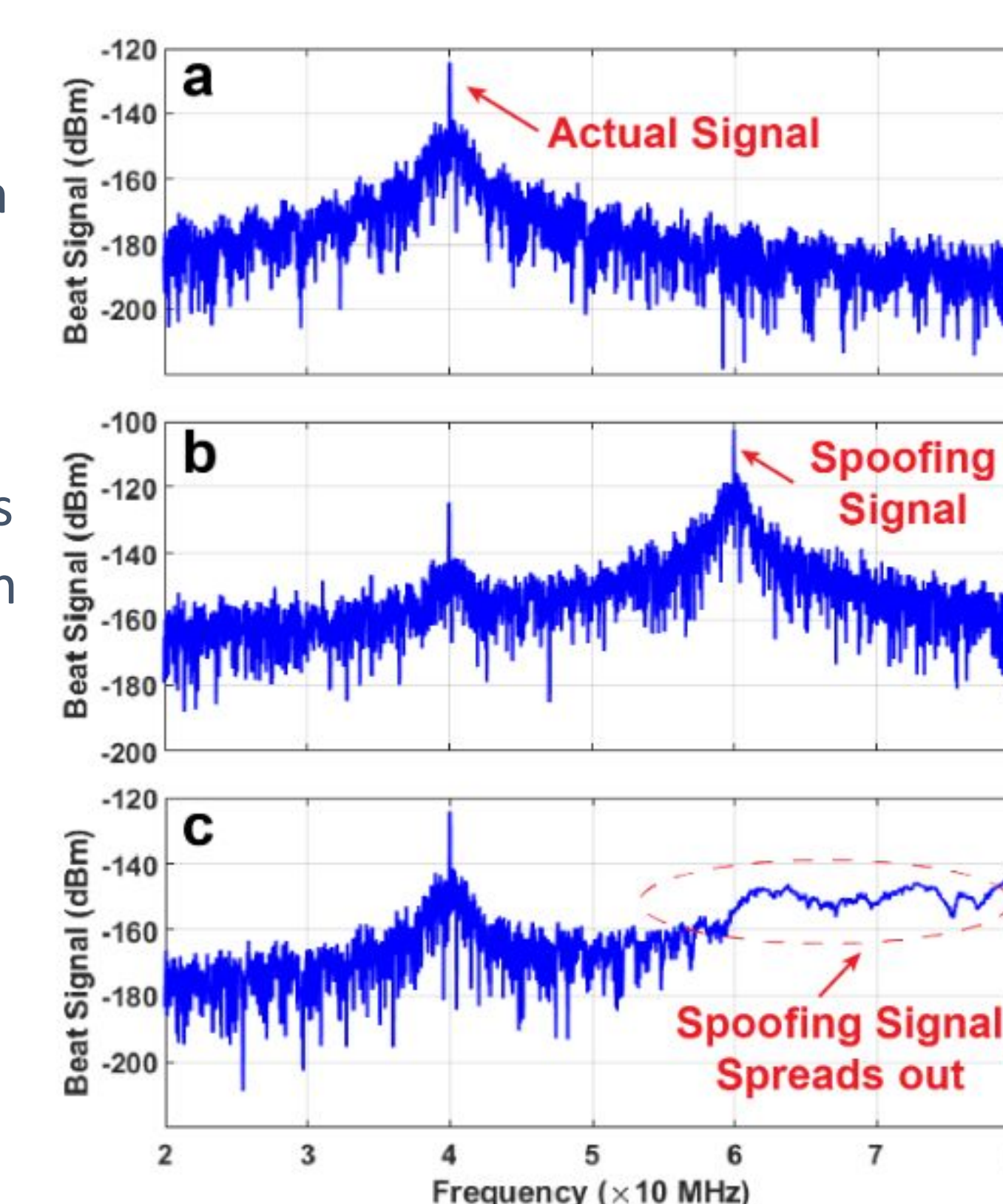
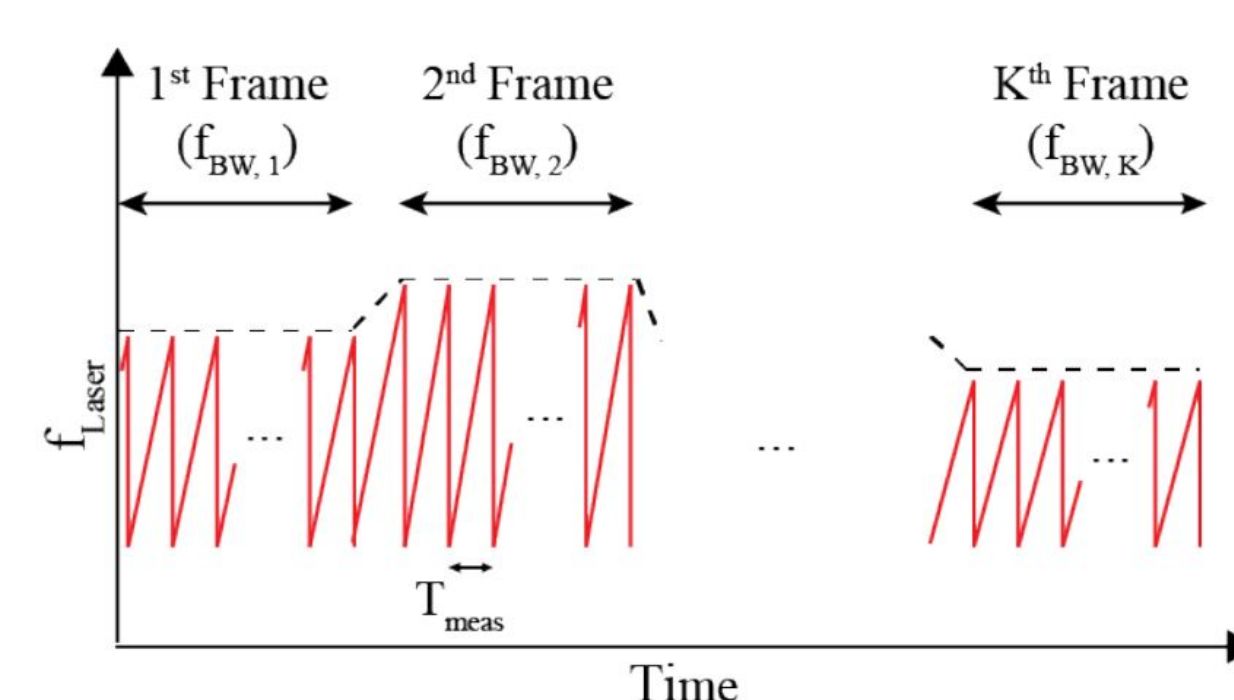
Spoofing Attack Architecture

- The attacker has a replica LiDAR- Optical Phased Locked Loop (OPLL)
- The proposed attacking scenario has 3 steps:
 - Coarse Tuning:** Decreasing the frequency offset between attacker's and victim's lasers
 - Fine Tuning (using the OPLL):** Locking attacker's laser frequency to the victim's laser using OPLL to find the chirp rate
 - Time Tuning (using zero-crossing method):** Finding the time delay between attacker's and victim's lasers, and delaying the spoofing signal to fool the victim's receiver system



Spoofing Attack Simulation Results & Attack Solution

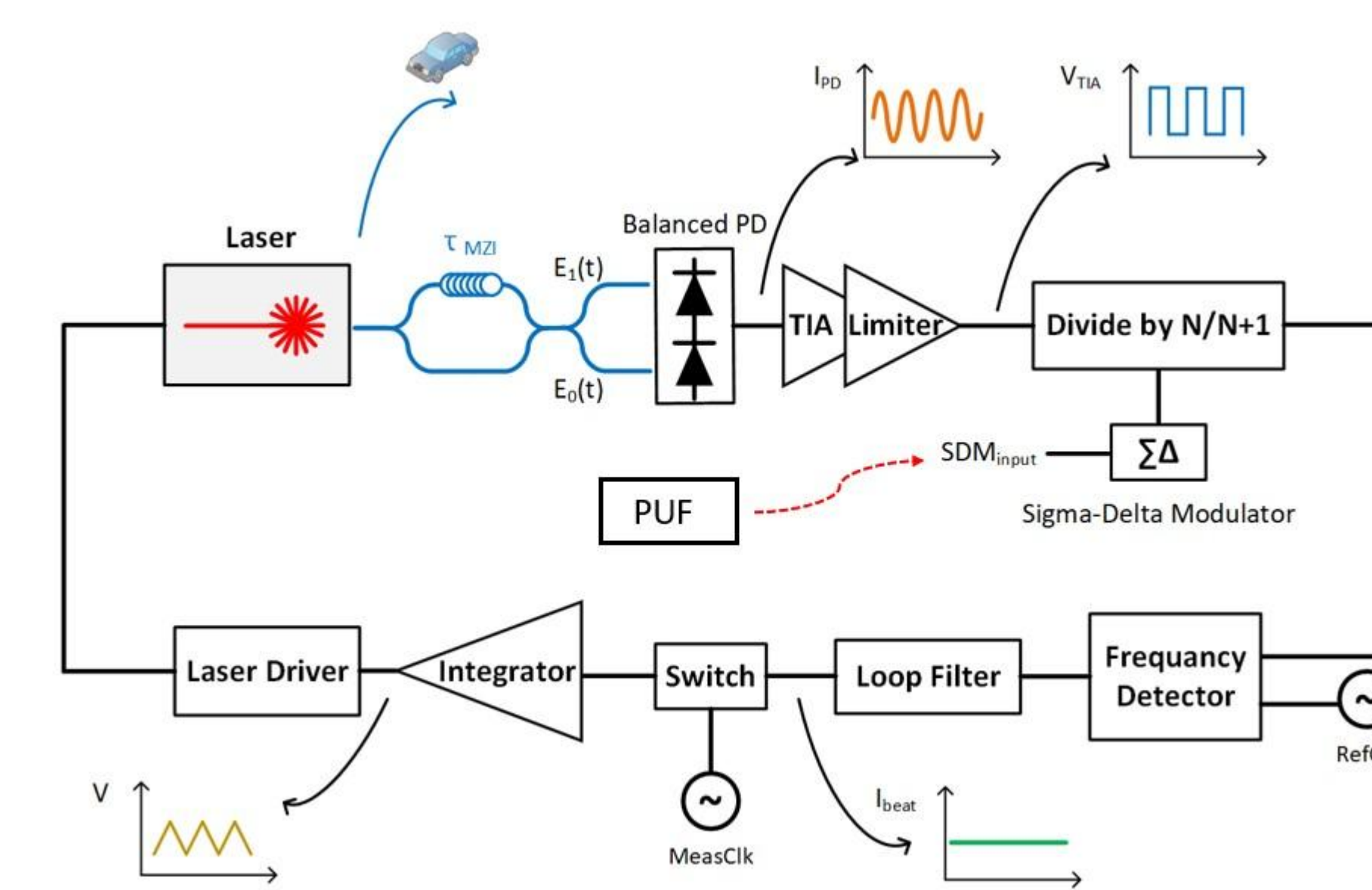
- Known chirp rate provides attacker with information necessary to attack LiDAR system
- Randomizing this chirp rate for each frame makes the system impossible to hack (chirp rate in Step 2 will be different)
- The minimum required $\Delta\gamma$ imposes trade-offs on the SNR, ranging precision and modulation bandwidth.



Beat signal at the victim's LiDAR: (a) without any spoofing signal, (b) with a spoofing signal with matching chirp rate, (c) with a spoofing signal with a different chirp rate ($\Delta\gamma/\gamma = \%20$)

Electro-Optical Synthesizer for FE-FMCW LiDAR Systems

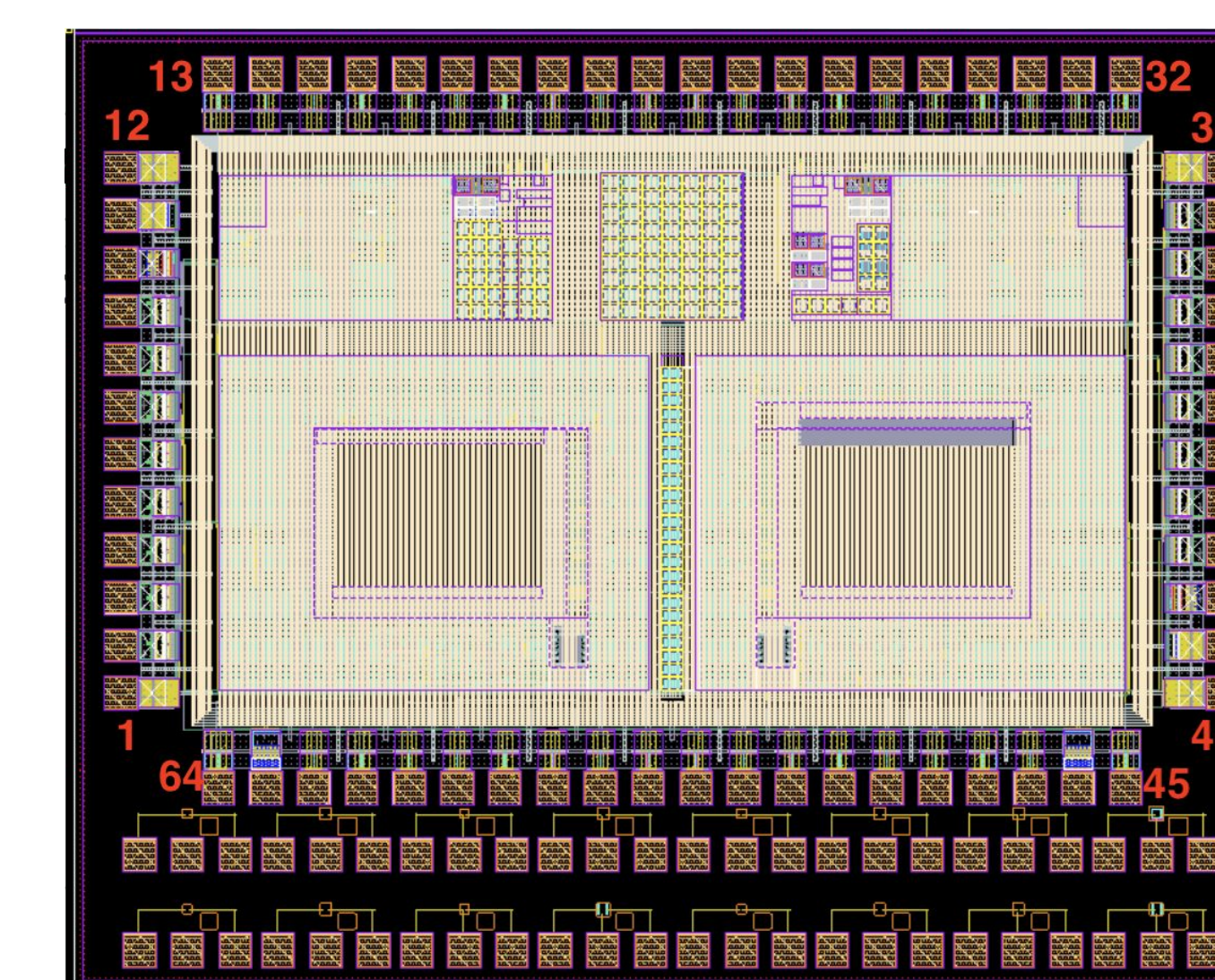
- Lasers can be modulated in a open loop and closed loop circuits
- We need a closed loop system to:
 - Mitigate laser nonlinearities
 - Remove disturbances effects
- When the loop is locked the input of the laser is a chirp signal with a desired chirp rate
- PUF block randomly changes the chirp rate



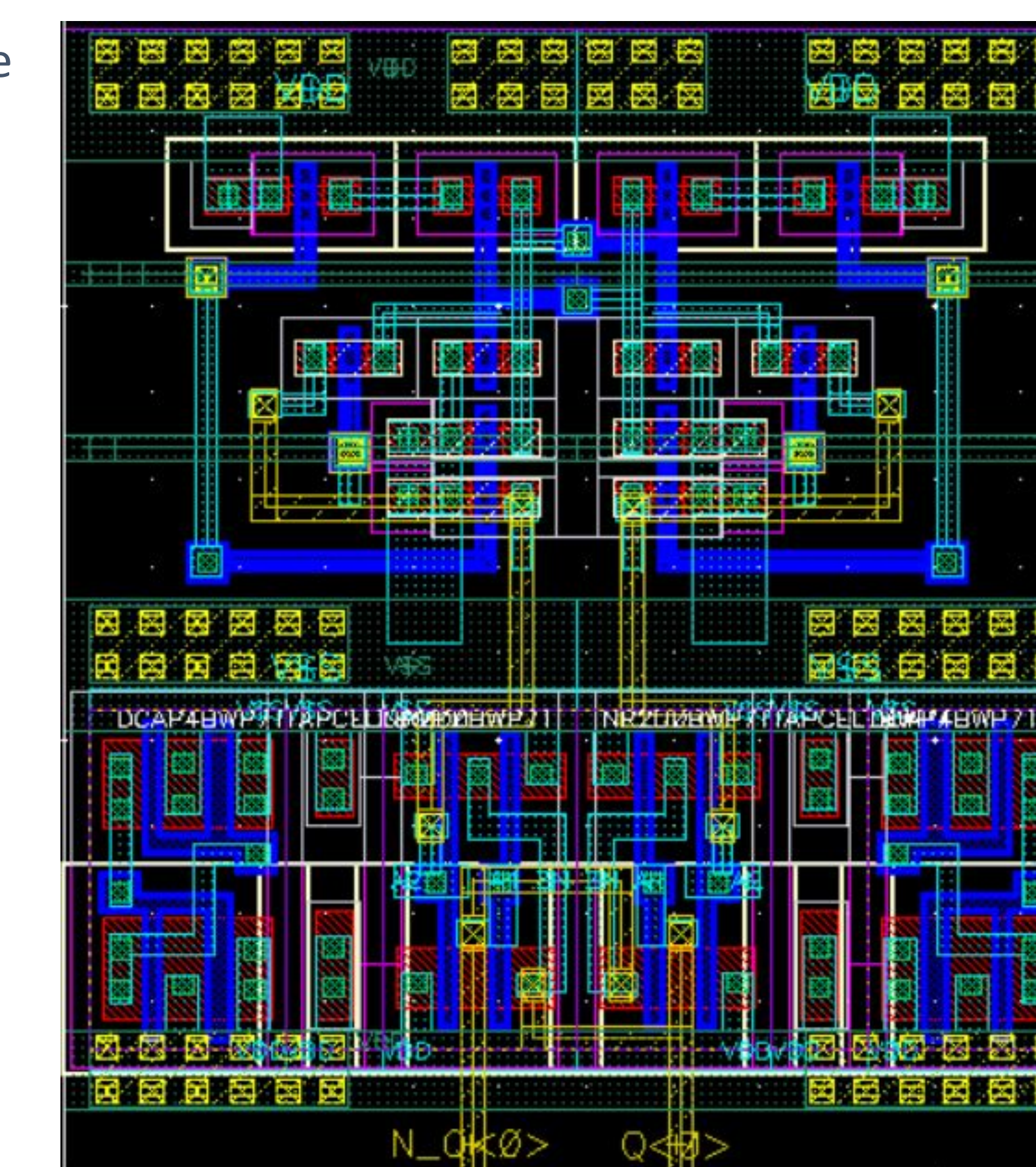
EO-Synthesizer architecture for a FE-FMCW LiDAR system

Frequency Encryption: Physically Unclonable Functions (PUF)

- Inherent variations in devices generate "unique" ID to be assigned for chirp rate generation
- SRAM topology used in conjunction with SR latch for random bitstream generation



FMCW IC



PUF Block Unit Cell

Next Steps/Acknowledgements

- Currently awaiting for chip to be sent back from fabrication
- Printed circuit board assembly and testing
- Special thanks to our advisor, **Professor Sajjad Moazeni** and the National Science Foundation (**NSF**) for their generous support, advice, expertise, and clarification on all matters big and small