Härtung der Wertschöpfungskette durch quelloffene, vertrauenswürdige EDA-Werkzeuge und Prozessoren.

Projektziel:

Verlässlichkeit und Vertrauenswürdigkeit durch

- Quelloffene Hardware (RISC-V)
- Quelloffene Werkzeuge (OpenRoad)
- Formale Verifikation

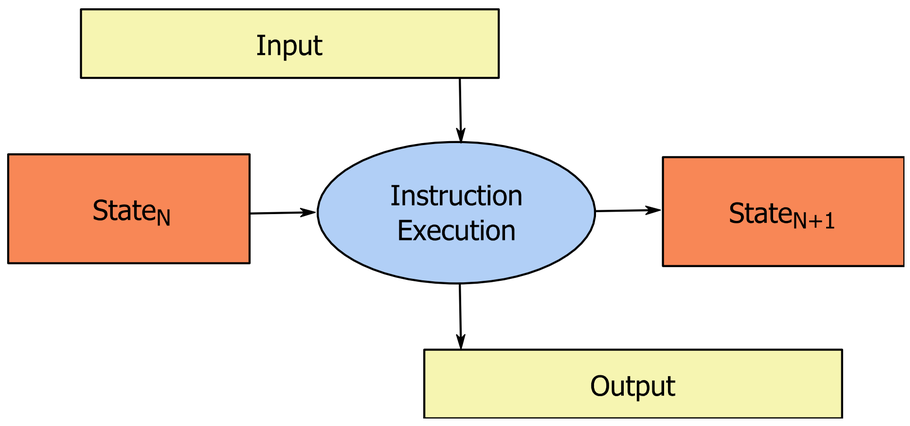
Ziel des Projekts ist es, erstmals wesentliche Teile der gesamten Wertschöpfungskette im Bereich Entwicklung und Fertigung von sicherheitsrelevanten Chips (Hardware Security Module) in Open Source zu realisieren. Dies bezieht sich sowohl auf die Entwicklung der Hardware als auch auf die Implementierung von Härtungsmechanismen, also dem Schutz vor Angriffen. Weiterhin werden Schwachstellen der Hardware-Wertschöpfungskette analysiert und offengelegt.

Funktionale Verifikation einer RISC-V CPU

Für die funktionale Verifikation wird eine Spezifikation des Systemverhaltens und ein (abstrahiertes) Modell des Systems benötigt. Das korrekte Verhalten wird durch Funktionen FS und FO für den Zustandsübergang und die Ausgabe modelliert :

$$State_{N+1} = FS(State_N, Input)$$
$$Output = FO(State_N, Input)$$

In unserem Fall wird das Systemverhalten durch die RISC-V ISA definiert, und das Modell des Systems (VexRiscV) ist in SpinalHDL formuliert. Der Zustand $State$ des abstrakten Modells ist die CPU mit all ihren Registern.

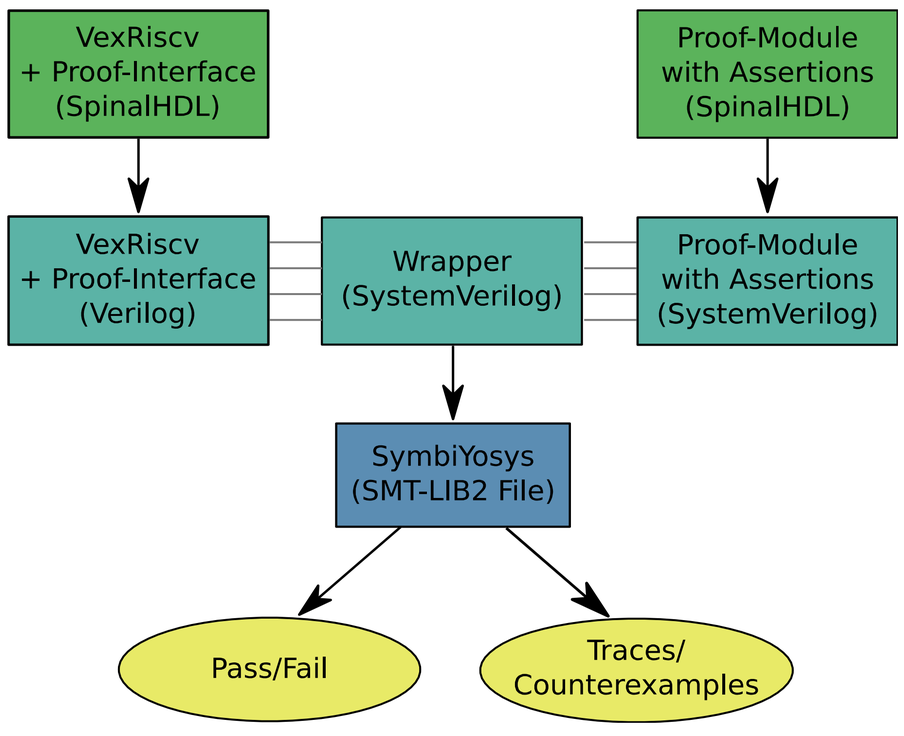


Aufbau und Werkzeugkette

Den Kern des formalen Beweises bildet eine in SpinalHDL formulierte Version der RISC-V ISA, welche in Abhängigkeit von einem Startzustand und Eingangssignalen die zu erwartende Systemreaktion ausgibt.

Diese kann nun mit der tatsächlichen Reaktion der RISC-V CPU abgeglichen werden. Die nötigen Informationen müssen dafür mittels eines Interfaces zur Verfügung gestellt werden.

Die Werkzeugkette übersetzt den Beweis und das Modell von SpinalHDL nach SystemVerilog, und nutzt SymbiYosys mit STM-Backend als Beweis-Engine:



Der Beweis ist in hochgradig parametrisierbar und kann so voll automatisiert in vielen Teilbeweisen generiert und ausgeführt werden. Damit ist die Nutzung bereits während des Design-prozesses möglich und die Ausführungszeit sinkt drastisch.

Evaluation

Für eine ausführliche Evaluation werden mit Yosys beliebig viele Mutationen der RISC-V CPU generiert und die entsprechenden Beweisergebnisse mit dem der Referenz verglichen.

Ergebnisse der Verifikation

- Induktionsanfang erfolgreich (16 Zyklen)
  - Core benötigt 9 Zyklen Startup
  - 7 Zyklen reguläre Ausführung von Instruktionen (Tiefe der Pipeline: 6)
  - 1521 Zeilen SpinalHDL, 1646 Zeilen SystemVerilog
- Ausführliche Evaluation mittels Mutationen
- Bewiesene Eigenschaften:
  - Korrekte Erkennung von illegalen Instruktionen/ Ausnahmen
  - Ausführung von 37 Basisinstruktionen
  - Korrekte Arithmetik der ALU
  - Korrektes Lesen und Schreiben der Register
  - Korrektes Verhalten des PC
  - Korrekte Interaktion mit dem Speicher

Partner:

Assoziiert:

Gefördert durch

Bundesministerium für Bildung und Forschung

Im Rahmen der Leitinitiative “*Vertrauenswürdige Elektronik*”.

Förderkennzeichen: 16KIS1342

Kontakt: Prof. Dr. Christoph Lüth

Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH
FB Cyber-Physical Systems

Phone: +49 218 59830
E-Mail: christoph.lueth@dfki.de
Web: www.dfki.de/cps