行政院國家科學委員會專題研究計畫 成果報告

硬體惡意行為檢測技術研究
研究成果報告(完整版)

計 畫 類 別 ：個別型
計 畫 編 號 ：NSC 100-2623-E-009-007-D
執 行 期 間 ：100 年 01 月 01 日至 100 年 12 月 31 日
執 行 單 位 ：國立交通大學資訊工程學系（所）

計 畫 主 持 人：陳穎平
共 同 主 持 人：許騰尹、范倫達

公 開 資 訊 ：本計畫可公開查詢

中 華 民 國 101 年 03 月 14 日

中 文 摘 要 ： 硬體木馬大部分是被動的監視並延長其運行壽命的週期，直到它們被觸發。硬體木馬特色是隱形，這表示在正常操作下他們會隱密自己的電路，並且不像一般電路一樣可以被控制觀察，若將晶片拆解後分析，這種毀滅性的檢測導致晶片必須被丟棄，並且不能保證其它晶片沒有受到硬體木馬的攻擊。本計畫預計採用旁通道訊號(side-channel signals)可被用來偵測硬體木馬，為屬於 testing-based 方法之一，是以量測旁通道訊號參數(消耗功率、延遲時間等)為基礎，當一個電路被惡意加入硬體木馬時，硬體木馬會使部分參數有明顯的變化，首先我們先量測一個無木馬(Trojan-free)電路的旁通道訊號參數，拿這參數為基準，去跟其他未確認有無木馬之電路旁通道訊號參數相比較，當兩參數無明顯變化則該電路無木馬存在，反之假如兩參數有很明顯的差異時，那麼我們就能確認該電路被人惡意放入木馬。

中文關鍵詞： 硬體安全防護、惡意電路、硬體木馬、旁通道訊號分析

英 文 摘 要 ： Most of the hardware Trojan horse is a passive monitor and extend the operational life cycle until they are triggered. Trojan hidden hardware features, this means that they are hidden under the normal operation of the circuit themselves, and unlike most circuits can be controlled as observed that if after the dismantling of the chip, the detection of this devastating result in the chip must be discarded, and can not guarantee that other chips have not been hardware Trojan horse attacks. This project is expected to adopt side-channel signals (SCS) to detect the hardware Trojans, as belonging to the testing-based methods, based on the measurement next to the channel signal parameters (power consumption, delay time, etc.). When a circuit is a malicious Trojan added hardware, the hardware Trojan causes some significant changes in parameters. In first, we can measure a non-Trojan (Trojan-free) circuit next to the channel signal parameters as a benchmark. If such parameters are significantly different, we can confirm that the circuit have been maliciously into the Trojan.

英文關鍵詞： hardware trojan horse, malicious circuit, hardware security detection, side-channel analysis

行政院國家科學委員會補助專題研究計畫 **■ 成 果 報 告**
□期中進度報告

硬體惡意行為檢測技術研究

計畫類別：■ 個別型計畫　　□ 整合型計畫
計畫編號：NSC-100-2623-E-009-007-D
執行期間：100　年　1　月　1　日至　100　年　12　月　31　日

計畫主持人：陳穎平 副教授
共同主持人：許騰尹 副教授，范倫達 副教授
計畫參與人員：林祐賢、趙冠傑、陳盈良、丁張玉、張家榮、陳柏憲、許凱閔、陳振國

成果報告類型(依經費核定清單規定繳交)：□精簡報告　■完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：國立交通大學 資訊工程系

中　華　民　國　　101　年　3　月　31　日

中文摘要

硬體木馬大部分是被動的監視並延長其運行壽命的週期，直到它們被觸發。硬體木馬特色是隱形，這表示在正常操作下他們會隱密自己的電路，並且不像一般電路一樣可以被控制觀察，若將晶片拆解後分析，這種毀滅性的檢測導致晶片必須被丟棄，並且不能保證其它晶片沒有受到硬體木馬的攻擊。本計畫預計採用旁通道訊號(side-channel signals)可被用來偵測硬體木馬，為屬於testing-based 方法之一，是以量測旁通道訊號參數(消耗功率、延遲時間等)為基礎，當一個電路被惡意加入硬體木馬時，硬體木馬會使部分參數有明顯的變化，首先我們先量測一個無木馬(Trojan-free)電路的旁通道訊號參數，拿這參數為基準，去跟其他未確認有無木馬之電路旁通道訊號參數相比較，當兩參數無明顯變化則該電路無木馬存在，反之假如兩參數有很明顯的差異時，那麼我們就能確認該電路被人惡意放入木馬。

關鍵詞：硬體安全防護、惡意電路、硬體木馬、旁通道訊號分析

Abstract

Most of the hardware Trojan horse is a passive monitor and extend the operational life cycle until they are triggered. Trojan hidden hardware features, this means that they are hidden under the normal operation of the circuit themselves, and unlike most circuits can be controlled as observed that if after the dismantling of the chip, the detection of this devastating result in the chip must be discarded, and can not guarantee that other chips have not been hardware Trojan horse attacks. This project is expected to adopt side-channel signals (SCS) to detect the hardware Trojans, as belonging to the testing-based methods, based on the measurement next to the channel signal parameters (power consumption, delay time, etc.). When a circuit is a malicious Trojan added hardware, the hardware Trojan causes some significant changes in parameters. In first, we can measure a non-Trojan (Trojan-free) circuit next to the channel signal parameters as a benchmark. If such parameters are significantly different, we can confirm that the circuit have been maliciously into the Trojan.

Keyword: ***hardware trojan horse, malicious circuit, hardware security detection, side-channel analysis***

目錄

1. 前言

近年來，積體電路(IC)設計越來越複雜化，為了使產品研發能更經濟、更快速，使得以往半導體產業的單一工廠整合元件模式，轉換為由 IC 設計公司、晶圓代工廠、封裝廠與系統整合商等全球化專業分工趨勢(圖 1) 降低製造成本，一顆 IC 就可能由全球各地不同公司團隊的工作結晶，現代 IC 內部皆會劃分為不同區塊，每個區塊負責處理不同功能，設計公司藉由取得擅長設計某些功能的第三方硬體矽智財(Intellectual Property)的授權，以解決和減緩設計生產率上的成本，但也產生新的問題，沒有 IC 設計公司不能夠完全明白 IC 內部的電路結構，無從確定各區塊內部是否是乾淨的，使得安全方面的議題浮出檯面，同樣外包的製造過程中也可能發生了安全性和完整性的問題，若 IC 在設計或製造的過程中受到故意微妙的改建或改變電路，這些改變在某些罕見和關鍵的觸發下使其工作與預期的結果有差異，可能導致該項電路的效能降低、改變功能甚至洩漏資訊等，而我們稱此被改建或改變的區域電路為惡意電路(malicious circuit)或硬體木馬(Hardware Trojan)。

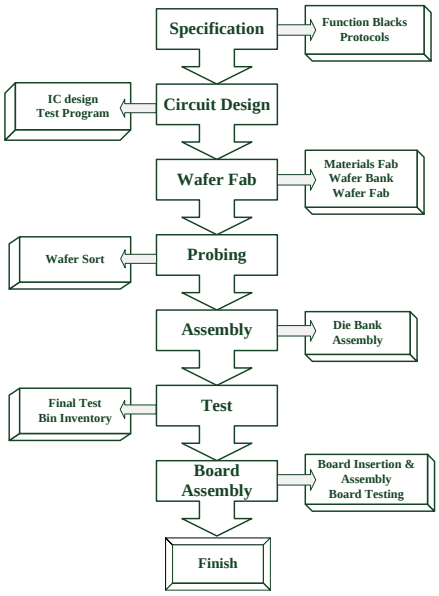


圖1. IC製造分工流程

此安全性問題擴及幾乎所有電子產品，金融基礎設施、運輸安全設施、通訊設備甚至可能威脅到軍事系統，美國國防部[1]及澳大利亞國防科技組織(DSTO)[2]皆有提出相關報告，雖然目前未發生IC被植入硬體木馬的硬體攻擊之實際案例，但在行動多媒體裝置在出產時有極少數夾帶電腦病毒，以及發生硬碟在外包生產過程中感染了軟體型硬體木馬，也顯示在IC設計製造的產業鏈中被嵌入惡意電路的可能性是不可被忽視的。且硬體木馬是實體上造成的損害，所以跟以前的軟體型病毒相比會更難處理，必須將有問題的硬體電路完全關閉或進行硬體更換以外沒有其他的解決方式。

於第二章將介紹硬體木馬的分類方式與偵測方法，第三章是此篇所使用的旁通道訊號分析技術與實作硬體木馬之研究方式，第四章為產出的模擬結果，最末章結論探討整個研究成果。

2. 硬體木馬之相關簡介

2.1 硬體木馬分類

在這個節列出不同硬體木馬的分類架構，了解木馬電路的行為，先得了解其種類，因此先參考國內外研究情形將諸種型態與攻擊模式予以分類。

Yun 等人在 2010 年提出被攻擊後的影響(Payload)和觸發條件(Trigger)的分類架構[3]，其中觸發部分如圖 2 所示。電路被攻擊者植入木馬後，在特定條件觸發後將會對電路造成影響，稱之為攻擊效果(Payload)。根據攻擊者目的會造成不同的效果。主要為以下三種: **(1)洩露機密資訊**：通常都是較敏感的訊息，如未加密過的私人資料；**(2)更改電路功能**：讓電路功能違反原本的設定，輸出非預期中的結果；**(3)毀壞晶片**：使其癱瘓停止運行。這些攻擊會在特定條件被觸發(Trigger)，又可分成觸發途徑(Accessibility)、觸發位置(Location)、觸發媒介(Medium)。 攻擊者若把硬體木馬植入於易被偵測的區域中，很容易硬體木馬運作前被發現且丟棄，因此攻擊者必會將硬體木馬植入在較難偵測的路徑。如在電路中較少出現的輸出(output)去觸發硬體木馬，抑或是特定計數器(dedicated counter)計數到特定值而觸發等的罕見條件。另一種可能是硬體木馬一直保持運作的狀態，對電路運作功能不造成影響，但卻耗損電路壽命。

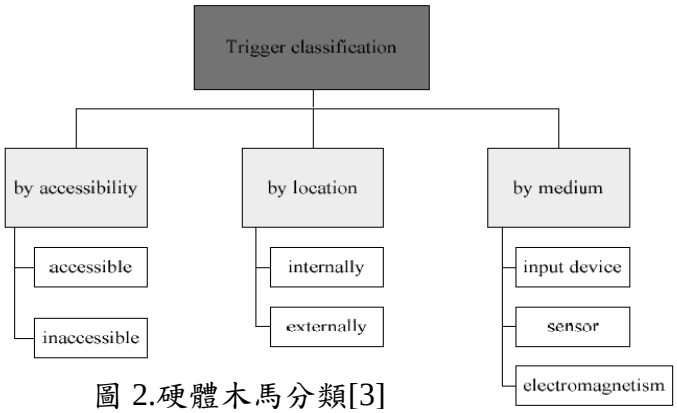


圖 2.硬體木馬分類[3]

於[4]中 Wang 等人提出依照(1)實體情況(Physical)、(2)活化方式(Activation)、(3)行為模式(Action)三層面之分類架構，其分類架構如圖 **3** 所示。

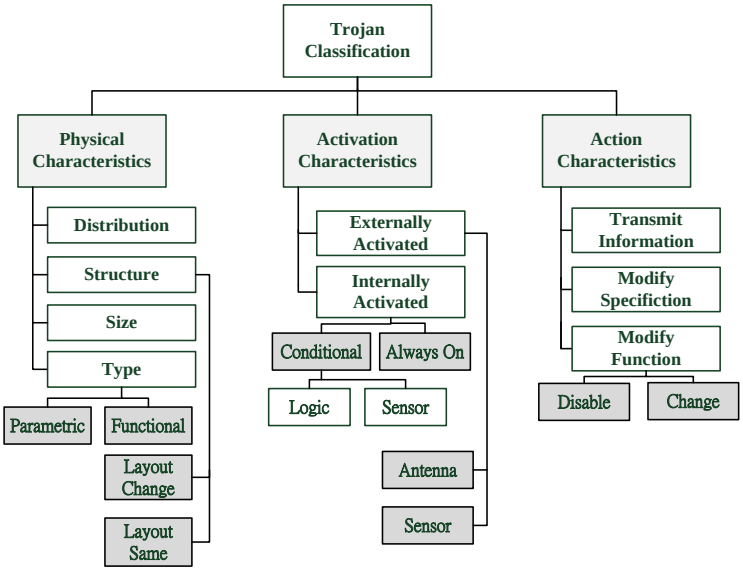


圖3.硬體木馬分類架構[4]

(1) **實體情況(Physical)**：型態(Type)分為功能或參數兩種型態。功能類型態包括硬體木馬物理實現，通過添加或刪除電晶體或邏輯閘，而參數是指不變動電路架構下修改電路線路參數或電晶體規格的方式放入硬體木馬。尺寸大小(Size)：在觸發的中硬體木馬大小是一個重要因素，多個輸入的小型硬體木馬的觸發率較單個大型硬體木馬的觸發率高。分佈(Distribution)：硬體木馬在晶片的分佈位置。例如，若晶片的佈局是鬆散的，硬體木馬便可在可用性的死角上佈局。若非常小的死角都可以佈局的話並假設攻擊者沒有改變晶片的小大為前提，攻擊者就可能會將較小的部份線路分佈在木馬的周圍。結構(Structure)：如果是重新佈局才能夠植入木馬，則會改變晶片的大小。這種變化可能會影響到不同元件或所有設計元件，任何晶片的物理佈局，其變化可以改變延遲和電力特性使其更容易偵測到木馬。

(2) **活化方式(Activation)**：潛藏在電路中的硬體木馬可能執行異常的行為，然而非全部的硬體木馬都處於運作狀態，若未啟動的硬體木馬在特定時間被觸發而運作，這類硬體木馬又稱為時間炸彈。時間炸彈被觸發的條件就稱為活化方式的行為。將體木馬觸發的分類為兩種，外部觸發(Externally activated)和內部觸發(Internally activated) ，內部觸發又分為兩類，一是硬體木馬始終是活動的，另一內部觸發的情形是一開始處於休眠狀態，直到特定條件得到滿足立即觸發木馬。

(3) **行為模式(Action)**：硬體木馬被植入電路之後，依照對整個電路的影響來分類，例如對某些功能造成影響，讓其產生非預期的輸出而傳遞下去，使整個電路失效，修改功能(Modify-function)、修改規格(Modify specification)、傳輸信息(Transmit info)。

於[5] Karri 等人提出除了在製程階段中可能會被植入硬體木馬種類、方式為基準，探討各硬體木馬會對電路造成合種影響，其分類如圖 4 所示:

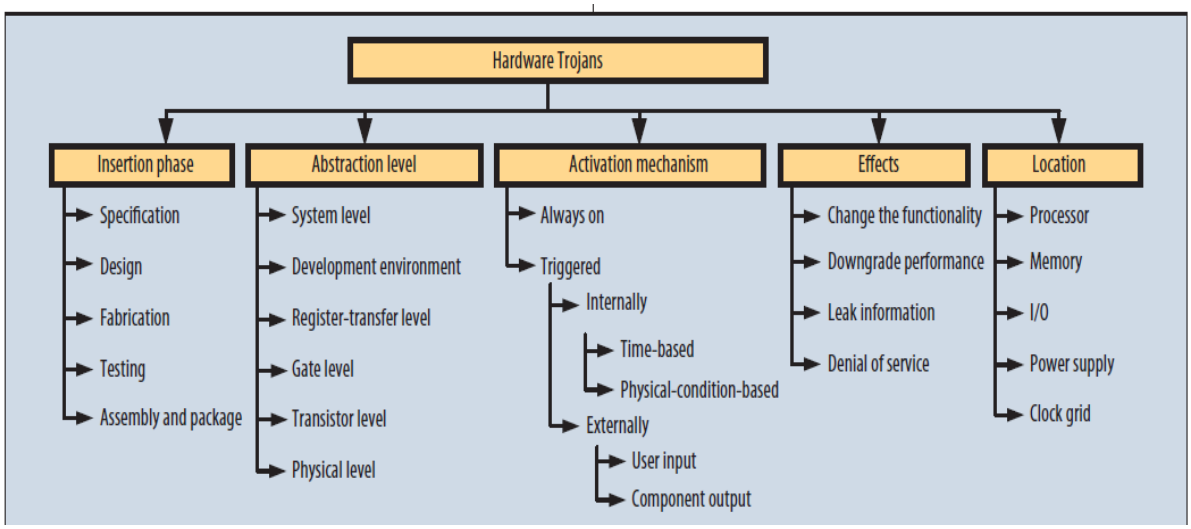


圖 4. Karri 硬體木馬分類架構[5]

(1) 植入區域(Insertion phase)：在一般 IC 設計的流程中，可能硬體木馬會在其中被植入，譬如說在設計層面(Design)的過程使用第三方的矽智財來執行功能單元，然而硬體木馬可能就是早已被植入在某些矽智財中，而達到攻擊的目的，該架構將此分為規格制定、設計、製造、測試以及封裝五個階段。

(2) 抽象層面(Abstraction level)：在此層面是最容易被修改的部分，只要攻擊者使用參數型(Parametric)或功能型(Functional)的改變，就可以造成一定程度的影響，例如暫存器轉換階層(Register transfer level)，設計開發者用暫存器、訊號和布林函數來表示功能單元，攻擊

者只要修改程式碼，就可以達到讓電路不正常運作的目的。細分為 a.系統層級 b. 暫存器轉換階層 c. 邏輯閘階層 d. 電晶體階層 e. 佈局層面

(3) 觸發層面(Activation mechanism)：少部分硬體木馬的設計是永遠處於執行狀態中，而其他的設計在一開始會處於休眠狀態，當硬體木馬被觸發後才開始有執行運作。一般來說，觸發有分成內部跟外部觸發兩種，內部觸發可能是經由時間或是物理上的特性來作為其觸發條件。另一方面外部觸發通常是由攻擊者或周邊設備輸入特定指令後，觸發硬體木馬，由攻擊者觸發方式如使用開關或鍵盤輸入特定字串讓硬體木馬發動，周邊設備的觸發方式是該設備的輸出透過 RS232 或其他傳輸方式連接至存在硬體木馬之裝置啟動硬體木馬。

(4) 影響層面(Effects)：這個分類分為四大項: a.改變設備的功能 b.改變規格 c.洩漏敏感的信息以及 d.拒絕服務。硬體木馬的影響輕則是造成非預期輸出，重者會危害整個系統的運作。洩露資訊就是一項相當重要的議題，可能外洩客戶資料或國家情報給攻擊者。

(4) 植入位置(Location)：硬體木馬可能潛在一個或多個元件中，處理器、記憶體、輸入/輸出端等等。若硬體木馬分佈在多個元件中，這些硬體木馬可能是獨立或集體運作而完成攻擊的任務。

在[6]-[9]中，也提出了類似的分類方法，綜合近幾年的研究，硬體木馬的分類主要以[5]為主流依照觸發條件與電路受影響之情況的架構去進行硬體木馬之相關研究。

2.2 硬體木馬偵測法

本節簡介幾種常見的硬體惡意行為檢測方法，。遍將硬體惡意行為檢測方法概分為下列三種：

1. **物理檢查(Physical Inspection) 和**
   逆向工程(Engineering Extremely)[4][10]

物理性質的分析技巧，是指使用儀器去測試晶片，然後分析收集來的資料去確認正確性。此類的分析儀器有很多種，例如掃描式光學顯微鏡(scanning optical microscopy (SOM))、掃描式電子顯微鏡(scanning electron microscopy (SEM))、微微秒成像電路分析(pico-second imaging circuit analysis (PICA))、電壓比對成像(voltage contrast imaging (VCI))、光束誘發電壓調變(light-induced voltage alternation (LIVA))、施感電壓調變(charge-induced voltage alternation (CIVA))等。在硬體木馬的攻擊中，通常攻擊者會將木馬隨機的植入晶片，所以每一片晶片都需要驗證，使用以上這些方法雖然可以百分之百的達到硬體惡意行為檢測的目的，但同時這些方法會耗費大量的時間及金錢成本，除此之外，這些方法還需要晶片背面薄化及反製程操作，會造成晶片本身無法還原之傷害。且另一個很重要的缺點是在奈米領域中，由於晶片尺寸的縮小，有些技巧逐漸失去效用。

2. **功能測試(Functional Testing)**

(1) ATPG 木馬檢測技術(ATPG-based Trojan Detection Techniques) [11]

ATPG 檢測技巧是使用標準超大型積體電路(VLSI)除錯檢測工具，自動測試樣本產生工具(automatic test pattern generation (ATPG))來檢測晶片的正確性。此種方法主要是給予晶片或模型一組數位測試向量，檢查其輸出資料來達到硬體惡意行為的檢測。因為詳盡的測試非常耗時，大型 IC 的木馬觸發機率很低且需要龐大的連續測資時間。

(2) 內建自我測試電路檢測技術(Built-In-Self-Test Techniques)[12][13][14]

在單晶片測試結構，即內建自我測試技術是在原先晶片中加上其他的功能電路，該電路設計用來監控訊號和發現晶片缺陷並減少測試時間的方式，其可用於製成變異檢測，也同樣可用於檢測惡意的邏輯電路。首先利用該技術於可信賴晶片使其產生特定檢測數值(familiar signature)，與未檢測晶片之數值相比以顯示缺陷或改變。該方法的優點在於，在這系統下擁有很強大的監視功能邏輯，並且可重新編譯監控邏輯，此外也是屬於非破壞性的硬體木馬防護方式，且可檢測參數型以及功能型木馬。但是這項方法更加的昂貴且複雜，另外在晶片設計上得花上更多的時間。

3. **旁通道訊號分析技巧**(Side Channel Signals Analysis)[4][10][11]

此研究採用旁通道訊號(side-channel signals)分析技術偵測硬體木馬，屬於testing-based方法，以量測旁通道訊號參數(消耗功率、延遲時間等)為基礎，當一個電路被惡意加入硬體木馬時，硬體木馬會使參數產生些許變化，即使只在電路中植入一個邏輯閘一般常用參數包含:漏電流增大、動態功率消耗加劇和節點間的延遲時間的增加，甚至是電路的運作時的溫度分布。第一步量測一個無木馬(Trojan-free)電路的旁通道訊號參數，拿這參數為基準，去跟其他未確認有無木馬之電路旁通道訊號參數相比較，當兩參數無明顯變化則該電路無木馬存在，反之假如兩參數有很明顯的差異時，簡單來說這項檢測策略是針對參數是否異常來判斷該電路是否被人惡意放入硬體木馬的可能性。使用此分析法大致為底下步驟：

(1) 隨機選擇部分同一系列IC(使用同一遮罩及晶圓廠)。
(2) 對這些IC執行夠多的I/O測試，並且在測試時對一或多種旁通道訊號收集夠多的資訊。
(3) 利用這些資訊去分析訊號的特徵表現。
(4) 確認被挑選出IC未被加入惡意電路。
(5) 在第一步驟未被挑選的IC，經由同樣的I/O測試取得旁通道訊號，在與第三步驟的結果相互比較，確認是否有硬體木馬入侵。

以旁通道分析為基礎的方法，其優點在於分析法比其他分析法需要較少的硬體開銷，且在測量訊號參數時假如木馬處於未觸發狀態，也能使用旁通道分析木馬的存在，因為被惡意加入硬體木馬會額外增加電路，而這些額外電路也會使得部分相關參數產生改變，且比對兩筆參數差異能迅速判斷木馬是否存在於電路，但是分析旁通道訊號來檢測硬體木馬，還是有它缺點存在，最大問題是此分析法需要一個已確認無木馬存在的電路，該電路所量測出的參數才可以當作基準，除非有原始設計模型可供模擬或必要時使用逆向工程還原電路，另外近年來製程技術發展迅速原件尺寸越做越小時製程飄移(process variation)的因素，以及量測時所出現的雜訊(noise)或者是量測儀器的環境因素都可能蓋過一個硬體木馬(特別是小型木馬)對訊號參數的影響。

3. 研究方法

此研究如何偵測硬體木馬之方法，是採用旁通道訊號分析模式來進行模擬無硬體木馬之電路與有硬體木馬存在之電路中，檢測統計其旁通道訊號之變化差異(如圖5.)。其中較常使用之旁通道訊號可分為是基於電力特性(power-based)或時間特性(timing-based)之訊號兩種。

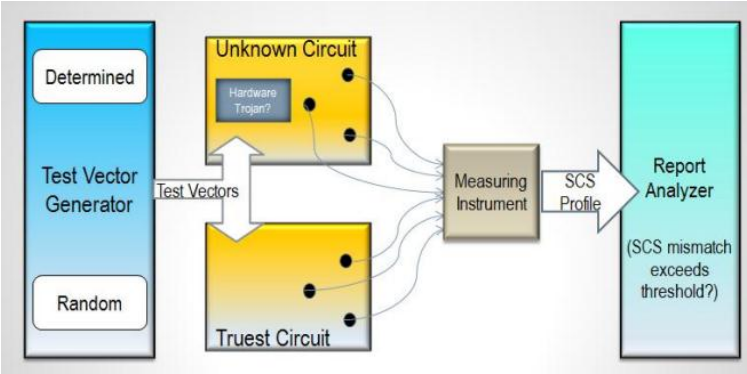


圖 5.檢測流程

3.1 時間特性分析

本研究實驗目標是量測分析路徑延遲時間此為時間特性旁通道訊號，此方法的關鍵點在於輸入測資必須盡量涵蓋整個電路，進行方式是同時對安全電路與未檢測電路施予相同測資並量測輸出訊號，比對輸出訊號之延遲時間之差異是否是在可接受的變化範圍(考慮製程飄移因素)，藉此判斷未檢測電路存在硬體木馬的可能性。

$$D = \Sigma d_i \qquad (1)$$

$$\Delta D = D_2 - D_1 \qquad (2)$$

D 為各階延遲時間d_i的總和。安全電路的延遲時間總和為D_1，未檢測電路的延遲總和為D_2，ΔD為兩者的差異，由該值的數值大小是否合理，判斷未檢測電路是否遭受到惡意攻擊。

3.2 實作惡意行為電路

DES3模組與硬體木馬植入：DES/DES3(Data Encryption Standard)：是一個加解密電路，加解密電路最注重的就是資料的安全性，且要加密的資料一定有一定程度的重要性，所以攻擊者要針對這個IP攻擊就可以針對未加密的資料竊取。

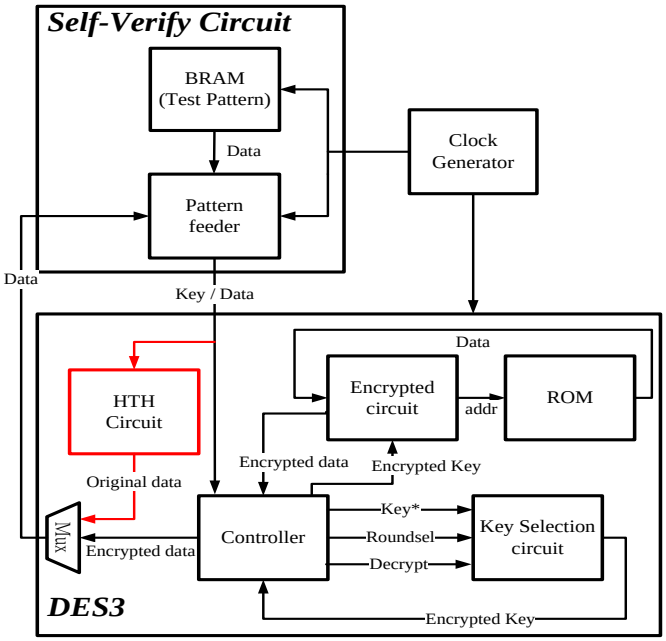


圖 6.DES3 模組與硬體木馬植入架構

在 DES3 模組架構中有兩個部分，第一個部分是 Self-Verify Circuit、第二個部分是 DES3，在第一部份中自我驗證的電路是設計將所要加解密資料和所選擇的金鑰送進 DES3 中，為了驗證方便，Pattern feeder 會先跟 BRAM 拿取測試檔案不停的送資料進去加解密，才好偵測運作過程中是否有硬體木馬的威脅，在這邊使用 BRAM 是為了將所有的資料都能在最後的步驟中燒入至 FPGA 版上，來執行自我偵測的步驟。

第二部分是 DES3 IP，共有 Key selection circuit、Encrypted circuit、ROM、Controller module，Key selection circuit 是將所獲得的 key 選擇如何使用來加密，DES3 是採用 3 個 key 作為加密金鑰，3 個金鑰的組合可能為全相同、兩同一異或全相異，而選擇哪一種方是就是由 Key selection circuit 所決定。Encrypted circuit 就是將選擇後的金鑰來跟 ROM 拿資料來加密送回到 controller，最後在由 controller 送出資料回 pattern feeder 驗證。 紅色區塊為硬體木馬電路的設計，在這邊設計的硬體木馬是要將 pattern feeder 送出的的資料竊取出來，但不影響整個 DES3 的運作，在 DES3 閒置的時候再將竊取的資料秘密地輸出。

目前採用 Virtex-5 ml507 當作開發平台，下圖是正在使用的 FPGA：

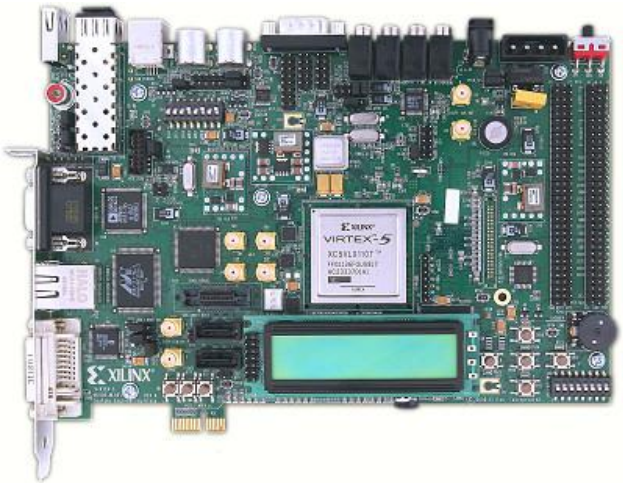


圖 7 Virtex-5 ml507

在開發平台確認後,使用 Xilinx ISE Design Suite 上模擬 IP 的行為是否正常,透過 nWave 來清楚看到模擬波型來驗證正確性，以下是 ISE 驗證整個 IP 的流程：

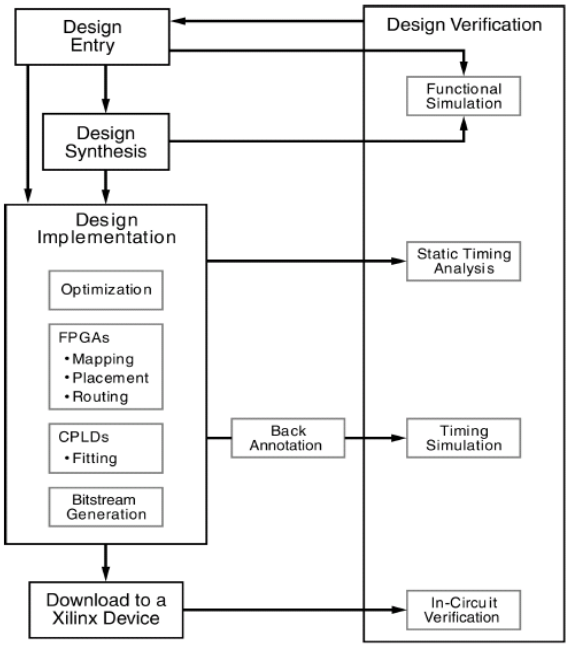


圖 8 ISE 設計流程

第一個步驟是將 Design Entry 拿去 Functional Simulation 執行原本設計的模擬，確認程式的正確性，在執行 Design Synthesis，也就做合成的動作，產生 netlist 再餵給 Design Implementation 去對應到整個 FPGA 實際的內容,在 Design Implementation 中先做一些最佳化後，會執行三個大動作，就是 Mapping、Placement、Routing，Mapping 的過程就是將一開始產生的 netlist 對應到 FPGA 上的真正的 slice 和一些特徵元件,Placement 根據你的 PCF 檔(設定一些原件限制的檔案)放到 FPGA 上,最後在 Routing 將 timing constrains 考量進去，在將過程拿到 Timing Simulation 做確認正確性，再產生 Bitstream 燒入至 FPGA 上。

在整個模擬完 IP 且燒入至 FPGA 上後，使用 Xilinx ChipScope 來監測燒入至 FPGA 上後的運作是否正做，符不符合當初的要求，ChipScope 的概念大致如下圖：

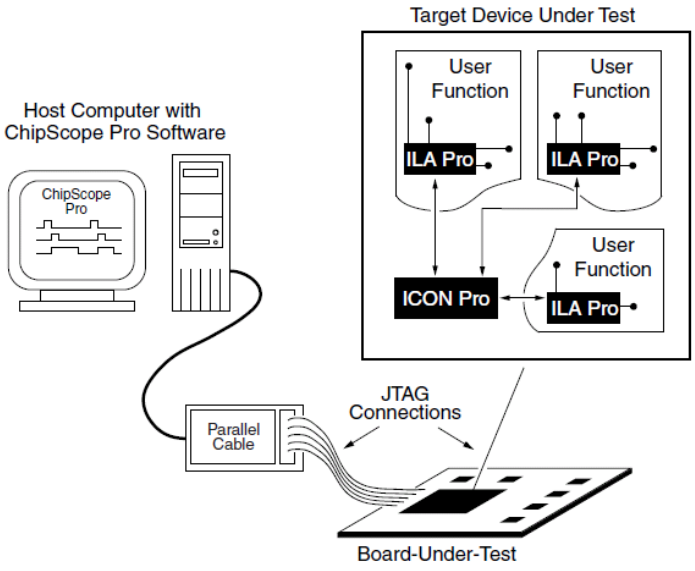


圖 9 Xilinx ChipScope 驗證流程

很清楚的可以看的FPGA經由JTAG傳回信號給PC端監測，觀察波型是否放至到FPGA上還是正確的。

FPGA設計的流程大致如上所描述，我們將會把原本使用的IP(沒有木馬的)先量測好他的數據，在將硬體木馬植入到IP中燒入至FPGA上，量測另一組數據來了解實際上的差別，可能會有Power、hardware overhead、area等等可比較的數據。

4. 研究成果

4.1 時間特性分析成果

本研究之模擬採用ISCAS-85 c432 27通道[16](c432約為160 gate count，參考圖10.)之中斷控制器電路來當做待測標準電路，並在此電路之通道編碼(電路編號out432)前插入硬體木馬電路來模擬硬體木馬電路，我們於TSMC之65nm製程下，分別於0℃、20℃、40℃、60℃和80℃的情況測試其插入電路後與原電路之延遲，而其中所使用的硬體木馬電路分為三種，分別使用二個(木馬一)、十個(木馬二)與二十(木馬三)個反向器所組成，木馬分別約為1、5、10 gate count，硬體木馬各佔總電路面積的0.6%、3%與5.9%，並且使用不同級數之反向器來做比較，依照不同溫度條件模擬其路徑延遲時間，其模擬結果分別顯示在圖11(a)~(e)。

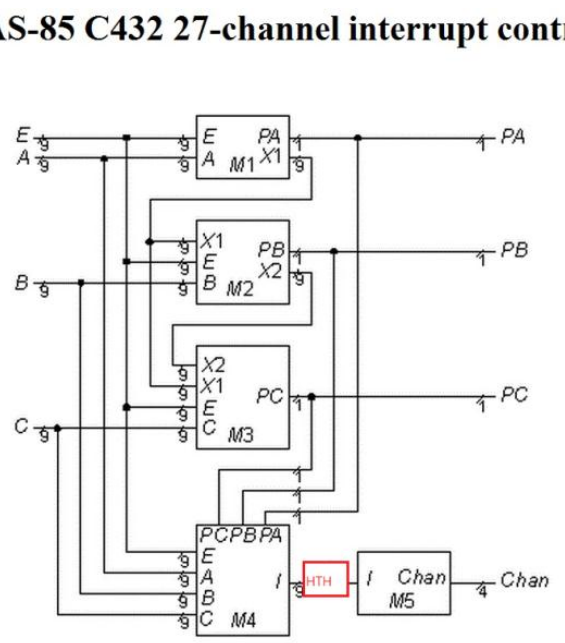


圖 10.ISCAS-85 C432 with Hardware trojan

圖11(a)~(e)波形圖為c432之輸出訊號(4bits分別命名標號421、430、431、432)中標號431輸出波形線，其431訊號線由左至右分別為原始c432電路、c432含木馬一電路、c432含木馬二電路、c432含木馬三電路。圖7(a)~(e)溫度分別為0℃、20℃、40℃、60℃與80℃。

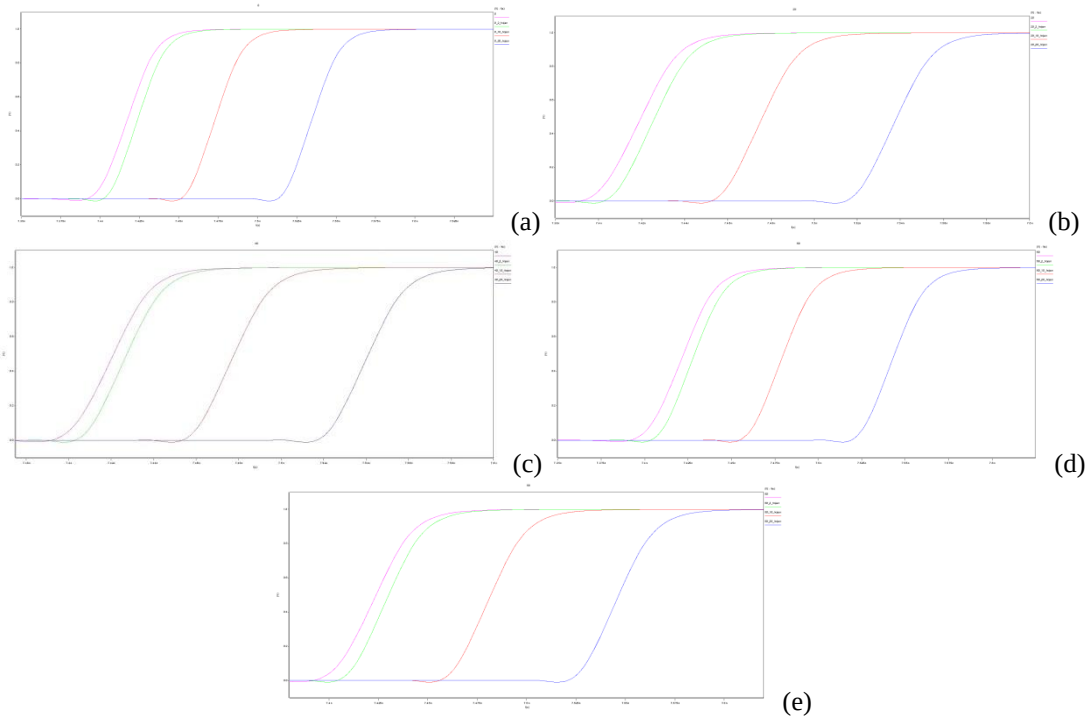


圖 11.路徑延遲波形圖(a-e 各波形由左至右分別為原始電路、含木馬一電路、含木馬二電路、含木馬三電路)

於0℃時增加的路徑延遲時間分別為

木馬一：6.4ps、木馬二：55.6ps、木馬三：117.2ps。

於20℃時增加的路徑延遲時間分別為

木馬一：6.4ps、木馬二：56.2ps、木馬三：118.6ps。

於40℃時增加的路徑延遲時間分別為

木馬一：6.3ps、木馬二：56.8ps、木馬三：120.0ps。

於60℃時增加的路徑延遲時間分別為

木馬一：6.3ps、木馬二：57.5ps、木馬三：121.5ps。

於80℃時增加的路徑延遲時間分別為

木馬一：6.3ps、木馬二：58.1ps、木馬三：122.9ps。

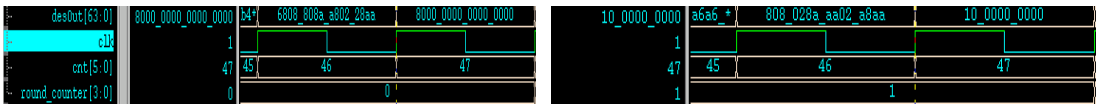
這其中我們可以發現被插入一硬體木馬後，我們可以發現其輸出延遲已經造成ps，我們可以借由此延遲來偵測出硬體木馬之存在可能性。另外我們也可以在此模擬硬體木馬側錄出中斷通道之編碼訊號，進而得知中斷會發給那一個通道，並且竄改訊號，造成硬體之功能運作出錯。

4.2 實作惡意行為電路成果

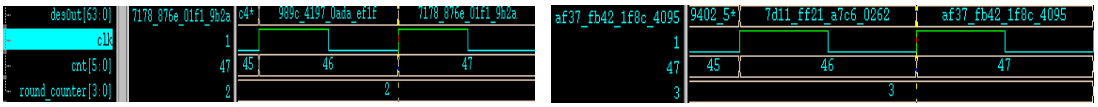
目前已經成功的植入硬體木馬在 DES3 上，以下是實作的成果：

- IP testing：
- Decrypt data：

1. 8000000000000000
2. 0000001000000000
3. 7178876E01F19B2A
4. AF37FB421F8C4095
5. 3D124FE2198BA318
6. FBABA1FF9D05E9B1
7. 18d748e563620572
8. C07d2a0fa566fa30
9. E6e6dd5b7e722974
10. e1ef62c332fe825b

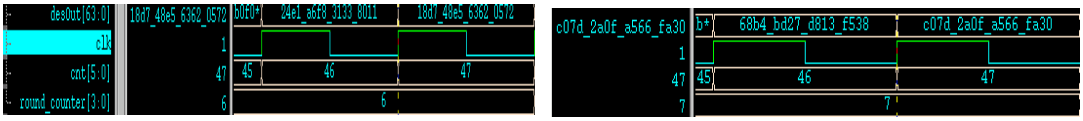


(a)Decrypt data 1　　(b)Decrypt data 2

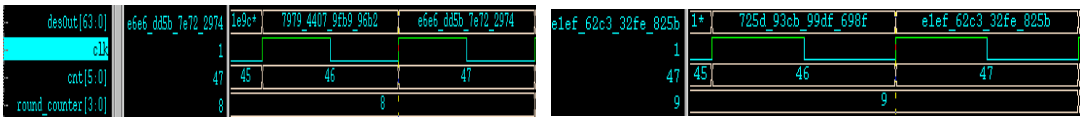


(c)Decrypt data 3　　(d)Decrypt data 4

(e)Decrypt data 5　　(f)Decrypt data 6



(g)Decrypt data 7　　(h)Decrypt data 8

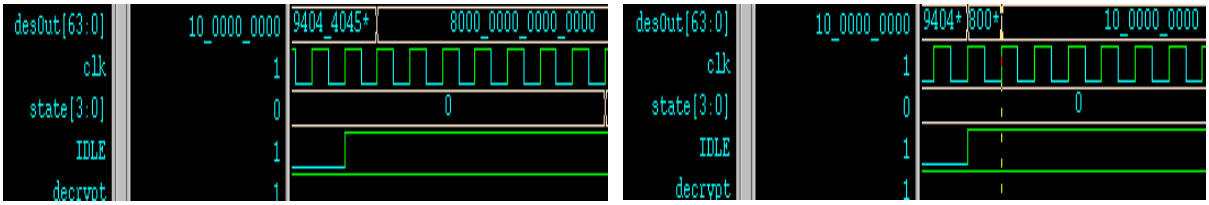


(i)Decrypt data 9　　(j)Decrypt data 10

圖 11 解密後資料

在圖 11(a)~(j)所示的是經過解密後的資料，在接下來的硬體木馬設計中會將其秘密地洩漏出來。

硬體木馬電路的設計(參考圖 6)，在這邊設計的硬體木馬是要將 pattern feeder 送出的解密後的資料竊取出來，在 DES3 controller 的狀態機轉換為 IDLE 時將解密資料洩漏出來，以下是兩個實際的範例，在加密完後(decrypt 為 0 表示為解密中，1 表示為加密中)改變狀態為 IDLE 時(0 表示 IDLE)將 desOut 把解密後的資料洩露出來，也就是說在電路加密的時候，就先把加密的資料竊取出來。



(1)硬體木馬竊取資料範例 1　　(2)硬體木馬竊取資料範例 2

圖 12 硬體木馬竊取資料範例

以上兩個圖是正在加密的過程中，每加密完一筆資料後會controller會IDLE準備下一筆資料的加密，在IDLE中原本輸出是不做任何事情的，但如圖所示在這邊卻輸出8000000000000000和0000001000000000兩筆資料(可以參考decrtpt data是未加密前兩筆資料)，這兩筆資料是沒有加密過的資料但DES3正在運作的是加密過程，這是相當異常的行為。

5. 結論

在今年度的研究議題上，主要分為旁通道訊號分析與設計硬體木馬。在旁通道訊號分析操作過程中，使用 ISCAS'85 C432 為原始電路，利用不同大小之延遲電路為木馬電路，由模擬結果可以得知量測旁通道訊號，並比對原始電路以及含木馬電路其旁通道訊號數值參數表徵，用以判斷硬體木馬存在可能性具有一定的可靠度，但但如果考慮製程飄移所產生的誤差，含木馬一之 c432 電路所產生的波形圖與原始 c432 電路之波形圖相近，容易發生錯誤判斷，所以目前偵測方式僅適用於原始電路屬於小電路，且使用該方式有種種因素需要克服，例如惡意電路植入位置、原始電路或惡意電路之大小與是否能取得原始電路編碼，後續研究將採取在原始電路中加入內建訊號，將大型電路劃分不同區域進行硬體惡意行為檢測。於惡意電路實作部分，已成功針對 DES 作出可竊取其資訊之硬體木馬，接著將持續進行影響功能單元之硬體木馬設計架構降低執行效能之硬體木馬設計架構的研究，並繼續收尋設計硬體木馬的案例，將可以拿來作為測試的對象。

此計畫為國防科技學術合作計畫，校方繳交下列產出給中山科學研究院

- 報告產出

  1. 惡意電路檢測技術蒐集與研析報告

  2.Power-based訊號分析報告

  3.Timing-based訊號分析報告

  4.旁通道訊號分析演算法之效能評估報告

  5.硬體木馬電路案例蒐集與研析報告

  6.設計硬體木馬電路報告

  7.硬體木馬偵測雛型規劃報告

- 相關程式碼

  針對DES之惡意電路設計流程相關程式碼

  路徑延遲旁通道訊號分析相關程式碼

6.參考文獻

[1] Defense Science Board, “DSB Task Force on High Performance Microchip Supply” , 2005.

[2] Beaumont, M.; Hopkins, B.; Newby, T., “Hardware Trojans - Prevention, Detection, Countermeasures (A Literature Review)”, 2011

[3] Song Yun, Qingbao Li, Hongbo Gao, Zhang Ping, "Towards Hardware Trojan：Problem analysis andTrojan Simulation " Information Engineering and Computer Science (ICIECS), 2010 2nd International Conference on , vol., no., pp.1-4, 25-26 DEC. 2010

[4] X. Wang; M. Tehranipoor; F. Koushanfar; , " Detecting malicious inclusions in secure hardware: Challenges and solutions" Hardware-Oriented Security and Trust, IEEE2008. HOST 2008. IEEE International Workshop on , pp.15, 9-9 June 2008

[5] R. Karri; J. Rajendran; K. Rosenfeld; M. Tehranipoor; , "Trustworthy Hardware: Identifying and Classifying Hardware Trojans," Computer , vol.43, no.10, pp.39-46, Oct. 2010

[6] R.S. Chakraborty; S. Narasimhan; S. Bhunia; , "Hardware Trojan: Threats and emerging solutions," High Level Design Validation and Test Workshop, 2009. HLDVT 2009. IEEE International , vol., no., pp.166-171, 4-6 Nov. 2009

[7] Y. Jin; N. Kupp; Y. Makris; , "Experiences in Hardware Trojan design and implementation,"

Hardware-Oriented Security and Trust, 2009. HOST '09. IEEE International Workshop on , vol., no., pp.50-57, 27-27 July 2009

[8] R.M. Rad; Xiaoxiao Wang; M. Tehranipoor; J. Plusquellic; , "Power supply signal calibration techniques for improving detection resolution to hardware Trojans," Computer-Aided Design, 2008. ICCAD 2008. IEEE/ACM International Conference on , vol., no., pp.632-639, 10-13 Nov. 2008

[9] J. Rajendran; E. Gavas; J. Jimenez; V. Padman; R. Karri; , "Towards a comprehensive and systematic classification of hardware Trojans," Circuits and Systems (ISCAS), Proceedings of 2010 IEEE International Symposium on

[10] Y. Alkabani and F. Koushanfar, "Extended Abstract: Designer's Hardware Trojan Horse,"in Proc. Hardware-Oriented Security and Trust 2008 (HOST' 08), pp. 82-83, 2008.

[11] M. Tehranipoor, F. Koushanfar. "A Survey of Hardware Trojan Taxonomy and Detection." IEEE Design and Test of Computers, Vol. 27, No. 1, 2010, pp. 10-25.

[12] C. Fagot, O. Gascuel, P. Girard and C. Landrault; On Calculating Efficient LFSR Seeds for Built-In Self Test, Proc. Of European Test Wkshop, pp 7-14, 1999.

[13] G. Hetherington, T. Fryars, N. Tamarapalli, M. Kassab, A. Hassan and J. Rajski; Logic BIST for large industrial designs: real issues and case studies, ITC, pp. 358-367, 1999.

[14] W. T. Cheng, M. Sharma, T. Rinderknecht and C. Hill; Signature Based Diagnosis for Logic BIST, ITC 2006, pp. 1 – 9, Oct. 2006.

[15] Ors, S.B. et al., "Power-Analysis Attack on an ASIC AES implementation", in Information Technology: Coding and Computing, 2004.

[16] http://www.eecs.umich.edu/~jhayes/iscas/

[17] ChipScope Pro 13.1Software and Cores user guide

[18] PlanAhead User Guide

[19] ISE Command Line Tools User Guide

[20] Virtex 5 FPGA User Guide

[21] Virtex 5 Constraints Guide

[22] Vittex 5 Libraries Guide

國科會補助計畫衍生研發成果推廣資料表

日期:2012/03/14

國科會補助計畫	計畫名稱: 硬體惡意行為檢測技術研究
	計畫主持人: 陳穎平
	計畫編號: 100-2623-E-009-007-D　　學門領域: 電子與資訊系統

無研發成果推廣資料

100 年度專題研究計畫研究成果彙整表

計畫主持人：陳穎平	計畫編號：100-2623-E-009-007-D
計畫名稱：硬體惡意行為檢測技術研究	

成果項目			量化			單位	備註（質化說明：如數個計畫共同成果、成果列為該期刊之封面故事...等）
			實際已達成數（被接受或已發表）	預期總達成數(含實際已達成數)	本計畫實際貢獻百分比		
國內	論文著作	期刊論文	0	0	100%	篇	
		研究報告/技術報告	0	0	100%		
		研討會論文	1	1	100%		100 年度(中科院及三軍)「國防科技學術合作計畫成果發表會」
		專書	0	0	100%		
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（本國籍）	碩士生	3	3	100%	人次	
		博士生	2	2	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		
國外	論文著作	期刊論文	0	0	100%	篇	
		研究報告/技術報告	0	0	100%		
		研討會論文	0	0	100%		
		專書	0	0	100%	章/本	
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（外國籍）	碩士生	0	0	100%	人次	
		博士生	0	0	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		

其他成果 (無法以量化表達之成果如辦理學術活動、獲得獎項、重要國際合作、研究成果國際影響力及其他協助產業技術發展之具體效益事項等，請以文字敘述填列。)	

	成果項目	量化	名稱或內容性質簡述
科教處計畫加填項目	測驗工具(含質性與量性)	0	
	課程/模組	0	
	電腦及網路系統或工具	0	
	教材	0	
	舉辦之活動/競賽	0	
	研討會/工作坊	0	
	電子報、網站	0	
	計畫成果推廣之參與（閱聽）人數	0	

國科會補助專題研究計畫成果報告自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估

■達成目標

□未達成目標（請說明，以 100 字為限）

□實驗失敗

□因故實驗中斷

□其他原因

說明：

2. 研究成果在學術期刊發表或申請專利等情形：

論文：■已發表 □未發表之文稿 □撰寫中 □無

專利：□已獲得 □申請中 ■無

技轉：□已技轉 □洽談中 ■無

其他：（以 100 字為限）

此計畫為國防科技學術合作計畫，校方繳交下列產出給中山科學研究院

報告產出

1.惡意電路檢測技術蒐集與研析報告

2.Power-based 訊號分析報告

3.Timing-based 訊號分析報告

4.旁通道訊號分析演算法之效能評估報告

5.硬體木馬電路案例蒐集與研析報告

6.設計硬體木馬電路報告

7.硬體木馬偵測雛型規劃報告

相關程式碼

針對 DES 之惡意電路設計流程相關程式碼

路徑延遲旁通道訊號分析相關程式碼

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）（以 500 字為限）

(一)學術技術面

IC 發展重點從 70 年代注重面積，80 年代著重於執行速度，90 年代功率，到現今應該要轉為安全、隱私方面去發展，本計畫研究硬體惡意行為檢測，是為了應付以往我們缺乏注意的領域，在計畫中採用了旁通道訊號分析的方式檢驗電路中是否有硬體木馬，也在 DES 電路中實作硬體木馬並驗證其效能，此研究可更進一步發展安全性 IC，於 IC 中放置檢測電路或防護模組，這項動作可能會導致面積的增大，速度的降低以及耗電量的增加，這在設計上以及概念上與傳統設計考量上差異頗大，但為了確保硬體的安全性是值得去研究。

(二)經濟面效益

雖然目前沒有惡意電路的商業案例，但各研究報告顯示依目前的 IC 設計流程具有不

少漏洞可以植入硬體木馬，此研究所探討的硬體安全性問題，讓業界考量其產品設計流程是否相同問題並佈局因應之道。