技術白皮書

基於形式驗證的高效RISC-V處理器驗證方法

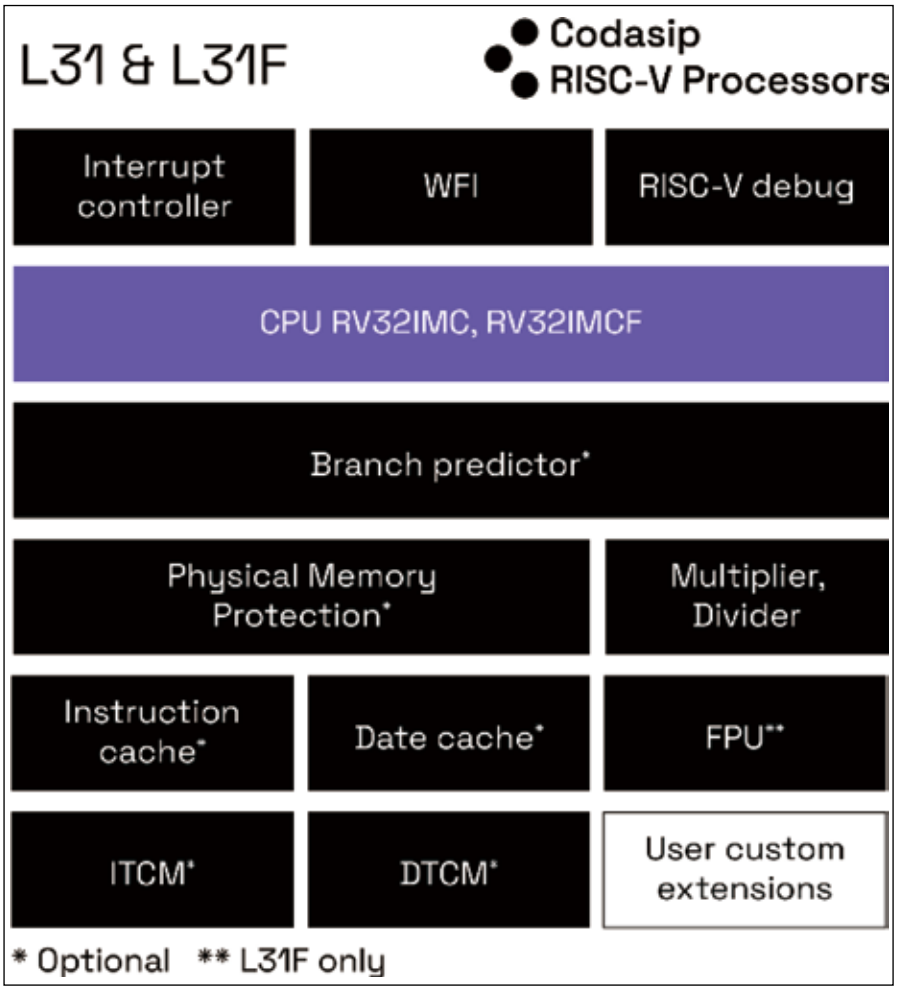
■作者：Laurent Arditi, Paul Sargent, Thomas Aird
Codasip 高級驗證 / 形式驗證工程師

RISC-V 的開放性允許定制和擴展基於 RISC-V 內核的架構和微架構，以滿足特定需求。這種對設計自由的渴望也正在將驗證部分的職責轉移到不斷壯大的開發人員社群。然而，隨著越來越多的企業和開發人員轉型 RISC-V，大家才發現處理器驗證絕非易事。新標準由於其新穎和靈活性而帶來的新功能會在無意中產生規範和設計漏洞，因此處理器驗證是處理器開發過程中一項非常重要的環節。

在複雜性一般的 RISC-V 處理器內核的開發過程中，會發現數百甚至數千個漏洞。當引入更多高級特性的時候，也會引入複雜程度各不相同的新漏洞。而某些類型的漏洞過於複雜，導致在模擬環節都無法找到它們。因此必須通過添加形式驗證來賦能 RTL 驗證方法。從極端漏洞到隱匿式漏洞，形式驗證能夠讓您在合理的處理時間內詳盡地探索所有狀態。

在本文中，我們將介紹一個基於形式驗證的、易於調動的 RISC-V 處理器驗證程式。與 RISC-V ISA 黃金模型和 RISC-V 合規性自動生成的檢查一起，展示了如何有效地定位那些無法進行模擬的漏洞。通過為每條指令提供一組專用的斷言範

圖 1：Codasip L31 處理器內核架構圖解 (來源：Codasip)



本來實現高度自動化，不再需要手動設計，從而提高了形式驗證團隊的工作效率。

1、基於先進內核的處理器開發

嵌入式系統的應用越來越廣泛，同時對處理器的性能、功耗和面積 (PPA) 要求越來越高，因此我們將這樣的產業和技術背景下用實際案例來分析處理器的驗證。Codasip L31 是一款用於微控制器應用的 32 位中端嵌入式 RISC-V 處理器內核。作為一款多功能、低功耗、通用型的 CPU，它實現了性能和功耗的理想平衡。從物聯網設備到工業和汽車控制，或作為大型系統中的深度嵌入式內核，L31 可在一個非常小巧緊湊的矽片面積中實現本地處理能力。L31 是通過 Codasip Studio 使用 CodAL 語言設計而成，該內核完全可定制，包括經典的擴展和特性，以及實現這些擴展和特性所需的高效和徹底的驗證。

表 1：Codasip L31 內核展示了 RISC-V 處理器的優異特性

特性	描述
指令集架構 (ISA)	RV32 I/M/C/F/B
流水線	3 級順序流水線
分支預測器	可選，優化過的單執行緒性能
並行乘法器	並行實現，單週期乘法
序列除法器	循序執行
記憶體保護	●具有 2/4/8/16 個區域的可選 MPU ●具有 2/4/8/16 個區域的實體記憶體屬性 機器和使用者許可權模式
緊耦合記憶體 (TCM)	●指令和資料 TCM ●可定制大小高達 2MB AHB-Lite TCM 輔助埠
介面	用於獲取和資料的 32 位元 AHB-Lite 介面 (帶緩存的 AXI-Lite)
浮點單元 (FPU)	可選，單精確度
調試	●標準 RISC-V 調試 ● 2/4 JTAG ● 2-8 個中斷點和觀察點 ●系統匯流排接入
中斷	●中斷控制器 ●標準 RISC-V CLINT 執行 ●多達 128 個中斷 ● WFI(等待中斷) ● NMI(不可遮罩中斷)

2、創建最優的 RISC-V 處理器驗證方法

處理器驗證需要制定合適的策略、勤勉的工作流程和完整性，而方興未艾的、更加靈活的 RISC-V 處理器開發則需要針對自己處理器功能設置做詳盡的驗證規劃；也需要參考一些內核供應商的內外部因素，比如該供應商自己的開發工具體現和外部開發工具夥伴，以及同系、同款或者同廠內核的出貨量等。

驗證處理器意味著需要考慮諸多不確定性。最終產品將運行什麼軟體？用例是什麼？可能發生哪些非同步事件？這些未知數意味著較大的驗證範圍。然而，覆蓋整個處理器狀態空間是無法實現的，這也不是 Codasip 這樣的領先內核供應商的目標。

在確保處理器品質的同時，充分利用時間和資源才是處理器驗證的正解。明智的處理器驗證意味著在產品開發過程中儘早並高效地發現相關漏洞。在頂層方面，Codasip 提供了多種創新的驗證路徑，其驗證方法基於以下內容：

- 驗證是在處理器開發期間與設計團隊合作完成的。
- 驗證是所有行業標準技術的組合。使用多種技術可以讓您最大限度地發揮每一種技術的潛力，並有效地覆蓋盡可能多的極端情況。

●驗證需持續進行。有效的辦法是運用隨著處理器複雜程度而不斷發展的技術組合。

在驗證 L31 內核時，我們的想法是讓模擬和形式驗證相輔相成。

2.1 模擬的優勢和目的

模擬實際上不可或缺，它允許我們在兩個級別上進行驗證設計：

●頂層模擬 (Top-level)，主要是為了確保設計在最常見的情況下符合其規範 (CPU 的 ISA)。

●塊級模擬 (Block-level)，以確保微架構按照預期設計。然而，很難將這些檢查與頂層架構規範聯繫起來，因為這通常依賴於定向隨機測試生成，因此能夠應付棘手和不尋常的情況。

頂層模擬通常不像塊級模擬那樣特意強調設計。因此，它可以實現針對 ISA 的設計的整體驗證。

2.2 形式驗證的優勢和目的

形式驗證使用數學技術對以斷言形式編寫的問題提供有關設計的明確答案。

形式驗證工具對斷言和設計的組合進行詳盡的分析。不需要指定任何刺激，除了指定一些非正常情況以避免假漏洞。該驗證工具可以提供詳盡的“已證實”答案或“失敗”答案，同時生成顯示刺激的波形，證明斷言是錯誤的。在大型和複雜的設計中，工具有時只能提供有限的證明，這意味著從重置到特定數量的週期都不存在漏洞場景。同時也存在不同的技術方法來增加該週期迴圈次數，或獲得“已證明”或“失敗”的答案。

形式驗證用於以下情況：

●為完整的驗證一個模組，潛在地消除了任何模擬的需要。由於形式驗證的計算複雜性，形式化驗收 (sign-off) 僅限於小模組。

●除了模擬之外，還要驗證一個模組，即使是個大模組，因為形式驗證能夠在極端情況下找到漏洞，而隨機模擬只能“靠運氣”找到，而且概率非常低。

●處理一些模擬不充分的驗證任務，例如時鐘門控、X 態傳播 (X-propagation)、資料增量處理 (CDC)、等價性檢查等。

●說明調查缺少調試資訊的已知漏洞，並確定潛在的設計修復。

●對漏洞進行分類和識別，以便通過形式驗證來學習和改進測試平臺 / 模擬。

●為了潛在地幫助模擬，填充覆蓋範圍中的漏洞。

3、解決方案：一種基於形式驗證的高效的 RISC-V 處理器驗證方法

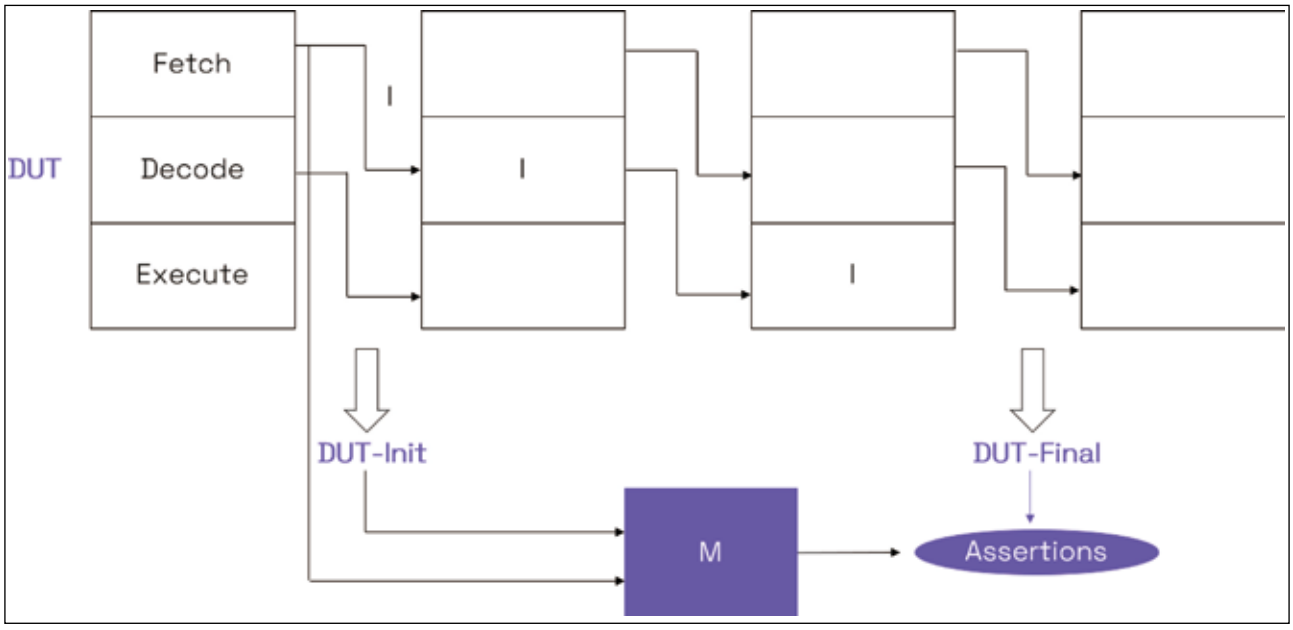
為了獲得一種高效的RISC-V處理器驗證方法，我們決定以採用西門子 EDA 處理器驗證 APP 來高效驗證 Codasip L31 RISC-V 內核為例，來進行詳盡的說明。該工具的目標是確保 RTL 級別的處理器設計正確且詳盡地實現指令集架構 (ISA) 規範，而本文希望介紹的是一種端到端的解決方案

1. 該工具從一個頂層並有效的“黃金模型”中生成以下：
   ●在 Verilog 語言中，ISA 的單週期執行模型。
   ●一組斷言，用於檢查待測試模組 (DUT) 和模型 (M) 在架構級別的功能是否相同。
   注意：這並沒有進行任何正式等價性檢查。
2. 當在 DUT 中獲取新指令 (I) 時，會捕獲架構狀態 (DUT-init)。
3. 該指令在流水線中運行。
4. 捕獲另一個架構狀態 (DUT-final)。
5. M 被輸入 DUT-init 和 I，並計算出一個新的 M-final 狀態。
6. 斷言檢查 M-final 和 DUT-final 中的資源是否具有相同的值。

這種端到端的驗證方法可以在比整個 CPU 更小、更簡單的模組 (例如資料緩存) 上合理實現。可以在緩存上寫入端到端斷言，以驗證寫入特定位址的資料是否從同一位址正確讀取。這使用了眾所周知的形式驗證技術，例如記分牌演算法。

然而，對於 CPU 來說，手動編寫這樣的斷言

圖 2:3 級 L31 內核的端到端驗證流程 (當驗證指令 I 既沒有停止也沒有清除緩存資料時)



是不可行的。它需要指定每條指令的語義，並與所有執行模式交叉。這通常根本不可能實現。CPU 的形式驗證被分成更小的部分，但是仍然無法驗證所有部分是否正確執行了 ISA。

使用建議的方法意味著能夠立即驗證完整的 L31 內核，而無需編寫任何複雜的斷言。如上所述，黃金模型和檢查斷言是自動生成的。

這種方法同時具有高度可配置性和自動化性，特別是對於 RISC-V CPU，例如 L31：

- 用戶可以指定設計執行的頂層 RISC-V 參數和擴展。
- 該工具能夠自動從設計中提取資料，例如將架構寄存器與實際每秒浮點運算次數相關聯。
- 該工具允許添加自訂，例如用來驗證的新指令 (具有為使用者“擴展”黃金模型的能力)。

最後，黃金模型不是由 Codasip 開發的 (除了一些自訂部分)，這一事實提供了額外的保證，這從驗證獨立性的角度來看很重要。

本文摘錄於《基於形式的高效 RISC-V 處理器驗證方法 — 形式化驗證》白皮書，出版人為總部位於歐洲的全球領先 RISC-V 供應商和處理器解決方案領導者，該公司的處理器 IP 目前已部署在數十億顆晶片中。Codasip 通過開放的 RISC-V ISA、Codasip Studio 處理器設計自動化工具與高品質的處理器 IP 相結合，為客戶提供定制計算。這種創新方法能夠輕鬆實現定制和差異化設計，從而開發出高性能的、改變遊戲規則的產品，實現真正意義上的轉型。如希望得到該白皮書的完整版本，可流覽 Codasip 中文網站或者關注該公司微信公衆號。

該技術白皮書英文版下載連結：https://codasip.com/papers/a-formal-based-approach-for-efficient-riscv-processor-verification CTA