SaTC:CORE:Small:Techniques for Software Model Checking of Hyperproperties

Challenge:

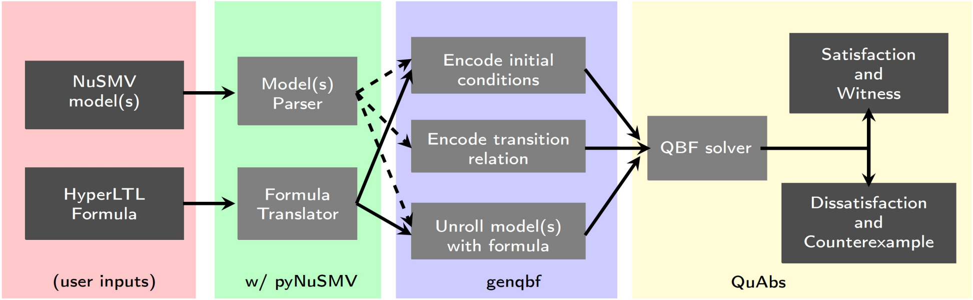
- Verification of ***information-flow security policies*** requires reasoning about multiple executions simultaneously.
- This increases the computation complexity significantly.
- Existing model checking tools are not able to handle verification of such polices.

Solution:

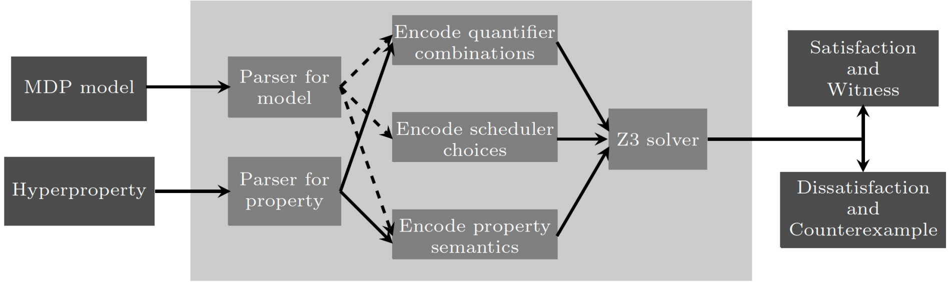
- We use the framework of ***hyperproperties.***
- We have designed new specification languages for hyperproperties (A-HLTL and HyperPCTL) to reason about hyperproperties.
- Effective model checking algorithms.

NSF Award 2100989
Michigan State University
PI: Borzoo Bonakdarpour (borzoo@msu.edu)

HyperQube



HyperProb



Scientific Impact:

- Verification of:
  - Scheduling attacks
  - Timing attacks
  - Secure compilation
  - Speculative execution
  - Concurrent information leaks
  - Cache flush attacks
  - Differential privacy
- Model Checking Tools
  - HyperQube
  - HyperProb

Broader Impact and Broader Participation:

- Partnership with Okemos High School in Michigan
- Partnership with women in computing and engineering clubs