經濟部 111 年度

《臺灣資安卓越深耕-半導體及資通訊供應鏈資安關鍵技術發展計畫(2/4)》

合作研究計畫

《硬體木馬偵測與防禦計畫》

建議書徵求文件

財團法人資訊工業策進會

中華民國　111 年 3 月 1 日

111年度合作研究計畫建議書徵求文件

一、 簡介

現今資訊化的時代，物聯網、自駕車與網路通訊等工業技術興起，晶片設計與開發扮演著不可或缺的角色。若是系統中部份晶片出現異常無法正常運作，往往牽一髮而動全身，影響整個系統的正常功能，而造成使用者的巨大損失。例如2007年敘利亞的一座雷達未能有效發起空襲警報，起因為系統晶片被植入後門，導致雷達功能失常；2014年紐約時報揭露美國國家安全局(NSA)在USB埠中植入木馬，使其能夠存取近乎全世界用戶的資料，甚至中國、俄羅斯等國的軍用網路。前述例子皆顯示出硬體晶片在資訊安全領域的重要性，不容疏忽。

硬體特洛伊木馬(hardware Trojan horse)泛指晶片中被惡意植入或修改的電路，只有當特定的邏輯閘達到特定訊號條件時會被觸發(triggered)，並且執行惡意安插的載體(payload)電路。其可能造成晶片資訊洩漏、功能失效或功能改變，更甚是直接損壞等後果。而這些觸發條件平時並不容易達成，只有在特殊操作或事件發生時才會滿足條件而啟動。在正常情況下，硬體木馬不會影響原電路運作，因此並不容易被察覺，晶片仍然會得到預期輸出；且硬體木馬並沒有形式化的型態或特徵，每個硬體木馬都可能是前所未見的型態，這些特性也使得硬體木馬不容易在晶片測試及驗證時被發現。

隨著晶片工業的全球化，晶片設計廠商越來越趨向「無廠」(fabless)化。晶片在設計與製造階段的分工更加細緻與專業，卻也讓晶片在不同階段受到各種潛在的威脅，更加凸顯硬體資訊安全領域中存在的隱憂。在設計階段，加速開發使用的開源資源可能本身就含有木馬，又或是未認證的第三方工具都可能使得元件或參數遭竄改，甚至直接被植入木馬；在製造量產階段，未被信任(untrusted)的製造商頻繁地接觸、合理地取得晶片設計與製造的細節，亦可能使晶片暴露在風險中。在如此充滿威脅的生產環境中，如何能夠在製造前有效率且精準地判別異常的內容，是晶片產業所需面對的一大課題，此技術將能有效增加晶片開發後使用上的安全性。

二、 計畫目標

在硬體木馬領域的研究內容中可根據生產階段主要分為佈局前(pre-layout)、佈局後(post-layout)與製造後(post-manufacturing)三大階段。佈局後與製造後兩個階段有許多偵測硬體木馬的方法，大致可分為電路特徵(circuit feature)分析、光學(optical)分析、旁通道(side channel)分析、邏輯測試(logic testing)等，在實務上往往需要投入大量時間成本，且因標準樣本電路(golden circuit)不易取得與硬體木馬種類及型態複雜，辨識結果不甚理想。另外，缺乏相關製程的標準元件庫(cell library)往往也是在佈局後階段辨識不易的一大主因。使用gate-level netlist做為判斷特徵的同時不一定能取得該電路設計使用的標準元件庫，其中的邏輯閘(logic gate)資訊無法完美匹配，因此用來判別硬體木馬的特徵可能不精確造成準確率的下降。而在另外的應用層面，以開發者的角度而言，就算精準的判別了硬體木馬，也難以在gate-level netlist與晶片上做修正並更改設計來去除問題。為了解決上述各種現象，可以在佈局前階段採取獨立(independent)於製程的硬體木馬偵測方式，解決部分開發上的資訊安全隱憂，把焦點著重於RTL(register-transfer level)的程式碼中。可以發現於佈局前做硬體木馬的異常特徵分析並進而偵測顯得格外重要，不用取得該製成的標準元件庫資訊且得到的資訊可在設計階段作為設計參考，為一個值得探討的議題。

本計畫目標為提出在RTL之硬體木馬偵測的解決方案。調查在RTL之硬體木馬種類並對其特徵進行分析，進而根據需求分析硬體描述語言之語言結構，使用有效的邏輯特徵擷取技術取得高品質的判別條件，並研發演算法對RTL之硬體木馬進行偵測。此外分析演算法之實務應用，在業界情境下根據情境調整精確率(precision)等指標來符合業界使用需求。最終希望能進一步優化偵測性能與耗降低所需時間與運算資源提升實用性。

三、 計畫範圍

本計畫預計研究以下主要項目：

- RTL之硬體木馬威脅模型的分析與討論
- RTL之硬體木馬偵測技術之探討與應用
- 開發RTL之硬體木馬偵測技術
- 提出技術與其他方法之比較分析

四、 預期成果

- 於111年7月31日前交付期中報告1篇。
- 於111年11月30日前交付期末報告1篇，及成果模組1份，並包含原始碼及使用說明。

※前述成果如有專利構想或專利申請產出時，需注意專利申請之新穎性(novelty)。因凡經公開發表之研發成果，如擬申請專利，須於公開發表後 6 個月內完成，前述成果如是以論文方式公開發表，將無法取得大陸與歐盟等國之專利。

五、 執行方式

- 合作計畫執行單位應配合本會計畫需求，隨時對計畫細項作調整。
- 於計畫執行期間，合作計畫執行單位須配合計畫所需，不定期與本單位進行研究心得報告與研討，報告內容以計畫範圍相關之技術主題。

六、 計畫期程及預估計畫總經費

計畫執行區間：111 年 1 月 1 日 至 111 年 12 月 15 日
總經費：700,000元

七、 驗收標準(含教育訓練)

- 依本建議書徵求文件第四點「預期成果」規定，如期繳交相關成果。

八、 技術能力需求

- 具備硬體木馬、硬體安全研究經驗之研究人員。
- 熟悉電路模擬工具並具備實際操作或研究經驗之研究人員。
- 具備演算法開發、機器學習、深度學習實務經驗之研究人員。