Transys: Leveraging Common Security Properties Across Hardware Designs

Rui Zhang (Presenter), Cynthia Sturton (PI)
University of North Carolina at Chapel Hill
https://www.cs.unc.edu/~csturton/HWSecurityatUNC/

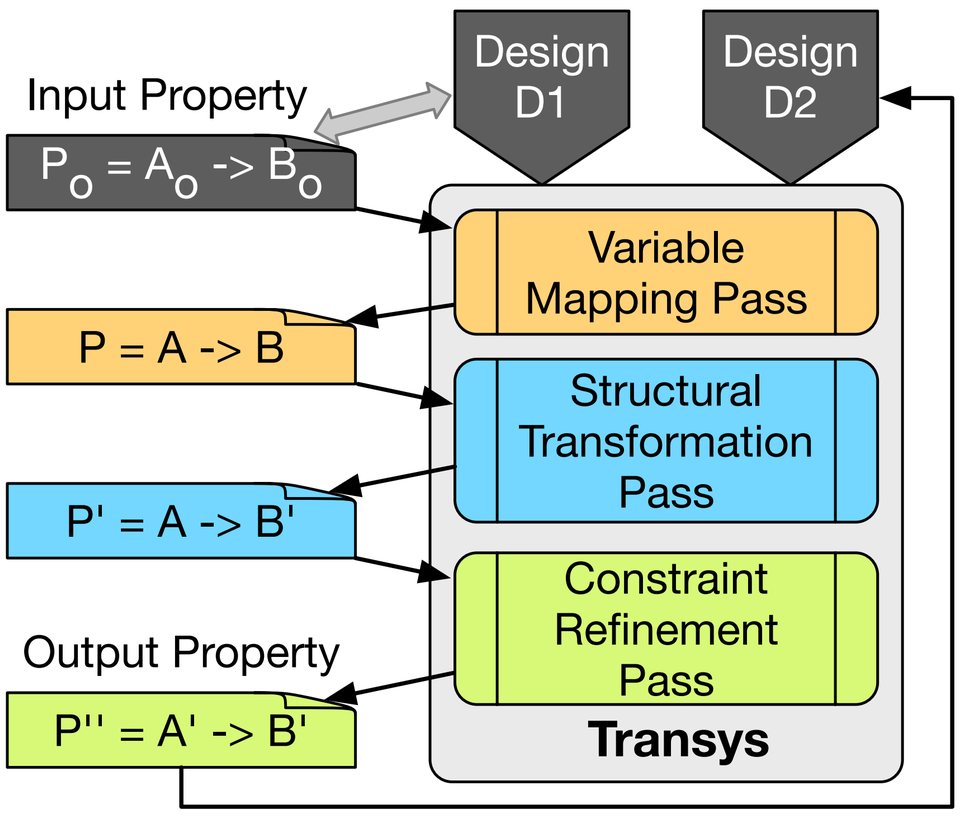
Background

- Validating the security of hardware designs is important.
- Assertion based verification (ABV) can be used for hardware security validation.

Insight

- Security properties developed for one hardware design can be leveraged and used for a second design.

Transys [IEEE S&P 2020]



Progress

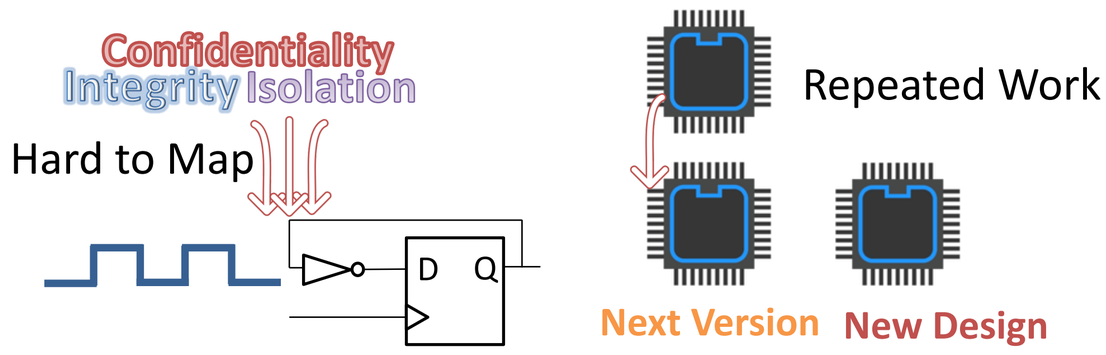
- A systematic approach for security property translation.
- A tool chain implementing our methodology.
- An evaluation of Transys for 36 properties on 38 AES, 3 RSA, and 5 RISC designs.

Intellectual Merit

- Exploration of the feasibility of property translation across hardware designs.
- Moving toward automating the identification and generation of hardware security properties.

Motivation

- Developing a comprehensive set of security properties is challenging.



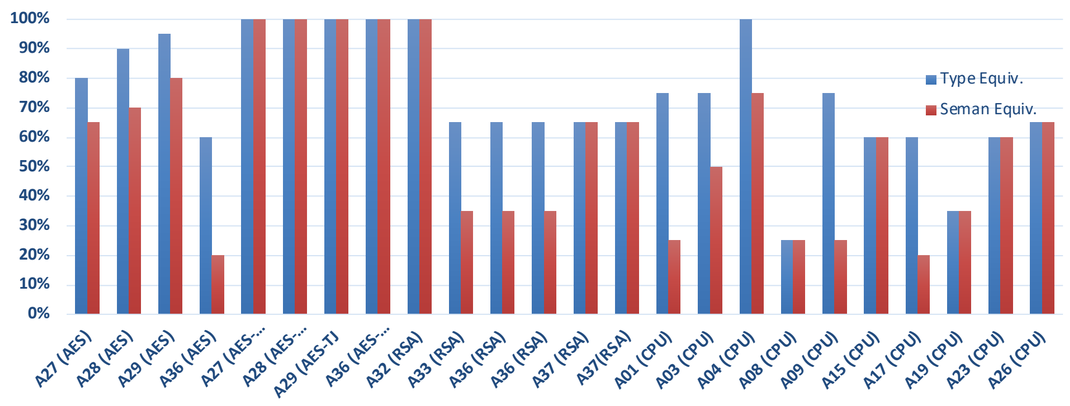
- Goal: Reduce the manual effort for developing security properties.

Approach

- **Variable Mapping**: Use features from AST, PDG to find appropriate counterpart.
- **Structural Transformation**: Learn the arithmetic expression between variables from PDG.
- **Constraint Refinement**: Add terms to the antecedent to make the property valid.

Main Results

Designs	Total Transl.	Total Succ.	Rate
AES	360	336	93%
AES w/ Trojans	400	400	100%
RSA	18	18	100%
CPU	46	39	85%
Total	824	793	96%



Designs	Average Transl. Time
AES	28.8s
RSA	0.46s
CPU	189s
Average	70s

Broader Impact

- Improving the state of the art in developing hardware security properties.