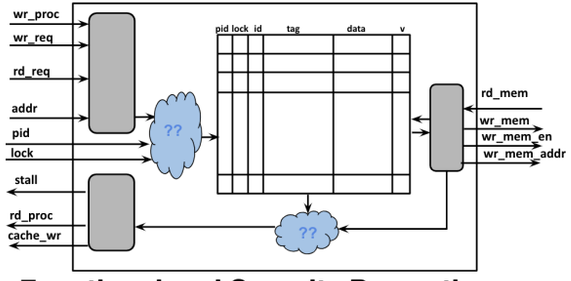
1) Sketch and Specification

Sketch: Incomplete Verilog Design

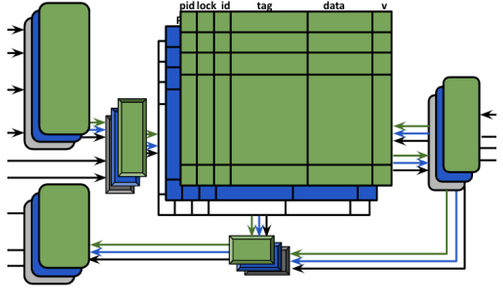


Functional and Security Properties, and Soft Constraints

```
if(pid == i && preload[addr])
   assume (index_s == High);
if(pid != i)
   assert (rd_proc_t == Low);
try (!skip && lru_update);
```

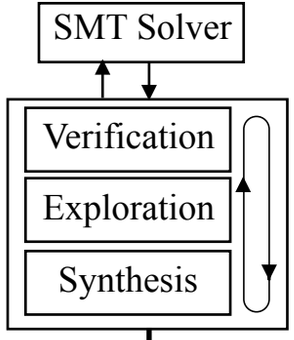
2) Instrumentation

Verilog Instrumented with Security Labels



3) Program Synthesis

Constraint-based Synthesis (CEGIS)



SAT

UNSAT

Modify Sketch and/or Properties

4) Secure and Correct Hardware Design

Verified Verilog