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

Borzoo Bonakdarpour, Michigan State University

https://www.cse.msu.edu/tart/tools

Information leak due to nondeterminism

T1

```
1  while (true){
2    await sem>0 then
3      sem = sem - 1;
4      print('a');
5      v = v+1;
6      print('b');
7      sem = sem + 1;
8  }
```

T2

```
1   while (true){
2     print('c');
3     if (h == l) then
4       await sem>0 then
5         sem = sem - 1;
6         v = v+2;
7         sem = sem + 1;
8     else
9       skip;
10    print(`d');
11  }
```

T3

```
1  while (true)
2    h = read(Channel1);
```

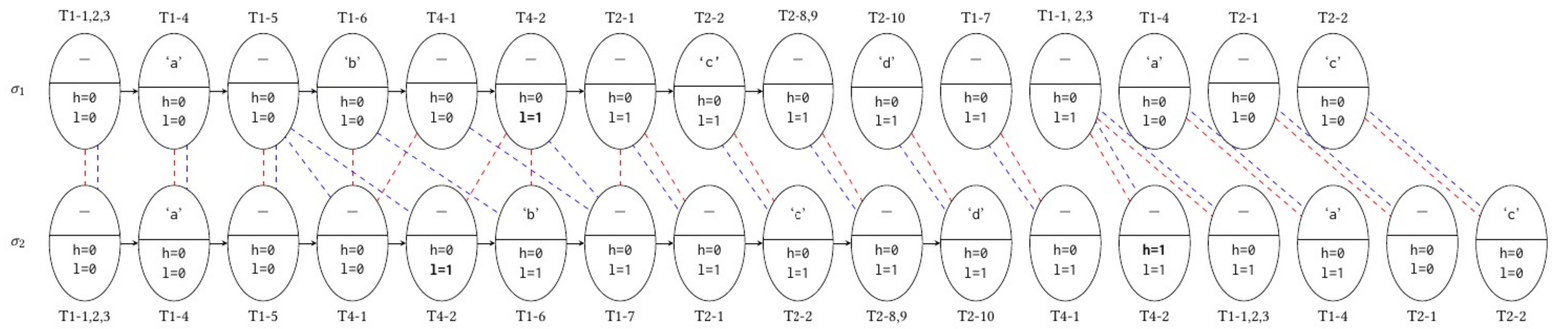
T4

```
1  while (true)
2    l = read(Channel2);
```

MICHIGAN STATE UNIVERSITY

Challenge:

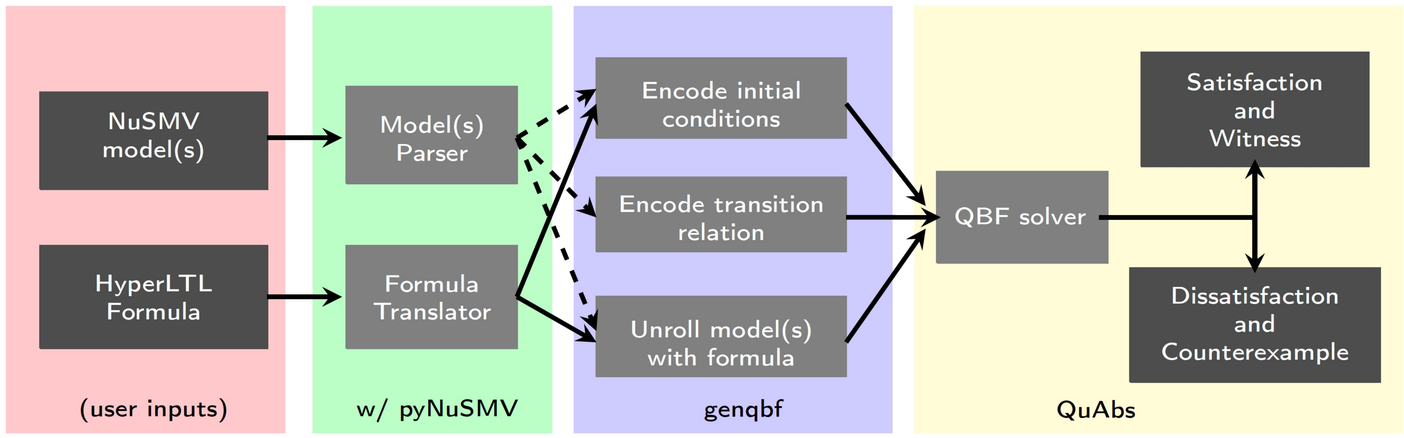
- Verification of *information-flow security policies* requires reasoning about multiple executions simultaneously.
- This increases the computation complexity significantly.
- Existing model checking tools are not able to handle verification of such polices.



Solution:

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

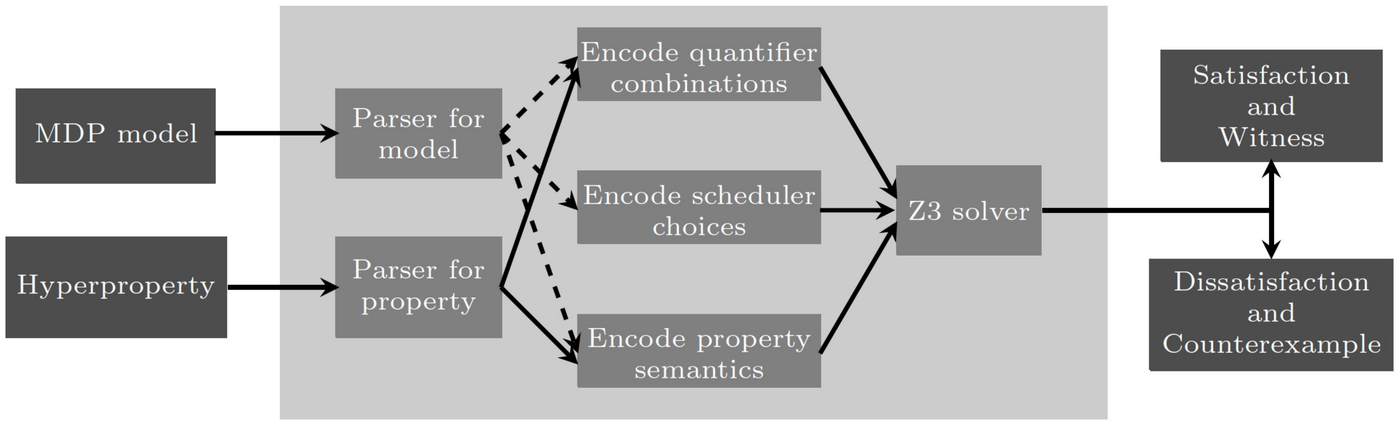
The Tool HyperQube



Scientific Impact:

- Verification of:
  - –Scheduling attacks
  - –Timing attacks
  - –Secure compilation
  - –Speculative execution
  - –Concurrent information leaks
  - –Cache flush attacks
  - –Differential privacy

The Tool HyperProb



Broader Impact and Broader Participation:

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