經濟部 111 年度

《臺灣資安卓越深耕-半導體及供應鏈資安關鍵技術發展計畫》

合作研究計畫

《旁通道攻擊自動化偵測與防禦計畫》

建議書徵求文件

財團法人資訊工業策進會

中華民國　111 年 03 月 24 日

111年度合作研究計畫建議書徵求文件

一、簡介

隨著近年來積體電路製程技術之快速演進，先進晶片中的電晶體密度也大幅成長，這些晶片的測試複雜度亦急遽增加。為有效測試這些晶片，在電路中加入一些易測性設計已成為開發晶片之必要方法，而其中尤以在晶片加入掃描鏈 (scan chain) 及配合國際測試標準，如IEEE Std. 1149.1 及 Std. 1687，之相關電路最廣為業界採用，目前幾已成為所有數位電路必備的電路測試架構。然而加入這些電路雖可增加晶片的可觀察性及可控制性，讓使用者能夠更有效地對晶片進行測試，但這些特性亦成為攻擊者攻擊晶片的一大利器。在沒有適當防禦機制下，這些電路架構很可能被攻擊者惡意操縱，竊取儲存在硬體電路內部的重要資訊，甚或破壞電路之運作功能，其中以各種加解密電路受到攻擊以致密鑰(cipher key)遭破解時最為嚴重。本計畫的目的是研究基於掃描鏈等的旁通道攻擊所引發的硬體資安的問題，以便充分了解若無適當防禦機制，則硬體或晶片亦如軟體程式一樣，極可能受到攻擊。本計畫需規劃針對目前常用之加密電路，設計其攻擊模型，透過掃描鏈及測試標準電路來攻擊加密電路，以竊取加密電路中所使用之密鑰。

二、計畫目標

本計畫目標在針對目前界常用之加密電路(例如 AES 加密電路)，進行分別基於掃描鏈及國際測試標準電路之攻擊，且在 FPGA 開發版上實現對加密電路之實際攻擊行為，以展示如何藉由這些電路竊取加密電路中所使用之密鑰，證實硬體資安漏洞是極可能發生而需要被重視的。本計畫需提供一個已加上掃描鏈及一個加上國際測試標準電路之加密電路之 Verilog code，並可透過 FPGA 系統之合成軟體將之植入 FPGA 電路板中以進行實際操作。本計畫亦需提供包含詳細攻擊進行步驟及所需控制訊號及資料之範例。本計畫可假設執行者已熟知所採用之加密電路之運作流程，且在運用本計畫之攻擊模式時，執行者需自行準備符合此實證所需之 FPGA 軟硬體設備，包含其操作軟體及系統整合工具。

三、計畫範圍

本計畫預計研究以下主要項目：

- 分析常用之加密技術如何在一般電路上針對資料進行加密
- 如何以 Verilog code 撰寫加密電路程式並完成其電路設計
- 如何在一個具加密電路之設計中加上掃描鏈
- 如何在一個具加密電路之設計中加上符合國際測試標準(如邊緣掃描 boundary scan, i,e., IEEE Std. 1149.1 及 internal boundary scan, i.e., IEEE

Std. 1687) 之電路

- 如何透過掃描鏈進行攻擊，竊取加密電路之金鑰
- 如何透過國際測試標準電路進行攻擊，竊取加密電路之金鑰
- 以上電路及攻擊方法在 FPGA 電路板之實作

四、 預期成果

本計畫須配合母計畫需要進行研究，並產出以下成果：

1. 一個具加密功能之電路之 Verilog code
2. 一個加上掃描鏈及加密電路之 Verilog code
3. 一個加上符合國際測試標準(如邊緣掃描 boundary scan 及 internal boundary scan) 及加密電路之 Verilog code
4. 一套透過掃描鏈對加密電路進行攻擊之方法及進行步驟
5. 一套透過國際測試標準電路對加密電路進行攻擊之方法及進行步驟
6. 以上之電路需能以 FPGA 系統之合成軟體將之植入 FPGA 電路板中並可進行實際操作。
7. 以上各項之詳細操作說明書

※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。

四、 執行方式

- 合作計畫執行單位應配合本會計畫監控機制。
- 於計畫執行期間，合作計畫執行單位須配合計畫所需，每月至少固定一次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為主。
- 於計畫執行期間，合作計畫執行單位須配合計畫所需，不定期與本單位回報研究進度與內容。
- 交付說明

項次	交付項目	交付內容	數量	交付型態	交付期限
1	期中研究報告	內容包含： 1. 一個具加密功能之電路之 Verilog source code 2. 一個加上掃描鏈及加密電路之	1 份	電子檔	111 年 6 月 30 日

		Verilog source code 3. 以 FPGA 系統之合成軟體將 1.及 2.項之電路植入 FPGA 電路板之說明書。 4. 在 3.項電路進行攻擊之構想及說明書。 5. 前述實證攻擊模型成效報告。			
2	期末研究報告	內容包含： 1. 一個加上符合國際測試標準(如邊緣掃描 boundary scan 或 internal boundary scan) 及加密電路之 Verilog source code 2. 以FPGA系統之合成軟體將上述符合國際測試標準及加密電路植入 FPGA 電路板中之說明書。 3. 在 2. 項電路進行攻擊之構想及說明書。 4. 前述實證攻擊模型成效報告。 5. 除期末研究報告(word 檔)外，另提供一份結案簡報(PPT 檔)	1 份	電子檔	111 年 10 月 30 日

五、 計畫期程及預估計畫總經費

計畫執行區間： 111 年 4 月 1 日 至 111 年 12 月 15 日

總經費：700,000元

六、 驗收標準(含教育訓練)

- 依本建議書徵求文件第五點「執行方式」內的交付說明要求，如期繳交相關成果。

七、 技術能力需求

提案者需具備以下設備及能力：

1. 進行電路模擬及合成之相關 EDA 軟體
2. 電腦及週邊相關硬體設備
3. 具備加密電路之相關知識
4. 具備硬體電路攻擊方法之相關知識

5. 具掃描鏈架構之相關知識
6. FPGA 開發版及相關軟體。