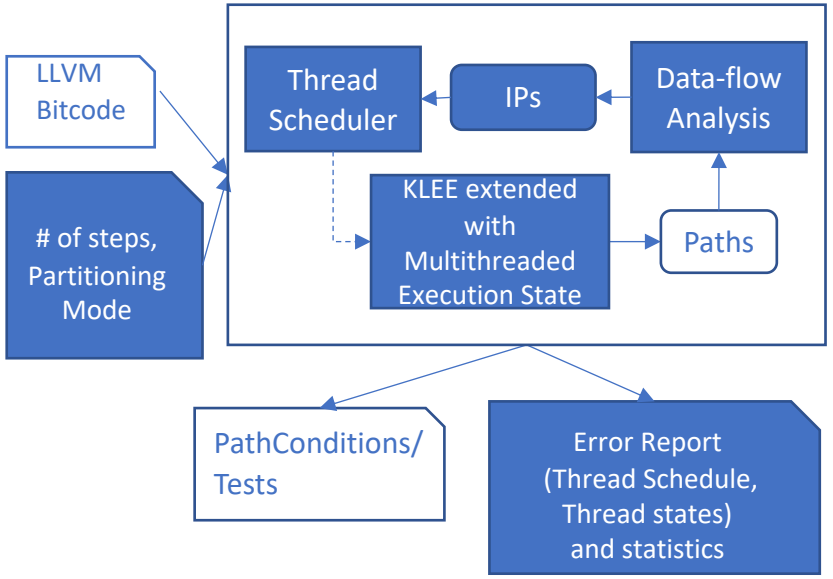
# SIFT: A Multithreading Extension to KLEE

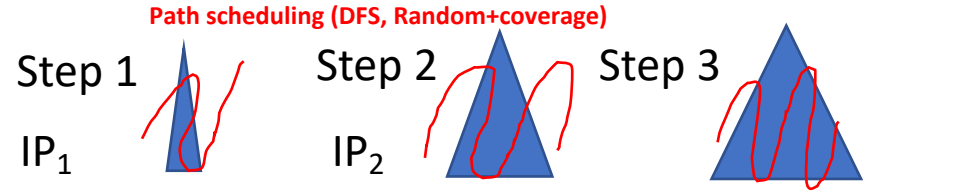
Tuba Yavuz, Associate Professor, ECE Department, University of Florida, tuba@ece.ufl.edu

## Architecture of SIFT

SIFT is a multithreaded extension of KLEE that performs selective thread scheduling to reveal bug triggering scenarios. It uses dynamic data-flow analysis and light-weight static analysis to identify property relevant interleaving points (IPs). Explicit properties include assertions within the code and memory safety is treated as the implicit property. Check out SIFT at https://github.com/sysrel/SIFT




## SIFT Exploration Steps

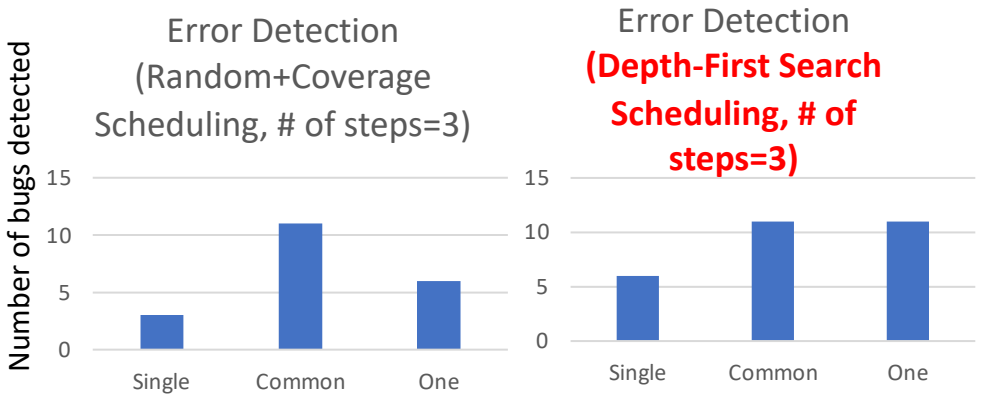



Conservative thread scheduling, i.e., when a thread blocks schedule another

New thread scheduling scenarios due to interleaving points in $IP_1$

New thread scheduling scenarios due to interleaving points in $IP_2 \setminus IP_1$

## SIFT on 10 CVE & 10 SVComp Benchmarks




Timeout=500secs

| Single | Common | One |
|---|---|---|
| > 0.07s < 19.96s | >0.07s <52.09s | >0.07s <24.62s |

**SIFT can detect the bugs in all 10 CVE benchmarks whereas ConVul misses one.**