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

《晶片安全檢測研究計畫》

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

電腦、電子設備、通訊等資通訊技術（以下簡稱ICT）已被大量使用於國防軍事系統以及與國民生計相關的關鍵基礎設施，且現代社會對ICT依賴程度日漸增加，而確保資訊安全是ICT應用的先決條件。在ICT採購全球化趨勢下，ICT產業供應鏈安全是所有產品與服務供應鏈的基礎。在ICT供應鏈中，各種軟硬體、應用程式、資訊服務，多少會使用外部供應商技術元件。但因為使用者可能無法有效掌握這些外部技術元件的安全性，一旦駭客能攻擊產業供應鏈中的環節，將對產品的安全性產生深遠的影響。

資料加密是達到資訊安全的基礎，而現代的資料加密技術須由晶片執行複雜的密碼演算法完成，故密碼演算法的性能及晶片本身的安全等級，都是影響ICT產品安全性的關鍵。對晶片本體進行非侵入式攻擊的目的，在竊取密鑰等關鍵安全參數（以下簡稱CSP），而其手法則包括旁通道攻擊等。因此，晶片本體抵禦旁通道攻擊的能力，亦應為ICT採購的指標，而此能力可交由公正之專業測試實驗室予以評估，以認證其安全等級。為達成上述目的，資策會執行經濟部「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」，欲委託學界協助完成對晶片本體進行攻擊測試的方法，以測試產品的密碼模組，是否可以抵禦旁通道攻擊。目的是提供業者於產品設計研發製造過程中的資安控制項目及做法之參考。

二、 計畫目標

本計畫將對於晶片抵禦非侵入式攻擊的能力進行評估，目標為研析如何以旁通道攻擊技術來對晶片本體進行攻擊測試，並據測試結果評估晶片本體之安全等級。旁通道攻擊手法包括：時序分析（以下簡稱TA）、簡單功耗分析/簡單電磁分析（以下簡稱SPA/SEMA）、差分功耗攻擊/差分電磁分析（以下簡稱DPA/DEMA）。檢測對象為對稱式及非對稱式密碼演算法，包括AES、RSA、ECC等。測試方法為從待測晶片收集足夠的量測資料，使用一套統計方法分析所收集的資料，並針對單個密碼演算法進行CSP 類別的安全測試，以分析其是否產生顯著之資訊外洩，並據以判定待測晶片是否過該測試類別。測試方法須滿足ISO/IEC 17825:2016之規範。

三、 計畫範圍

本計畫預計研究以下主要項目：

- 定義對於對稱式密碼演算法（包括AES）進行TA、SPA/SEMA、DPA/DEMA所需之測試資料集（Test Pattern Set）。該測試資料集必須符合ISO/IEC 17825:2016之規範。
- 定義對於非對稱式密碼演算法（包括RSA、ECC）進行TA、SPA/SEMA、DPA/DEMA所需之測試資料集。該測試資料集必須符合ISO/IEC 17825:2016之規範。
- 在上述各種檢測手法中，其測試資料集必須對安全等級3（Security Level 3）及安全等級4（Security Level 4）分別定義。

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. 配合主計畫執行進度，協助進行晶片安全相關專利一案之工作項目，包含撰寫專利構想書及交付專利提案簡報、出席專利審查會議進行答辯等。

2. 於111年5月底交付期中報告，內容包含：
   - 對AES進行TA所需之測試資料集，含安全等級3及安全等級4之測試資料集。
   - 對AES進行SPA/SEMA所需之測試資料集，含安全等級3及安全等級4之測試資料集。
   - 對AES進行DPA/DEMA所需之測試資料集，含安全等級3及安全等級4之測試資料集。
3. 於111年9月底交付期末報告，內容包含：
   - 對RSA進行TA所需之測試資料集，含安全等級3及安全等級4之測試資料集。
   - 對RSA進行SPA/SEMA所需之測試資料集，含安全等級3及安全等級4之測試資料集。
   - 對RSA進行DPA/DEMA所需之測試資料集，含安全等級3及安全等級4之測試資料集。
   - 對ECC進行TA所需之測試資料集，含安全等級3及安全等級4之測試資料集。
   - 對ECC進行SPA/SEMA所需之測試資料集，含安全等級3及安全等級4之測試資料集。
   - 對ECC進行DPA/DEMA所需之測試資料集，含安全等級3及安全等級4之測試資料集。
4. 於111年11月底前，完成國內外研討會或期刊論文投稿兩篇。

※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. 對 AES 進行 TA 所需之測試資料集，含安全等級 3 及安全等級 4 之測試資料集。 2. 對 AES 進行 SPA/SEMA 所需之測試資料集，含安全等級 3 及安全等級 4 之測試資料集。 3. 對 AES 進行 DPA/DEMA 所需之測試資料集，含安全等級 3 及安全等級 4 之測試資料集	1 份	電子檔	111 年 5 月 31 日
2	期末研究報告	內容包含： 1. 對 RSA 進行 TA 所需之測試資料集，含安全等級 3 及安全等級 4 之測試資料集。	1 份	電子檔	111 年 9 月 30 日

		2. 對 RSA 進行 SPA/SEMA 所需之測試資料集，含安全等級 3 及安全等級 4 之測試資料集。 3. 對 RSA 進行 DPA/DEMA 所需之測試資料集，含安全等級 3 及安全等級 4 之測試資料集。 4. 對 ECC 進行 TA 所需之測試資料集，含安全等級 3 及安全等級 4 之測試資料集。 5. 對 ECC 進行 SPA/SEMA 所需之測試資料集，含安全等級 3 及安全等級 4 之測試資料集。 6. 對 ECC 進行 DPA/DEMA 所需之測試資料集，含安全等級 3 及安全等級 4 之測試資料集。			
3	協助進行晶片安全相關專利	依主計畫執行進度，配合執行晶片安全相關專利之工作項目，內容包含但不限於： ● 專利構想書 ● 專利提案簡報	1 案	電子檔	111 年 11 月 30 日
4	投稿國內外知名研討會或期刊論文	論文投稿接受證明	2 篇	電子檔	111 年 11 月 30 日

六、 計畫期程及預估計畫總經費

計畫執行區間： 111 年 01 月 01 日 至 111 年 11 月 30 日

總經費：800,000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 IC 晶片電路設計，或擁有相關授課經驗之學界研究人員。
- 熟悉密碼演算法之學界研究人員。
- 熟悉硬體安全知識領域，並對各類非侵入式攻擊有實際操作或研究經驗的技術或學界研究人員。